Номер проекта:

04-01-00167

Название проекта:

“Моделирование процессов защиты информации в компьютерных сетях в антагонистической среде: формальный подход, математические модели, многоагентная архитектура, программный прототип и экспериментальная оценка”.

Ф.И.О. руководителя проекта:

Котенко Игорь Витальевич

Краткая аннотация:

Основная задача проекта заключалась в разработке, прототипировании и оценке формальных моделей процессов защиты информации в компьютерных сетях, рассматриваемых в виде антагонистического взаимодействия злоумышленников и компонентов систем защиты информации, а также выработке рекомендаций по их использованию для защиты информации в компьютерных сетях и созданию теоретических основ построения интегрированных многоагентных систем защиты, способных функционировать в антагонистической среде (на примере реализации распределенных атак “Отказ в обслуживании” и механизмов защиты от них, а также вирусных эпидемий и защиты от них).

При выполнении проекта решены следующие основные подзадачи:

(1) разработан формальный подход к основанному на агентских технологиях моделированию процессов защиты информации в компьютерных сетях в антагонистической среде;

(2) предложены принципы построения и структура основанной на онтологии, распределенной базы знаний для моделирования процессов компьютерного противоборства;

(3) разработаны формальные модели командной работы агентов-злоумышленников и агентов защиты (в том числе их кооперации, самоадаптации и эволюции), а также формальные модели компьютерной сети Интернет;

(4) разработана многоагентная архитектура системы моделирования процессов компьютерного противоборства;

(5) реализован программный прототип этой системы, обладающий развитыми возможностями по моделированию и исследованию процессов защиты информации;

(6) на основе проведения комплекса экспериментов по моделированию антагонистических процессов противоборства злоумышленников и компонентов защиты осуществлена оценка предложенных результатов. Эксперименты были проведены для различных сценариев атак и механизмов защиты, исследовались сети различной структуры, в которых были реализованы разные политики безопасности.

Проведенные эксперименты показали возможность и эффективность использования предлагаемого подхода и инструментального средства для моделирования перспективных механизмов защиты и анализа защищенности проектируемых сетей.

Кроме того, в работе получен ряд дополнительных результатов, которые существенно расширяют сферу применения основных результатов. В частности, разработаны модели функционирования ложных (обманных) информационных систем, модели, методики и прототипы активного анализа защищенности компьютерных сетей, основанного на автоматической генерации и выполнении распределенных сценариев атак с учетом разнообразия целей и уровней знаний злоумышленников, архитектура, отдельные модели и прототипы компонентов верификации политик безопасности компьютерных сетей и их проактивного мониторинга.

Abstract:

The primary goal of the project consisted in the development, prototyping and estimation of the formal models of computer network security processes considered as antagonistic interaction of malefactors and security components. We also intended to develop recommendations on application of these models for computer networks security solutions and for creating the theoretical foundations of integrated multi-agent security systems capable to function in an antagonistic environment (on an example of "Distributed Denial of Service (DDoS)" attacks and mechanisms of protection against them, and also virus epidemics and protection against them).

During the project the following main subtasks were solved:

(1) The multi-agent approach to the modeling and simulation of computer network security processes in conditions of antagonistic environment was suggested;

(2) The principles of construction and the structure of ontology-based distributed knowledge base for modeling and simulation of computer network counteraction processes were offered;

(3) The formal models of teamwork of agents-malefactors and security agents (including their cooperation, self-adapting and evolution), and also the formal models of the Internet were developed;

(4) The multi-agent environment framework for simulation of computer network counteraction processes was developed;

(5) The software prototype of this system was implemented; it possesses advanced opportunities for investigation of security processes;

(6) The estimation of the offered results was carried out on the basis of fulfillment of different experiments. The experiments have been lead for various attacks scenarios, security mechanisms, network structures and security policies.

The experiments have shown efficiency of the offered approach and an opportunity of its usage for modelling and simulation of perspective protection mechanisms and the security analysis of computer networks designed.

Furthermore, in the project we developed a number of additional results which essentially expand the sphere of application of the main results. The models of deception information systems were elaborated. The models, techniques and prototypes for active security analysis of computer networks (based on automatic generation and fulfillment of distributed attack scripts) were developed. These models, techniques and prototypes take into account a variety of purposes and knowledge levels of malefactors. The generalized architecture, particular models and prototypes of components for verification and proactive monitoring of security policies in computer networks were designed and implemented.

Развернутый научный отчет:

Коды классификатора, соответствующие содержанию фактически проделанной работы

01-201 01-202 01-211 07-520 07-530 07-570

Объявленные ранее цели проекта

Задача проекта формулировалась как разработка и исследование математических моделей процессов защиты информации в компьютерных сетях в виде компьютерного противоборства злоумышленников и компонентов защиты информационных ресурсов компьютерных сетей на основе использования формальных моделей и методов распределенного искусственного интеллекта, в том числе многоагентных технологий.

Решение этой задачи планировалось осуществить на основе исследовательского компьютерного многоагентного моделирования указанного противоборства.

При выполнении проекта предполагалось:

(1) разработать формальный подход к основанному на агентских технологиях моделированию процессов защиты информации в компьютерных сетях в антагонистической среде;

(2) предложить принципы построения и структуру основанной на онтологии, распределенной базы знаний для моделирования процессов компьютерного противоборства;

(3) разработать формальные модели командной работы агентов-злоумышленников и агентов защиты, а также формальные модели компьютерной сети;

(4) разработать многоагентную архитектуру системы моделирования процессов компьютерного противоборства;

(5) реализовать программный прототип этой системы;

(6) осуществить теоретическую и экспериментальную оценку предложенных результатов.

Основными целями проекта на 2006 год являлись:

(1) разработка уточненной постановки задачи, концептуальной модели, онтологии и формальных моделей реализации антагонистических процессов противоборства злоумышленников и компонентов защиты;

(2) разработка моделей самоадаптации и эволюции агентов;

(3) доработка программного прототипа системы моделирования;

(4) теоретическая и экспериментальная оценка предложенного подхода и разработанной системы моделирования, а также разработка рекомендации по их использованию.

Степень выполнения поставленных в проекте задач

Все задачи, запланированные в проекте, выполнены полностью.

Решены также дополнительные задачи, связанные с разработкой модели функционирования ложных (обманных) информационных систем, созданием моделей, методик и прототипов активного анализа защищенности компьютерных сетей, основанного на автоматической генерации и выполнении распределенных сценариев

атак с учетом разнообразия целей и уровней знаний злоумышленников, разработкой архитектуры, отдельных моделей и прототипов компонентов верификации политик безопасности компьютерных сетей и их проактивного мониторинга.

Полученные за отчетный год важнейшие результаты

Основные результаты проекта – математические и компьютерные модели процессов защиты информации, реализуемых в компьютерных сетях, в том числе в Интернет, которые формализуют антагонистическое взаимодействие злоумышленников и компонентов систем защиты информации, а также разработанная программная система многоагентного моделирования этих процессов и сами результаты компьютерного моделирования.

Дадим характеристику отдельных результатов, полученных за отчетный период:

1. Разработаны постановка задачи и концептуальная модель реализации антагонистических процессов противоборства злоумышленников и компонентов защиты компьютерных сетей, основанной на агентских технологиях. Задача многоагентного моделирования процессов кибернетического противоборства представлена как моделирование коэволюционного антагонистического взаимодействия команды агентов-злоумышленников и агентов защиты. Для исследовательского моделирования процессов кибернетического противоборства предложено использовать семейство различных моделей (аналитических, гибридных (аналитико-имитационных), имитационных на уровне сетевых пакетов, полунатурных и натурных). Выбор моделей диктуется, в первую очередь, необходимой точностью и масштабируемостью моделирования. Например, аналитические модели позволяют имитировать глобальные процессы, происходящие в Интернет (например, вирусные эпидемии), однако эти модели описывают моделируемые процессы только на абстрактном уровне. Имитационное моделирование на уровне пакетов предоставляет возможность достаточно адекватно воспроизводить протекающие процессы, представляя атакующие и защитные действия с помощью обмена сетевыми пакетами, точно имитируя работу по протоколам канального, сетевого, транспортного и прикладного уровней. Наибольшая точность имитации достигается на аппаратных стендах при натурном моделировании, однако при этом удается моделировать достаточно ограниченные фрагменты взаимодействий агентов. Основное внимание в настоящем проекте уделено применению имитационного моделирования на уровне пакетов с использованием в качестве базового уровня среды моделирования соответствующих средств имитационного моделирования, позволяющих имитировать сетевые процессы (задействуя сетевой, транспортный и прикладной уровни). Концептуальная модель противоборства включает в себя: (1) онтологию приложения в области защиты информации, содержащую множество понятий приложения и отношений между ними; (2) протоколы командной работы агентов различных команд (команд злоумышленников и команд (компонентов) системы защиты информации; (3) модели сценарного индивидуального, группового и общекомандного поведения агентов в рамках конкретных намерений, реализуемых сценариями; (4) коммуникационную компоненту, предназначенную для обмена сообщениями между агентами; (5) модели среды функционирования – компьютерной сети, включающие топологический и функциональные компоненты.

2. Разработан фрагмент основанной на онтологии, распределенной базы знаний для моделирования процессов компьютерного противоборства (на примере реализации распределенных атак “Отказ в обслуживании” и механизмов защиты от них). Эта онтология структурирует основные известные типы атак и отношений между ними и включает в себя макро-уровень, на котором описываются структурные отношения на множестве атак, и микро-уровень, на котором описываются модели реализации конкретных атак в виде последовательностей атакующих действий. Верхний уровень онтологии механизмов защиты от DDoS-атак составляют узлы, задающие уровни механизмов защиты (системный, сетевой, глобальный). На нижних уровнях онтологии эти узлы раскрываются на конкретные механизмы защиты. Механизмы разделяются на четыре класса: (1) предупреждения атаки, (2) обнаружения факта атаки, (3) определения источника атаки, (4) противодействия атаке.

3. Разработаны формальные модели командной работы агентов-злоумышленников и агентов защиты, основанных на гибридном подходе к реализации командной работы агентов (на примере реализации распределенных атак “Отказ в обслуживании” и механизмов защиты от них). Разработаны формальные модели защищаемой компьютерной сети.

Предлагаемый гибридный подход базируется на совместном использовании элементов теории общих намерений, теории разделяемых планов и комбинированных подходов. Предполагается, что командная работа агентов организуется с помощью общего (группового) плана действий, особенности которого заключаются в следующем: (1) групповой план действий требует, чтобы команда агентов пришла к согласию выполнять предписание (множество заданных инструкций); (2) агенты должны принять на себя обязательства по отношению не только к своим индивидуальным действиям, но также к действиям других агентов и действиям группы в целом; (3) план групповой деятельности может иметь в качестве компонентов как планы индивидуальных агентов для назначенных действий, так и планы подгрупп; (4) при выполнении командной работы агенты команды должны с помощью коммуникаций прийти к согласию с предписанием, а также согласовать собственные намерения друг с другом.

Выделены два основных типа компонентов системы атаки: “демон” – агент, непосредственно выполняющий атаку DoS, “мастер” – агент, выполняющий действия по координации остальных компонентов системы. Демоны могут выполнять атаку в различных режимах. Это влияет на возможности команды защиты по обнаружению и блокированию атаки, а также прослеживанию и устранению агентов атаки. Демоны могут отправлять пакеты атаки с различной интенсивностью, подменять адрес отправителя и делать это с различной частотой.

Определены следующие классы агентов защиты: первичной обработки информации (“сенсор”); сбора данных для формирования модели трафика сети и обучения распознаванию атак (“сэмплер”); детектирования (“детектор”); фильтрации (“фильтр”); расследования. Дополнительно выделяется еще один класс агентов – агенты управления (“менеджеров”), которые служат для взаимодействия с администратором безопасности и конфигурирования системы защиты. Агенты-сенсоры осуществляют мониторинг сетевых процессов с целью сбора статистических данных. Полученные данные передаются агентам детектирования для выявления аномалий и возможности атаки DDoS. Сэмплеры собирают дынные о нормальном функционировании сети, чтобы затем выявлять аномалии. Агенты детектирования принимают решение, есть ли опасность атаки DDoS, и от каких узлов она может

исходить. Они передают эту информацию агентам расследования и (или) фильтрации. Агенты фильтрации устанавливаются на пути прохождения сетевых пакетов к защищаемому узлу или сети. Агенты фильтрации могут использовать различные механизмы фильтрации злонамеренных сетевых пакетов. Агенты расследования пытаются проследить источники атак DDoS и обезвредить их путем вывода из строя соответствующих агентов атаки.

Специализация каждого агента атаки или защиты отражается подмножеством узлов разработанной онтологии. Некоторые узлы онтологии могут быть общими для пары или большего количества агентов. Обычно только один из этих агентов обладает детально структурированным описанием этого узла. Именно этот агент является обладателем соответствующего фрагмента базы знаний. В то же время, некоторая часть онтологических баз знаний является общей для всех агентов, и именно эта часть знаний является тем фрагментом, который должен играть роль общего контекста (общих знаний).

4. Разработана многоагентная архитектура системы моделирования компьютерного противоборства команд агентов-злоумышленников и агентов защиты (на примере реализации распределенных атак “Отказ в обслуживании” и механизмов защиты от них) и объектно-ориентированный проект прототипа системы моделирования компьютерного противоборства команд агентов-злоумышленников и агентов защиты.

Для реализации подхода используется архитектура среды моделирования, включающая базовую систему имитационного моделирования (Simulation Framework), модуль (пакет) моделирования сети Интернет (Internet Simulation Framework), подсистему агентно-ориентированного моделирования (Agent-based Framework) и модуль (библиотеку) имитации процессов предметной области (Subject Domain Library).

Компонент Simulation Framework представляет систему моделирования на основе дискретных событий. Остальные компоненты являются надстройками или моделями для Simulation Framework.

Компонент Internet Simulation Framework – комплект модулей, позволяющих реалистично моделировать узлы и протоколы сети Интернет. Наивысший уровень абстракции в моделировании IP – это сеть, состоящая из IP-узлов. Узел может быть маршрутизатором или хостом. IP-узел отвечает компьютерному представлению стека протоколов Интернет. Предполагается, что модули, из которых он состоит, организованы так, как происходит обработка IP-дейтаграммы в операционных системах. Обязательным является модуль, отвечающий за сетевой уровень (реализующий обработку IP) и модуль “сетевой интерфейс”. Дополнительно можно подключать модули, реализующие протоколы транспортного уровня.

Многоагентное моделирование реализуется посредством компонента Agent-based Framework, который использует модуль имитации процессов предметной области. Данный компонент представляет собой библиотеку модулей, задающих интеллектуальных агентов, реализованных в виде приложений. При проектировании и реализации модулей агентов подразумевается использование элементов абстрактной архитектуры FIPA. Для взаимодействия агентов необходим язык коммуникаций. Передача сообщений между ними происходит поверх TCP-протокола, реализованного в компоненте Internet Simulation Framework. Каталог агентов является обязательным только для агента, координирующего действия других. Агенты могут управлять другими модулями с помощью сообщений.

Компонент Subject Domain Library – это библиотека, служащая для имитации процессов предметной области, а также модули, дополняющие функциональность IP-узла: таблица фильтрации и анализатор пакетов.

5. Разработана программная система моделирования распределенных атак “отказ в обслуживании” и механизмов защиты от них.

Для выбора инструментария моделирования сети и процессов передачи информации был проведен анализ различных пакетов моделирования (Network simulators), включая NS2, OMNeT++ INET Framework, SSF Net, J-Sim INET Framework и ряда других. Проведенный анализ показал, что предъявляемым требованиям в наилучшей степени удовлетворяет OMNeT++ INET Framework. На основе INET Framework разработан прототип среды для многоагентного моделирования сетевых атак и механизмов защиты от них.

Таким образом, для реализации исследовательской среды используется архитектура системы моделирования, включающая базовую систему имитационного моделирования (на базе OMNeT++), модуль (пакет) моделирования сети Интернет (с использованием OMNeT++ INET Framework), подсистему агентно-ориентированного моделирования и модуль (библиотеку) имитации процессов предметной области (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. В процессе экспериментов можно варьировать топологию и конфигурацию сети, структуру и конфигурацию компонентов атаки и защиты, механизмы реализации атак и защиты, параметры кооперации и противоборства и др. На основе экспериментов проводятся измерения различных показателей эффективности механизмов защиты, и выполняется анализ условий и возможности их применения.

В реализованной к настоящему времени версии среды система OMNeT++ INET Framework подверглась множеству различных модификаций. В том числе были созданы таблица фильтрации пакетов на сетевом уровне для моделирования действий агентов защиты, модуль, позволяющий просматривать весь трафик данного узла для ведения статистики, а также для моделирования действий агентов защиты. Подверглись изменению модули, отвечающие за работу Sockets для моделирования атак и механизмов защиты. Агенты атаки и защиты были реализованы в виде сложных модулей (compound module). Они содержат простые модули, отвечающие за работу по различным сетевым протоколам, и ядро агента. Ядро агента служит для управления остальными модулями. Агент, как сложный модуль, имеет ряд шлюзов для подключения к стандартному сетевому узлу из INET Framework. Эти шлюзы относятся к соответствующим сетевым протоколам. Подключение или установка агента может происходить во время проведения моделирования.

При проектировании и реализации агентов были использованы элементы абстрактной архитектуры FIPA: язык коммуникаций, транспортный и сетевой уровни, каталог агентов. Агенты устанавливались в среду моделирования с помощью подключения к транспортному и сетевому уровням OMNeT++ INET Framework. Сеть для многоагентного моделирования состоит из трех подсетей: подсеть защиты, где расположена команда защиты; промежуточная подсеть, в которой расположены узлы, создающие типовой трафик в сети, в том числе к защищаемому узлу; подсеть атаки, где расположена команда атаки.

Пример *пользовательского интерфейса* среды моделирования показан на рис.1. На основном окне визуализации (рис. 1, справа) отображается компьютерная сеть для

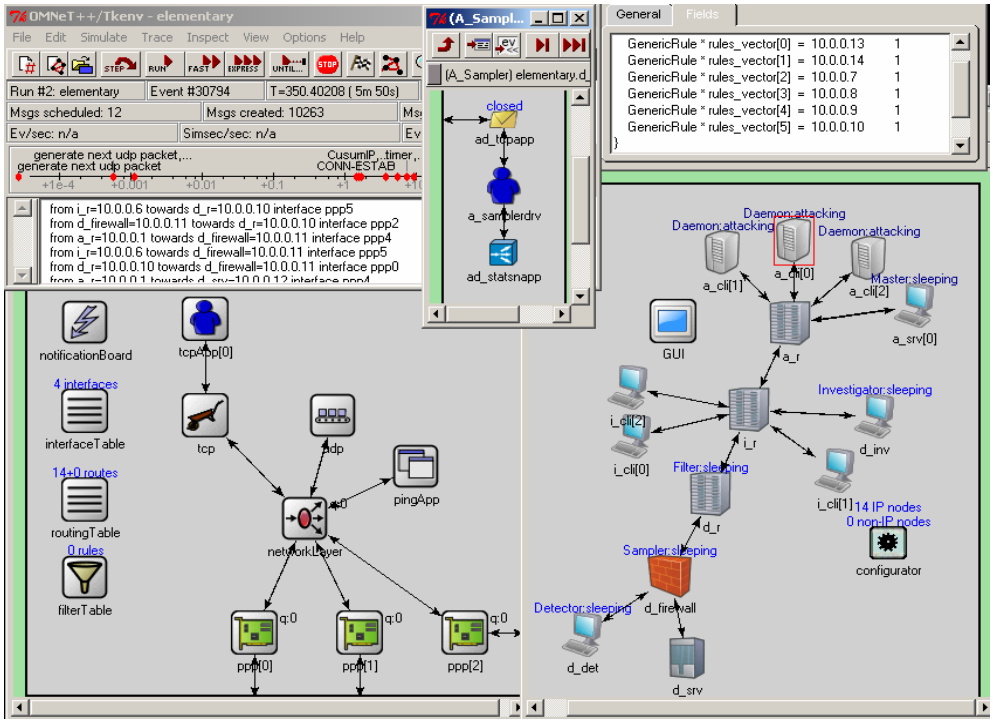

Рис.1. Пример пользовательского интерфейса

проведения моделирования. Окно управления процессом моделирования (рис. 1, слева вверху) позволяет просматривать и менять параметры моделирования. В данном окне на шкале времени можно наблюдать события, значимые для понимания атак и механизмов защиты. Шкала времени отображается над окном с текстовым описанием событий. На рис. 1 можно видеть, например, события установки соединения TCP, действие сенсора, инициирование атаки и др. Для отображения текущего состояния команд агентов служат соответствующие окна состояний (рис. 1, сверху посередине). Можно открывать различные окна, характеризующие функционирование (статистические данные) отдельных хостов, протоколов и агентов, например, на рис. 1 (справа вверху) отображено, характеризующее таблицу фильтрации одного из хостов. Приложения (в том числе и агенты) устанавливаются на узлы сети, подключаясь к соответствующим модулям протоколов. Агенты устанавливаются в среду моделирования с помощью подключения к транспортному и сетевому уровням OMNeT++ INET Framework (Рис.1, вверху посередине).

Пример основного окна, на котором отображается *компьютерная сеть для проведения моделирования*, показан на Рис.. Исследуемая компьютерная сеть представляет собой набор узлов, соединенных каналами связи. Узлы могут нести различную функциональность в зависимости от их параметров или набора внутренних модулей. Овальным значком обозначены маршрутизаторы. Красным подсвечены узлы, на которых располагаются агенты команды атаки, зеленым – узлы, на которых находятся агенты команды защиты. Над окрашенными узлами есть соответствующие надписи, говорящие о типе агента и его состоянии. Остальные узлы – типовые, создающие стандартный трафик сети. Узлы сети соединяются между собой каналами связи, параметры которых можно изменять.

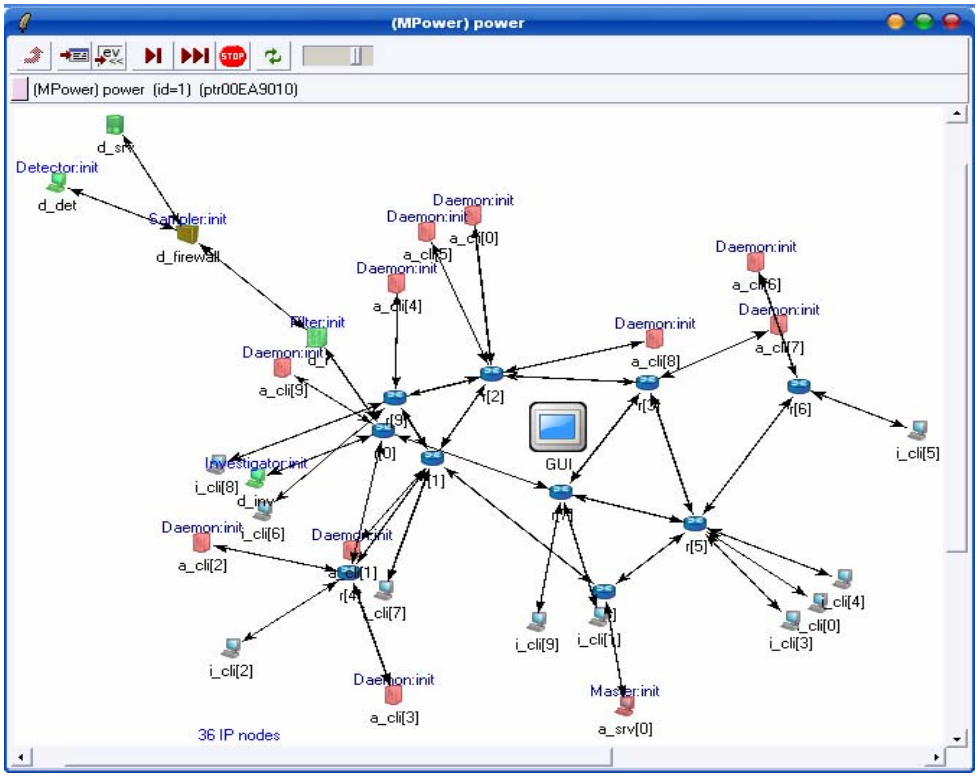

Рис.2. Пример компьютерной сети для проведения моделирования

6. На примере моделирования процессов реализации распределенных атак “отказ в обслуживании” и механизмов защиты от них проведено множество различных экспериментов по имитации противоборства в сети Интернет. Эксперименты были проведены для различных сценариев атак и механизмов защиты, исследовались сети различной структуры, в которых были реализованы разные политики безопасности.

В процессе экспериментов можно варьировать топологию и конфигурацию сети, структуру и конфигурацию команд атаки и защиты, механизмы реализации атак и защиты, параметры кооперации команд и др. На основе экспериментов проводятся измерения различных показателей эффективности механизмов защиты, и выполняется анализ условий и возможности их применения.

Сети, используемые для моделирования, состоят из различных подсетей, являющихся, например, зонами ответственности различных провайдеров. Выделяются подсеть защиты, где расположен ресурс, являющийся целью атаки, промежуточная подсеть, в которой находятся узлы, создающие типовой трафик, а также подсети атаки, где располагаются команды атаки. Сети генерируются с помощью алгоритмов, позволяющих создавать конфигурации, близкие к сети Интернет.

Для команды атаки в процессе экспериментов варьируется, например, интенсивность атаки в пакетах в секунду и способ подмены адреса отправителя. Для команд защиты в процессе экспериментов варьируются используемые методы защиты и параметры кооперации, задающие количество используемых в командах сэмплеров, способ кооперации и др. Исследованы следующие параметры эффективности механизмов защиты: доля отброшенного легитимного трафика (false positive); доля пропущенного трафика атаки (false negative); время реакции на атаку и др. Параметры эффективности механизмов защиты исследовались в зависимости от следующих параметров: конфигурация команд защиты (количество сэмплеров); конфигурация сети (количество легитимных клиентов); способ подмены адреса отправителя, используемый при атаке; интенсивность атаки и др.

Проведенные эксперименты показали эффективность предлагаемого подхода и возможность его использования для моделирования перспективных механизмов защиты и анализа защищенности проектируемых сетей.

7. Разработаны модели функционирования ложных (обманных) информационных систем, представляющих собой программно-аппаратные средства обеспечения информационной безопасности, основанные на технологии “ловушек” и ложных целей. Предлагаемый подход базируется на программной эмуляции компонентов информационных систем и на выделении трех уровней введения злоумышленников в заблуждение: (1) сегмента сети – эмулируется работа целого сегмента сети; (2) хоста – среди рабочих серверов используется хост-приманка; (3) сервисов и приложений – на серверах применяются программы, эмулирующие работу сервисов и приложений. Выполнена разработка прототипа программных средств обманной информационной системы. Реализованы программные средства, эмулирующие работу серверов FTP и HTTP, а также программные средства, реализующие пользовательский интерфейс, предоставляющий администратору возможности взаимодействия с компонентами системы и управления ими. Проведены эксперименты по изучению возможностей по реализации основных функций введения злоумышленников в заблуждение при реализации различного рода атак.

8. Разработаны модели, методики и прототипы для активного анализа защищенности компьютерных сетей, основанного на автоматической генерации и выполнении распределенных сценариев атак с учетом разнообразия целей и уровней знаний злоумышленников, и предназначенного для реализации на различных этапах жизненного цикла компьютерной сети, включая этапы проектирования и эксплуатации. Предложенный подход основан на применении базирующегося на экспертных знаниях комплекса моделей злоумышленника, генерации сценариев атак, оценки уровня защищенности, компьютерной сети и др. Результатами работы системы анализа защищенности, основанной на предлагаемом подходе, являются найденные уязвимости, трассы (графы) возможных многошаговых атак, “узкие места” в компьютерной сети, на которых основываются эти атаки, а также различные метрики безопасности, которые могут быть использованы для оценки уровня защищенности компьютерной сети и ее компонентов, а также сравнения различных конфигураций сети и реализаций политик безопасности.

9. Разработана обобщенная архитектура, отдельные модели и прототипы компонентов верификации политик безопасности компьютерных сетей. Предложены механизмы работы с политиками трех уровней: (1) верхнего уровня, приближенного к языку требований пользователя, (2) среднего уровня, классифицирующего правила по нескольким категориям, и (3) нижнего уровня, описывающего политику в формате Common Information Model (CIM).

Разработанные модели и программные средства предназначены для устранения возможных противоречий в спецификациях различных правил политик безопасности, а также определения возможности реализации этих правил на заданной компьютерной сети. Подход основан на многомодульной архитектуре и реализации механизмов поиска и разрешения противоречий с использованием как (1) модулей общего назначения (базирующихся на исчислении событий и абдуктивном выводе, а также на технике проверки на модели), позволяющих обнаруживать большинство противоречий (в том числе динамических), так и (2) специализированных модулей, работающих эффективно на конкретных типах противоречий.

10. Разработан подход, модели и программные компоненты проактивного мониторинга выполнения политики безопасности в компьютерных сетях. Подход к мониторингу политики безопасности базируется на активной имитации различных действий пользователей (как разрешенных, так и запрещенных политикой безопасности) и определении расхождений реакций системы от предписанных. Подход основан на планировании и формировании комплекса сценариев для проведения мониторинга политик, использовании распределенной системы сканеров, сбора и корреляции полученной от них информации. Предложенный подход, 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.

Степень новизны полученных результатов

Основные научные результаты являются новыми. Отличительной особенностью результатов является то, что они направлены на формализацию комплексного антагонистического характера обеспечения информационной безопасности как сложного организационно-технического процесса. В работе сделана попытка представления системы обеспечения информационной безопасности как единой холической системы, 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, которое разворачивается в настоящее время в Интернет, и перспективные подходы к обеспечению информационной безопасности.

Оригинальность полученных результатов подтверждается тем фактом, что до настоящего времени задача базирующегося на агентских технологиях моделирования компьютерного противоборства злоумышленников и компонентов защиты информации как соответствующих команд агентов в России не ставилась, а за рубежом проблема использования многоагентных систем для моделирования сложных антагонистических процессов защиты информации в компьютерных сетях была вынесена на обсуждение ориентировочно только в конце 90-х годов.

“Изюминкой” разработанного подхода, моделей и программных средств реализации исследовательской среды для изучения компьютерных атак и механизмов защиты от них является то, что они основаны на комбинировании агентно-ориентированного моделирования и имитационного моделирования на уровне сетевых пакетов. Это позволяет изучать сложные аспекты защиты с достаточной степенью адекватности. Разработанная программная среда моделирования основана, кроме того, на использовании открытой “библиотеки” методов реализации атак и защиты от них, что позволяет добавлять и исследовать новые модели атак и защиты.

Дальнейшее развитие работы направлено на развитие теоретического подхода и среды моделирования. В будущих исследованиях планируется расширение библиотеки атак и механизмов защиты, развитие функциональности отдельных компонентов моделирования. Важной составляющей будущих исследований является проведение многочисленных экспериментов по исследованию различных атак и эффективности перспективных механизмов защиты (предупреждения атаки, обнаружения факта атаки,

определения источника атаки и противодействия атаке) и их комбинации. Особое внимание будет уделяться исследованию кооперативных распределенных механизмов защиты, основанных на размещении компонентов защиты в различных подсетях Интернет, имитирующих взаимодействие различных поставщиков услуг Интернет.

Сопоставление полученных результатов с мировым уровнем

Все результаты, полученные в процессе выполнения проекта, соответствуют мировому уровню.

Разработанная среда позволяет исследовать различные классы атак и механизмов защиты. Авторы не нашли близких аналогов предлагаемому подходу и исследовательской среде в существующих разработках ведущих исследовательских центов в мире.

Авторы проекта апробировали и опубликовали полученные результаты на нескольких престижных российских и международных конференциях, семинарах, а также в журналах, в частности на 19-я Европейской мультиконференции по моделированию “Моделирование в расширенной Европе” (Рига, Латвия, 1–4 июня 2005 г.), Втором международном семинаре по безопасности в многоагентных системах - SASEMAS '05 (Утрехт, Голландия. 26 июля 2005 г.), Международном семинаре NATO по перспективным исследованиям "Безопасность и встроенные системы" (Патрас, Греция, 22-26 августа 2005 г.), 6-ом Международном семинаре по агентно-ориентированному моделированию (ABS6, Эрланген. Германия. 12 – 15 сентября 2005 г.), Третьем международном семинаре “Математические методы, модели и архитектуры систем защиты компьютерных сетей (MMM-ACNS-2005)” (Санкт-Петербург, 24-28 сентября 2005 г.), Международном семинаре NATO (Advanced Study Institute) “Безопасность компьютерных сетей и обнаружение вторжений” (Норк, Ереван, Армения, 1-12 октября 2005 г.), Международной конференции по интеллектуальным агентам, Web-технологиям и Интернет-коммерции - IAWTIC'2005 (Вена, Австрия, 28 – 30 ноября 2005 г.), 20-й Европейской конференции по моделированию (Бонн, Германия, 2006 г.), 9-й Международной конференции “Слияние информации” (Information Fusion-06, Флоренция, Италия, 2006 г.), Международной конференции по защите информации и криптографии (Сетубаль, Португалия, 2006 г.), 9-й Международной конференции по информационной безопасности (ISC-06, Самос, Греция, 2006 г.), 10-й Международной конференции IFIP по безопасности коммуникаций и мультимедиа (CMS'2006, Ираклион, Греция, 2006 г.), Международной конференции по кибермирам (CYBERWORLDS - CW2006, Лозанна, Швейцария, 2006 г.) и др.

Статья по результатам проекта была признана лучшей работой на 9-й Международной конференции по информационной безопасности (ISC-06, Самос, Греция, 2006 г.).

Руководитель проекта - И.В.Котенко – за цикл статей по проекту был признан победителем конкурса лучших работ в области искусственного интеллекта за 2004-2006 годы в номинации “Прикладные исследования” (на X Национальной конференции по искусственному интеллекту, сентябрь 2006 г.).

Практические результаты проекта демонстрировались на ряде выставок и конкурсов программных систем, в том числе, выставке программных средств на Европейской конференции и выставке в области защиты информации ISSE 2006 (Information Security Solutions Europe conference, Рим, Италия, 2006 г.), X Национальной

конференции по искусственному интеллекту с международным участием (КИИ-2006, Обнинск, 2006 г.), Международной конференции IST 2006 (Information SocietyTechnologies – Технологии информационного общества, Хельсинки, Финляндия, 2006 г.) и др.

Методы и подходы, использованные в ходе выполнения проекта

В качестве базиса для исследований в области моделирования противоборства злоумышленников и систем защиты в сети Интернет, используются 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 и др. При разработке предложенных формальных постановок, моделей, архитектур и прототипов использованы методы системного анализа и теории больших систем, методы распределенного искусственного интеллекта, теории защиты информации, теории имитационного моделирования, теории автоматов и синтаксического анализа, 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).

Предлагаемый в настоящей работе подход к организации командной работы агентов базируется на совместном использовании элементов теории общих намерений, теории разделяемых планов и комбинированных подходов и учитывает опыт программной реализации многоагентных систем. Структура команды агентов описывается в терминах иерархии групповых и индивидуальных ролей. Листья иерархии отвечают ролям индивидуальных агентов, промежуточные узлы – групповым ролям. Спецификация иерархии планов действий осуществляется для каждой из ролей. Для каждого плана описываются: начальные условия, когда план предлагается для исполнения; условия, при которых план прекращает исполняться; действия, выполняемые на уровне команды, как часть общего плана. Для групповых планов явно выражается совместная деятельность. Механизмы взаимодействия и координации агентов базируются на трех группах процедур: (1) обеспечение согласованности действий; (2) мониторинг и восстановление функциональности агентов; и (3) обеспечение селективности коммуникаций (для выбора наиболее “полезных” коммуникационных актов). Агенты могут реализовать механизмы самоадаптации и эволюционировать в процессе функционирования.

Для формирования команд агентов и координации действий между командами и отдельными агентами в зависимости от задачи моделирования могут быть использованы комбинации следующих методов и моделей:

(1) традиционные BDI-модели, определяемые схемами функционирования агентов, обуславливаемыми зависимостями предметной области;

(2) методы распределенной оптимизации на основе ограничений, использующие локальные взаимодействия при поиске локального или глобального оптимума;

(3) методы распределенного принятия решений на основе частично-наблюдаемых Марковских сетей, позволяющих реализовать координацию командной работы при наличии неопределенности в действиях и наблюдениях;

(4) теоретико-игровые модели и модели аукциона, фокусирующиеся на координации среди различных команд агентов, использующих рыночные механизмы принятия решений.

К настоящему времени программная среда позволяет исследовать различные механизмы защиты и модели кооперации между командами защиты, распределенными в сети: (1) кооперация на уровне агентов «фильтров»: команда, на сеть которой направлена атака, может применять правила фильтрации на «фильтрах» других команд; (2) кооперация на уровне агентов «сэмплеров»: команда, на сеть которой направлена атака, может получать информацию о трафике от «сэмплеров» других команд; (3) «Слабая» кооперация: команды могут получать информацию о трафике от «сэмплеров» некоторых других команд и применять правила фильтрации на «фильтрах» также некоторых других команд. В зависимости от степени кооперации каждой команде задается то или иное количество «известных» ей команд; (4) «Полная» кооперация: команда, на сеть которой направлена атака, может получать информацию о трафике от всех «сэмплеров» других команд и применять правила фильтрации на всех «фильтрах» других команд. Такие схемы кооперации используются в кооперативных методах защиты от DDoS: COSSACK, Perimeter-based DDoS defense, DefCOM, Gateway-based и ACC pushback, MbSQD, SOS и tIP router architecture. Схемы кооперации могут быть исследованы на основе анализа различных параметров, например, (1) величины входного трафика до и после «фильтра» команды, (2) процента нормального трафика и трафика атаки от всего трафика; (3) процента ложных срабатываний и пропусков атак команды. В качестве «эталона» для сравнения результатов используются результаты моделирования механизмов защиты без кооперации.

Адреса ресурсов в Интернете, 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=

Библиографический список всех публикаций по проекту за весь период выполнения проекта, предшествующий данному отчету

1. Котенко И.В. Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Конфидент, 2004. № 2, С.72-76; № 3, С.78-82.
2. Котенко И.В. Теоретические аспекты построения ложных информационных систем // III Санкт-Петербургская Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2003”). Труды конференции. Санкт-Петербург. 2004. С.59-68.
3. Котенко И.В., Степашкин М.В. Прототип имитатора информационной системы: архитектура и сценарии проведения экспериментов // III Санкт-Петербургская Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2003”). Труды конференции. Санкт-Петербург. 2004. С.68-73.
4. Уланов А.В., Котенко И.В. Моделирование атаки “Распределенный отказ в обслуживании” на примере использования вируса Mydoom // IX Санкт-Петербургская Международная Конференция “Региональная информатика-2004” (“РИ-2004”). Материалы конференции. СПб., 2004. С.155-156.
5. Степашкин М.В., Котенко И.В. Анализ признаков сетевых соединений и журналов регистрации событий операционной системы для обнаружения вторжений // IX Санкт-Петербургская Международная Конференция “Региональная информатика-2004” (“РИ-2004”). Материалы конференции. СПб., 2004. С.152-153.
6. Котенко И.В., Степашкин М.В. Мониторинг работы пользователей в компьютерных сетях // IX Санкт-Петербургская Международная Конференция “Региональная информатика-2004” (“РИ-2004”). Материалы конференции. СПб., 2004. С.136-137.
7. Котенко И.В., Степашкин М.В. Обманные системы для защиты информационных ресурсов в компьютерных сетях // Труды СПИИРАН, Вып.2. СПб: СПИИРАН, 2004. С.211-230.
8. Gorodetski V., Karsayev O., Kotenko I., Samoilov V. Multi-Agent Information Fusion: Methodology, Architecture and Software Tool for Learning of Object and Situation Assessment // The 7th International Conference on Information Fusion. Proceedings. Stockholm, Sweden. June 28 - July 1, 2004. P.346-353.
9. Laskov P., Schafer C., Kotenko I. Intrusion detection in unlabeled data with one-class Support Vector Machines // Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2004), Lecture Notes in Informatics (LNI), No. 46, Dortmund, Germany, July 2004. P.71-82.
10. Котенко И.В., Степашкин М.В. Интеллектуальные обманные системы для защиты информации в компьютерных сетях // Труды Международных научно-технических конференций “Интеллектуальные системы (IEEE AIS'04)” и “Интеллектуальные САПР (CAD-2004)”. М.: Изд-во Физико-математической литературы, 2004. С.204-209.
11. Котенко И.В. Распознавание планов агентов-хакеров при обнаружении компьютерных атак // Труды Международных научно-технических конференций “Интеллектуальные системы (IEEE AIS'04)” и “Интеллектуальные САПР (CAD-2004)”. М.: Изд-во Физико-математической литературы, 2004. С.198-204.
12. Kotenko I., Tishkov A., Tishkova M. The event calculus implementation using ILOG JRules for security policy verification // 9-th International Workshop SPEECH AND COMPUTER (SPECOM'2004) 20-22 September 2004, St. Petersburg, Russia. 2004. P.630-633.
13. Котенко И.В. Многоагентные технологии для анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Новости искусственного интеллекта, № 1, 2004. С.56-72.
14. Kotenko I.V. Modeling and Simulation of Attacks for Verification of Security Policy and Vulnerability Assessment // Seventh International Symposium on Recent Advances in Intrusion Detection. RAID 2004. Abstract and Poster sessions. Sophia-Antipolis, French Riviera, France, September 15-17, 2004.
15. Котенко И.В. Многоагентное моделирование атак “Распределенный отказ в обслуживании” // КИИ-2004. IX Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. Том 2. М.: Физматлит, 2004. С.723-731.
16. Gorodetsky V., Kotenko I. Scenarios Knowledge base: A Formal Framework for Proactive Coordination of Coalition Operations // Knowledge Systems for Coalition Operation. M.Pechoucek, A.Tate (eds.). Third International Conference on Knowledge Systems for Coalition Operations (KSCO-2004). Pensacola, Florida. 2004. P.83-97.
17. Тишков А.В., Котенко И.В. Система верификации политик безопасности в защищенных вычислительных сетях // Методы и технические средства обеспечения безопасности информации. Материалы XII Общероссийской научно-технической конференции. 4-5 октября 2004 года. Санкт-Петербург. Издательство Политехнического университета. 2004. С.129.

18. Котенко И.В., Степашкин М.В., Михайлов Д.Ю. Система сбора анализа и хранения данных аудита работы пользователей // Методы и технические средства обеспечения безопасности информации. Материалы XII Общероссийской научно-технической конференции. 4-5 октября 2004 года. Санкт-Петербург. Издательство Политехнического университета. 2004. С.124.
19. Котенко И.В., Степашкин М.В. Распознавание целей и планов злоумышленников при обнаружении компьютерных атак // Методы и технические средства обеспечения безопасности информации. Материалы XII Общероссийской научно-технической конференции. 4-5 октября 2004 года. Санкт-Петербург. Издательство Политехнического университета. 2004. С.97.
20. Уланов А.В., Котенко И.В. Модели DDoS атак и механизмов защиты от них // Методы и технические средства обеспечения безопасности информации. Материалы XII Общероссийской научно-технической конференции. 4-5 октября 2004 года. Санкт-Петербург. Издательство Политехнического университета. 2004. С.106.
21. Котенко И.В. Многоагентные модели противоборства злоумышленников и систем защиты в сети Интернет // Третья Общероссийская Конференция «Математика и безопасность информационных технологий» (МаБИТ-04). Москва, МГУ, 2004.
22. Тишков А.В., Котенко И.В. Спецификация и верификация политик безопасности защищенной вычислительной сети: использование исчисления событий // Третья Общероссийская Конференция «Математика и безопасность информационных технологий» (МаБИТ-04). Москва, МГУ, 2004.
23. Laskov P., Schafer C., Kotenko I., Muller K.-R. Intrusion detection in unlabeled data with quarter-sphere Support Vector Machines // PIK (Praxis der Informationsverarbeitung und Kommunikation), No. 4/04 (27). Germany. 2004. P.228-236.

24. В.Городецкий, И.Котенко. Концептуальные основы стохастического моделирования в среде Интернет // Труды института системного анализа РАН, том 9: Фундаментальные основы информационных технологий и систем. Под ред. С.В.Емельянова. URSS, Москва, 2005, С.168–185.
25. Котенко И. В. Многоагентные модели противоборства злоумышленников и систем защиты в сети Интернет // Математика и безопасность информационных технологий. Материалы конференции в МГУ. М.: МЦНМО, 2005, С.257-265.
26. Тишков А.В., Котенко И.В. Спецификация и верификация политик безопасности защищенной вычислительной сети: использование исчисления событий // Математика и безопасность информационных технологий. Материалы конференции в МГУ. М.: МЦНМО, 2005, С.279-283.
27. Котенко И.В. Модели противоборства команд агентов по реализации и защите от распределенных атак “Отказ в обслуживании” // Интеллектуальные системы. Коллективная монография. / Под редакцией В.М. Курейчика. М.: Физматлит, 2005. С.181-188.
28. Котенко И.В., Нестеров С.А. О подходе к развитию функциональности сетевых сканеров безопасности // XII Всероссийская научная конференция “Проблемы информационной безопасности в системе высшей школы”. 26 января 2005 г. Сборник научных трудов. Москва: МИФИ, 2005. С.115-116.
29. Котенко И.В., Михайлов Д.Ю. Многоагентные технологии в задачах автоматизированного мониторинга информационно-вычислительных систем предприятий промышленности // Наука и технологии в промышленности. №.1, 2005.
30. Kotenko I. Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet // 19th European Simulation Multiconference “Simulation in wider Europe”. ESM’05. Riga, Latvia, 1–4 June 2005. P.533-543.
31. Kotenko I., Ulanov A. Multiagent modeling and simulation of agents’ competition for network resources availability // The Fourth International Conference on Autonomous Agents and Multi-Agent Systems. Second International Workshop on Safety and Security in Multiagent Systems (SASEMAS '05). Utrecht, The Netherlands. 2005. P. 27-43.
32. Котенко И.В., Степашкин М.В. Использование ложных информационных систем для защиты информационных ресурсов компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2005, №. 1, С.63-73.
33. И.В.Котенко, А.В.Уланов. Атака «Распределенный отказ в обслуживании» как пример командной работы интеллектуальных агентов. // Математика в вузе. Материалы XVIII международной научно-методической конференции. 2005. С.120-122.
34. Юсупов Р.М., Котенко И.В. Безопасность компьютерных сетей и систем: состояние и перспективные направления научных исследований // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.90-91.

35. Тишков А.В., Котенко И.В. Многомодульная архитектура верификатора политик безопасности // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.79-80.
36. Котенко И.В., Степашкин М.В. Имитационные модели оценки уровня защищенности информационных систем на этапе их проектирования // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.63-64.
37. Степашкин М.В., Котенко И.В. Стенд проверки решений по защите информации в компьютерных сетях // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.77-78.
38. Уланов А.В., Котенко И.В. Моделирование противостояния атакам DDOS на основе командной работы интеллектуальных агентов // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.81-82.
39. Котенко И.В., Уланов А.В. Агентно-ориентированное моделирование процессов защиты информации: противоборство агентов за доступность ресурсов компьютерных сетей // Труды Международных научно-технических конференций “Интеллектуальные системы (AIS'05)” и “Интеллектуальные САПР (CAD-2005)”. М.: Физматлит, 2005. Т.1. С.296-301.
40. Котенко И.В., Степашкин М.В. Интеллектуальная система анализа защищенности компьютерных сетей на различных этапах жизненного цикла // Труды Международных научно-технических конференций “Интеллектуальные системы (AIS'05)” и “Интеллектуальные САПР (CAD-2005)”. М.: Физматлит, 2005. Т.1. С.231-237.
41. Kotenko I., Ulanov A. Teamwork Approach for Modeling and Simulation of DDOS attacks in Internet // 6th Workshop on Agent-Based Simulation. ABS6. Erlangen. Germany. September 12 - 15, 2005. P.28-33.
42. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science, Springer-Verlag, V.3685. The Third International Workshop "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-05). September 24-28, 2005, St. Petersburg, Russia. P. 317-330.
43. Tishkov A., Kotenko I. Security Checker Architecture for Policy-based Security Management // Lecture Notes in Computer Science, Springer-Verlag, V.3685. The Third International Workshop "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-05). September 24-28, 2005, St. Petersburg, Russia. P. 469-474.
44. Богданов В.С., Котенко И.В., Степашкин М.В. Активный анализ защищенности компьютерных сетей // Методы и технические средства обеспечения безопасности информации. Материалы XIV Общероссийской научно-технической конференции. 4-6 октября 2005 года. Санкт-Петербург. Издательство Политехнического университета. 2005. С.95.
45. Котенко И.В., Уланов А.В. Программная среда для моделирования механизмов защиты от распределенных атак “Отказ в обслуживании” // Методы и технические средства обеспечения безопасности информации. Материалы XIV Общероссийской научно-технической конференции. 4-6 октября 2005 года. Санкт-Петербург. Издательство Политехнического университета. 2005. С.96.
46. Степашкин М.В., Богданов В.С., Котенко И.В. Подсистема пассивного анализа защищенности компьютерных сетей // Методы и технические средства обеспечения безопасности информации. Материалы XIV Общероссийской научно-технической конференции. 4-6 октября 2005 года. Санкт-Петербург. Издательство Политехнического университета. 2005. С.100.
47. Тишков А.В., Котенко И.В. Верификация политик безопасности в компьютерных системах // Методы и технические средства обеспечения безопасности информации. Материалы XIV Общероссийской научно-технической конференции. 4-6 октября 2005 года. Санкт-Петербург. Издательство Политехнического университета. 2005. С.101.
48. Степашкин М.В., Котенко И.В., Богданов В.С. Имитация атак для активного анализа уязвимостей компьютерных сетей // Вторая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика». ИММОД-2005. Сборник докладов. Том 1. Санкт-Петербург, 19-21 октября 2005 г. С.269-273.
49. Котенко И.В., Уланов А.В. Многоагентная среда моделирования механизмов защиты от распределенных компьютерных атак // Вторая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика». ИММОД-2005. Сборник докладов. Том 1. Санкт-Петербург, 19-21 октября 2005 г. С.220-224.

50. Черватюк О.В., Тишков А.В., Котенко И.В. Верификация на модели в задаче динамического обнаружения конфликтов в политике безопасности компьютерных сетей // Вторая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика». ИММОД-2005. Сборник докладов. Том 1. Санкт-Петербург, 19-21 октября 2005 г. С.283-287.
51. Kotenko I.V., Ulanov A.V. Agent-based simulation of DDOS attacks and defense mechanisms // Journal of Computing, Vol. 4, Issue 2, 2005. P.113-123.
52. Gorodetski V., Kotenko I., Skormin V. (Editors). Computer Network Security. Lecture Notes in Computer Science, Vol.3685, Springer Verlag, 2005.
53. Котенко И.В., Тишков А.В., Лакомов Д.П., Черватюк О.В., Сидельникова Е.В. Проверка правильности политик безопасности // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Труды конференции. Санкт-Петербург. 2005.
54. Котенко И.В., Степашкин М.В., Богданов В.С. Модель атак для имитации действий злоумышленника в системе анализа защищенности компьютерных сетей // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Труды конференции. Санкт-Петербург. 2005.
55. Котенко И.В., Юсупов Р.М. Компьютерная безопасность: перспективные направления исследований СПИИРАН // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Труды конференции. Санкт-Петербург. 2005.
56. Kotenko I. Multi-agent modeling and simulation of computer network security processes: “a game of network cats and mice” // NATO Advanced Study Institute (ASI). “Network Security and Intrusion Detection”. 1-12 October 2005. Nork, Yerevan, Armenia, IOS Press. 2005.
57. Лакомов Д.П., Скрипник А.А. Формализация политик безопасности компьютерной системы средствами CIM // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.64-65.
58. Прието-Иларион Б.Л., Смирнов Б.В. Использование формата MOF для представления топологии и процессов в системе безопасности вычислительной сети // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.72-73.
59. Резник С.А., Тишков А.В. Подход к обнаружению и разрешению конфликтов в системах безопасности, основанных на политиках // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.73-74.
60. Сидельникова Е.В. Использование исчисления событий и абдуктивного вывода при анализе защищенности вычислительной сети // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.76.
61. Степашкин М.В. Метрики для оценки уровня защищенности компьютерных систем на этапе их проектирования // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.77.
62. Уланов А.В. Использование симуляторов компьютерной сети в задачах моделирования процессов защиты информации // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.80-81.
63. Черватюк О.В.. Методики получения XML схемы для классов CIM модели системы безопасности вычислительной сети // IV Межрегиональная конференция “Информационная безопасность регионов России” (“ИБРР-2005”). Материалы конференции. СПб, 2005. С.86-87.

64. Kotenko I.V., Ulanov A.V. The Software Environment for multi-agent Simulation of Defense Mechanisms against DDoS Attacks // Proceedings of International Conference on Intelligent Agents, Web Technologies and Internet Commerce - IAWTIC'2005. 28 - 30 November 2005, Vienna – Austria. 2005. IEEE Computer Society. 2006. P.283-288.
65. Kotenko I., Stepashkin M., Ulanov A. Agent-based modeling and simulation of malefactors' attacks against computer networks // Security and Embedded Systems. D.N.Serpanos, R.Giladi (Eds.). IOS Press. 2006. P.139-146. ISSN 1574-5589.
66. Котенко И.В., Степашкин М.В. Системы-имитаторы: назначение, функции, архитектура и подход к реализации // Изв. вузов. Приборостроение, Т.49, № 3, 2006, С.3-8.
67. Котенко И.В., Степашкин М.В., Богданов В.С. Анализ защищенности компьютерных сетей на различных этапах их жизненного цикла // Изв. вузов. Приборостроение. Т.49, № 5, 2006, С.3-8.
68. Котенко И.В., Тишков А.В., Черватюк О.В., Лакомов Д.П. Поиск конфликтов в политиках безопасности // Изв. вузов. Приборостроение, Т.49, № 11, 2006. (Принята к печати).

69. 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.49, № 11, 2006. (Принята к печати).
70. Котенко И.В., Юсупов Р.М. Перспективные направления исследований в области компьютерной безопасности // Защита информации. Инсайд, № 2, 2006. С.46-57.
71. Котенко И.В., Степашкин М.В. Метрики безопасности для оценки уровня защищенности компьютерных сетей на основе построения графов атак // Защита информации. Инсайд, № 3, 2006. С.36-45.
72. Котенко И.В., Уланов А.В. Моделирование противоборства программных агентов в Интернет: общий подход, среда моделирования и эксперименты. Часть 1 // Защита информации. Инсайд, № 4, 2006, С.44-52.
73. Котенко И.В., Уланов А.В. Моделирование противоборства программных агентов в Интернет: общий подход, среда моделирования и эксперименты. Часть 2 // Защита информации. Инсайд, № 5, 2006. С.48-56.
74. Котенко И.В., Уланов А.В. Программный полигон и эксперименты по исследованию противоборства агентов нападения и защиты в сети Интернет // Материалы международной конференции по проблемам безопасности и противодействия терроризму. М.: МЦНМО, 2006, С.78-91.
75. Котенко И.В., Тишков А.В., Черватюк О.В. Архитектура и модели для верификации политик безопасности // Материалы международной конференции по проблемам безопасности и противодействия терроризму. М.: МЦНМО, 2006, С.282-292.
76. Kotenko I.V., Ulanov A.V. Software testbed and experiments for exploring counteraction of attack and defense agents in the Internet // Proceedings of the International Security and Counteracting Terrorism Conference. Moscow. Lomonosov Moscow State University Intellectual Center. 2006. P.80-93.
77. Kotenko I.V., Tishkov A.V., Chervatuk O.V. Architecture and Models for Security Policy Verification // Proceedings of the International Security and Counteracting Terrorism Conference. Moscow. Lomonosov Moscow State University Intellectual Center. 2006. P.253-262.
78. Kotenko I., Ulanov A. Agent-based Simulation of Distributed Defense against Computer Network Attacks // Proceedings of 20th European Conference on Modelling and Simulation (ECMS 2006). Bonn. Germany. May 28th - 31st, 2006. P.560-565.
79. Kotenko I., Ulanov A. Antagonistic Agents in the Internet: Computer Network Warfare Simulation // The 9th International Conference on Information Fusion. Florence (Italy), 10-13 July, 2006.
80. Kotenko I., Stepashkin M. Analyzing network security using malefactor action graphs // IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.6, June 2006. P.226-235. ISSN: 1738-7906.
81. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006. International Conference on Security and Cryptography. Proceedings. Portugal. 7-10 August 2006. P.339-344.
82. Kotenko I., Ulanov A. Agent-based modeling and simulation of network softbots’ competition // Knowledge-Based Software Engineering. Proceedings of the Seventh Joint Conference on Knowledge-Based Software Engineering (JCKBSE'06). Tallinn, Estonia. August 28-31. 2006. IOS Press, 2006. P.243-252.
83. Kotenko I., Ulanov A. Simulation of Internet DDoS Attacks and Defense // 9th Information Security Conference. ISC 2006. Samos, Greece. August 30 - September 2, 2006. Proceedings. Lecture Notes in Computer Science, Vol. 4176, 2006. P.327-342.
84. Kotenko I., Ulanov A. Simulation Environment for Investigation of Cooperative Distributed Attacks and Defense // 9th International Symposium on Recent Advances in Intrusion Detection. RAID 2006. Abstract and Poster sessions. Hamburg, Germany September 20-22, 2006.
85. Kotenko I., Stepashkin M. Attack Graph based Evaluation of Network Security // The 10th IFIP Conference on Communications and Multimedia Security. CMS'2006. Heraklion, Greece. 19 - 21 October 2006. 2006. Proceedings. Lecture Notes in Computer Science, Vol. 4237, 2006. P.216-227.
86. Kotenko I., Ulanov A. Agent Teams in Cyberspace: Security Guards in the Global Internet // International Conference on CYBERWORLDS. CW2006. Lausanne, Switzerland, November 28-30, 2006. Proceedings. IEEE Computer Society, 2006. P.133-140.
87. Богданов В.С., Котенко И.В. Проактивный мониторинг выполнения политики безопасности компьютерных сетей // Методы и технические средства обеспечения безопасности информации. Материалы XV Общероссийской научно-технической конференции. 26-28 июня 2006 года. Санкт-Петербург. Издательство Политехнического университета. 2006. С.117.

88. Степашкин М.В., Котенко И.В. Методика анализа защищенности компьютерных сетей, основанная на моделировании действий внутренних и внешних нарушителей // Методы и технические средства обеспечения безопасности информации. Материалы XV Общероссийской научно-технической конференции. 26-28 июня 2006 года. Санкт-Петербург. Издательство Политехнического университета. 2006. С.121.
89. Котенко И.В., Тишков А.В. Подход к построению и реализация системы управления защитой информации в компьютерных сетях, основанной на политиках безопасности // Методы и технические средства обеспечения безопасности информации. Материалы XV Общероссийской научно-технической конференции. 26-28 июня 2006 года. Санкт-Петербург. Издательство Политехнического университета. 2006. С.122.
90. Котенко И.В., Уланов А.В. Исследование механизмов нападения и защиты в Интернет // Методы и технические средства обеспечения безопасности информации. Материалы XV Общероссийской научно-технической конференции. 26-28 июня 2006 года. Санкт-Петербург. Издательство Политехнического университета. 2006. С.123.
91. Котенко И.В., Степашкин М.В., Богданов В.С. Оценка уровня защищенности компьютерных сетей на основе построения графа атак // Международная Научная Школа "Моделирование и Анализ Безопасности и Риска в Сложных Системах (МА БР - 2006), Санкт-Петербург, 4-8 июля, 2006. С.150-154.
92. Уланов А.В., Котенко И.В. Исследование механизмов защиты против распределенных атак “Отказ в обслуживании” на основе многоагентного моделирования // Международная Научная Школа "Моделирование и Анализ Безопасности и Риска в Сложных Системах (МА БР - 2006), Санкт-Петербург, 4-8 июля, 2006. С.333-339.
93. Городецкий В.И., Котенко И.В., Юсупов Р.М. Защита компьютерных сетей // Вестник РАН, № 7, 2006. С.668-670. ISSN: 0869-5873.
94. Котенко И.В., Уланов А.В. Многоагентное моделирование распределенных атак “Отказ в обслуживании” // Труды СПИИРАН, Выпуск 3, Том 1. СПб.: Наука, 2006. С.105-125.
95. Котенко И.В., Степашкин М.В., Юсупов Р.М. Математические модели, методы и архитектуры для защиты компьютерных сетей: аналитический обзор перспективных направлений исследований по результатам Международного семинара МММ-ACNS-2005 // Труды СПИИРАН, Выпуск 3, Том 2. СПб.: Наука, 2006. С.11-29.
96. Котенко И.В., Степашкин М.В., Богданов В.С. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности // Труды СПИИРАН, Выпуск 3, Том 2. СПб.: Наука, 2006. С.30-49.
97. Богданов В.С., Котенко И.В. Архитектура, модели и методики функционирования системы проактивного мониторинга выполнения политики безопасности // Труды СПИИРАН, Выпуск 3, Том 2. СПб.: Наука, 2006. С.50-69.
98. Тишков А.В., Котенко И.В., Черватюк О.В., Лакомов Д.П., Резник С.А., Сидельникова Е.В. Обнаружение и разрешение конфликтов в политиках безопасности компьютерных сетей // Труды СПИИРАН, Выпуск 3, Том 2. СПб.: Наука, 2006. С.102-114.
99. Тишков А.В., Черватюк О.В., Лакомов Д.П., Резник С.А., Сидельникова Е.В. Обнаружение и разрешение противоречий в спецификациях сложных систем // КИИ-2006. X Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. Том 1. М.: Физматлит, 2006. С.87-90. ISBN: 5-9221-0757-7.
100. Степашкин М.В., Котенко И.В., Богданов В.С. Интеллектуальная система анализа защищенности компьютерных сетей // КИИ-2006. X Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. Том 1. М.: Физматлит, 2006. С.149-157.
101. Котенко И.В., Степашкин М.В. Модели действий хакеров-злоумышленников при реализации распределенных многошаговых атак // КИИ-2006. X Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. Том 2. М.: Физматлит, 2006. С.617-625.
102. Котенко И.В., Уланов А.В. Агентно-ориентированное моделирование поведения сложных систем в среде Интернет // КИИ-2006. X Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. Том 2. М.: Физматлит, 2006. С.660-668.
103. Уланов А.В., Котенко И.В. Система многоагентного моделирования механизмов защиты компьютерных сетей // КИИ-2006. X Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. Том 3. М.: Физматлит, 2006. С.867-876.
104. Котенко И.В., Уланов А.В. Кооперативная работа команд агентов при защите от сетевых атак нарушения доступности // Труды Международных научно-технических конференций

“Интеллектуальные системы (AIS'06)” и “Интеллектуальные САПР (CAD-2006)”. М.: Физматлит, 2006. С.306-313.
105. Богданов В.С., Котенко И.В. Анализ выполнения политики безопасности в компьютерных сетях: проактивный подход // Труды Международных научно-технических конференций “Интеллектуальные системы (AIS'06)” и “Интеллектуальные САПР (CAD-2006)”. М.: Физматлит, 2006. С.313-320.
106. Котенко И.В., Степашкин М.В., Богданов В.С. Модели и методика интеллектуальной оценки уровня защищенности компьютерных сетей // Труды Международных научно-технических конференций “Интеллектуальные системы (AIS'06)” и “Интеллектуальные САПР (CAD-2006)”. М.: Физматлит, 2006. С.321-328.
107. Котенко И.В., Уланов А.В. Команды агентов в кибер-пространстве: моделирование процессов защиты информации в глобальном Интернете // Проблемы управления кибербезопасностью информационного общества. Сборник Института системного анализа РАН, URSS, Москва, 2006. (Принята к печати).
108. Котенко И.В., Уланов А.В. Моделирование игры в “сетевые кошки-мышки”: многоагентные технологии для исследования киберпротивоборства между антагонистическими командами кибер-агентов в Интернет // Новости искусственного интеллекта, № 3, 2006. (Принята к печати).
109. Котенко И.В., Степашкин М.В., Богданов В.С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006, №. 2. (Принята к печати).
110. Воронцов В. В., Котенко И.В. Исследование подходов к автоматическому обнаружению и предотвращению вирусных атак на основе комбинированных механизмов ограничения сетевого трафика // X Санкт-Петербургская Международная Конференция “Региональная информатика-2006” (“РИ-2006”). Материалы конференции. СПб., 2006. С.105-106.
111. Десницкий В.А., Котенко И.В. Защита программного обеспечения от взлома: анализ методов // X Санкт-Петербургская Международная Конференция “Региональная информатика-2006” (“РИ-2006”). Материалы конференции. СПб., 2006. С.108-109.
112. Котенко И.В., Юсупов Р.М. Основные направления научных исследований в области защиты компьютерных сетей и систем // X Санкт-Петербургская Международная Конференция “Региональная информатика-2006” (“РИ-2006”). Материалы конференции. СПб., 2006. (Принята к печати).
113. Котенко И.В., Уланов А.В. Противостояние в Интернет: моделирование противодействия распределенным кибератакам // Пятая Общероссийская Конференция «Математика и безопасность информационных технологий» (МаБИТ-06). Москва, МГУ, 2006. (Принята к печати).
114. Богданов В.С., Котенко И.В., Степашкин М.В. Проактивный подход к мониторингу выполнения политики безопасности компьютерных сетей // Пятая Общероссийская Конференция «Математика и безопасность информационных технологий» (МаБИТ-06). Москва, МГУ, 2006. (Принята к печати).
115. Тишков А.В., Котенко И.В., Сидельникова Е.В., Черватюк О.В. Обнаружение и разрешение противоречий в политиках безопасности // Пятая Общероссийская Конференция «Математика и безопасность информационных технологий» (МаБИТ-06). Москва, МГУ, 2006. (Принята к печати).
116. Степашкин М.В., Котенко И.В., Богданов В.С. Оценка защищенности компьютерных сетей на основе анализа графов атак // Пятая Общероссийская Конференция «Математика и безопасность информационных технологий» (МаБИТ-06). Москва, МГУ, 2006. (Принята к печати).