Title of the Project:
"Modeling of information security processes in computer networks in adversarial environment: formal framework, mathematical models, multi-agent architecture, software prototype and experimental evaluation". Project from Russian Foundation of Basic Research, № 04-01-00167, 2004-2006.

Principal Investigator: Igor Kotenko

Short annotation:

The formal problem statement and the conceptual model of antagonistic cybernetic counteraction of malefactors and computer network security components based on agent-technologies were specified more exactly.

For investigative simulation it was offered to use the family of various models - analytical, hybrid, imitational (at a level of network packages), scaled-down and actual testing.

The specified conceptual model of this cybernetic counteraction includes:

(1) the ontology of information security application containing a set of application concepts and relations between them;

(2) the protocols of teamwork for agents from various teams (teams of malefactors and (components of) information security system;

(3) the models of individual, group and team behaviour of agents within the framework of particular intentions implemented by different scripts of agents actions;

(4) communication component, intended for message exchange between agents;

(5) the models of environment (the computer network), including topological and functional components.

The fragment of ontology based distributed knowledge base for simulation of computer counteraction (on an example of realizing "Distributed Denial of Service" attacks and mechanisms of protection against them) was elaborated.

The formal models for teamwork of agents-malefactors and security agents based on a hybrid approach to teamwork realization were specified and modified.

The formal models of a computer network under defense were advanced.

The multiagent architecture of the system for simulating computer counteraction of teams of agents-malefactors and security agents (on an example of realizing "Distributed Denial of Service" attacks and mechanisms of protection against them) were developed.

On the basis of INET Framework the research prototype for packet based simulation of "Distributed Denial of Service" attacks and protection mechanisms against them was implemented. At designing and realization of agents the following elements of the FIPA (Foundation for Intelligent Physical Agents) abstract architecture were used: Agent Communication Language (ACL), message-transport-service, service directory, agent directory.

On an example of realizing "Distributed Denial of Service" attacks and mechanisms of protection against them, the experiments on imitation of counteraction of agents' teams in the Internet have been fulfilled. The experiments have been realized for various scripts of attacks and protection mechanisms, for networks with diverse structures and different 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.

The models of deception information systems were elaborated more exactly. These systems represent hardware-software information safety tools based on technology of “traps” and false objects.

The models, techniques and prototypes for active security analysis of computer networks (based on automatic generation and fulfillment of distributed attack scripts) were elaborated. 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 of security policies for computer networks are developed.

Название проекта:
“Моделирование процессов защиты информации в компьютерных сетях в антагонистической среде: формальный подход, математические модели, многоагентная архитектура, программный прототип и экспериментальная оценка”. Грант РФФИ № 04-01-00167, 2004-2006.

Ф.И.О. руководителя проекта: Котенко Игорь Витальевич

Краткая аннотация на русском языке:

Уточнены постановка задачи и концептуальная модель реализации антагонистических процессов противоборства злоумышленников и компонентов защиты компьютерных сетей, основанной на агентских технологиях.

Для исследовательского моделирования предложено использовать семейство различных моделей (аналитических, гибридных, имитационных на уровне сетевых пакетов, полунатурных и натурных).

Уточненная 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 индивидуального, группового и общекомандного поведения агентов в рамках конкретных намерений, реализуемых сценариями действий агентов;

(4) коммуникационную компоненту, предназначенную для обмена сообщениями между агентами;

(5) модели среды функционирования – компьютерной сети, включающие топологический и функциональные компоненты.

Доработан 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).

Уточнены и доработаны формальные модели командной работы агентов-злоумышленников и агентов защиты, основанных на гибридном подходе к реализации командной работы агентов.

Переработаны формальные модели защищаемой компьютерной сети.

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).

На основе INET Framework разработан исследовательский прототип моделирования распределенных атак “Отказ в обслуживании” и механизмов защиты от них, базирующийся на имитации на уровне сетевых пакетов. При проектировании и реализации агентов были использованы следующие элементы абстрактной архитектуры FIPA (Foundation for Intelligent Physical Agents): язык коммуникаций, транспортный и сетевой уровни, каталог агентов.

На примере моделирования процессов реализации распределенных атак “отказ в обслуживании” и механизмов защиты от них проведен ряд 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. Проведенные эксперименты показали возможность использования предлагаемого подхода для моделирования перспективных механизмов защиты и анализа защищенности проектируемых сетей.

Детализированы модели функционирования ложных (обманных) информационных систем, представляющих собой программно-аппаратные средства обеспечения информационной безопасности, основанные на технологии “ловушек” и ложных целей.

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.

Разработана обобщенная архитектура, отдельные модели и прототипы компонентов верификации политик безопасности компьютерных сетей.

Развернутый научный отчет:

Задача проекта формулируется 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 планируется осуществить на основе исследовательского компьютерного многоагентного моделирования указанного противоборства. Основной результат проекта – создание интегрированного подхода к построению систем защиты информации, действующих в агрессивном антагонистическом окружении.

При выполнении проекта предполагается:

(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.

Основной целью исследований, запланированных на 2005 год, являлось продолжение начатых в предыдущем году работ по разработке и прототипированию формальных моделей процессов защиты информации в компьютерных сетях, рассматриваемых в виде антагонистического взаимодействия злоумышленников и компонентов систем защиты информации компьютерных сетей (на примере реализации распределенных атак “Отказ в обслуживании” и механизмов защиты от них).

Конкретные задачи, запланированные на 2005 год, были таковы:

1. Уточнение и детализация постановки задачи и концептуальной модели реализации антагонистических процессов противоборства злоумышленников и компонентов защиты компьютерных сетей, основанной на агентских технологиях.

2. Разработка основанной на онтологии, распределенной базы знаний для моделирования процессов компьютерного противоборства (на примере реализации распределенных атак “Отказ в обслуживании” и механизмов защиты от них).

3. Уточнение и разработка формальных моделей и программных прототипов командной работы агентов-злоумышленников и агентов защиты, основанных на гибридном подходе к реализации командной работы агентов и перспективных механизмах защиты информации в компьютерных сетях.

Все задачи, запланированные в проекте на 2005 год, выполнены. Решен также ряд дополнительных задач, в том числе разработка моделей компонентов ложных информационных систем и обмана злоумышленников, разработка моделей и методов анализа уязвимостей, распознавания планов агентов-хакеров, спецификации и верификации политик безопасности компьютерных сетей, а также мониторинга их выполнения. Все полученные результаты предполагается использовать при многоагентном моделировании процессов защиты информации в компьютерных сетях.

Важнейшие результаты, полученные за отчетный период, таковы:

1. Уточнены 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 уделяется 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).

Уточненная 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. Доработан 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. Уточнены и доработаны 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). Переработаны 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 (“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.

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.

5. Разработан исследовательский прототип моделирования распределенных атак “отказ в обслуживании”.

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.

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.

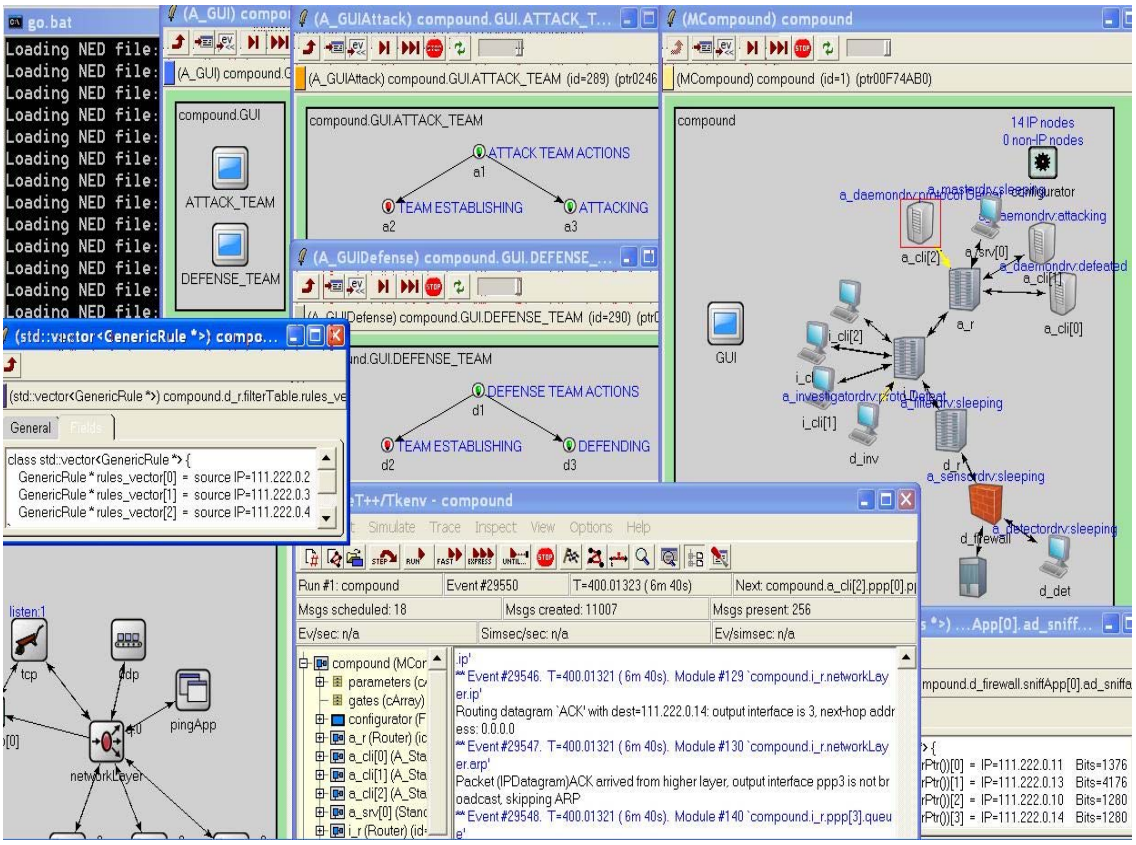

Рис.1. Пример пользовательского интерфейса среды моделирования

Пример пользовательского интерфейса среды моделирования показан на рис.1. На основном окне визуализации (рис.1, справа вверху) отображается компьютерная сеть для проведения моделирования. Окно управления процессом моделирования (рис.1, внизу посередине) позволяет просматривать и менять параметры моделирования. 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 (внизу слева) отображено окно функционирования одного из хостов.

Основное окно, на котором отображается компьютерная сеть для проведения моделирования, показано на рис.2. Исследуемая компьютерная сеть представляет собой набор узлов, соединенных каналами связи. Узлы могут нести различную функциональность в зависимости от их параметров или набора внутренних модулей.

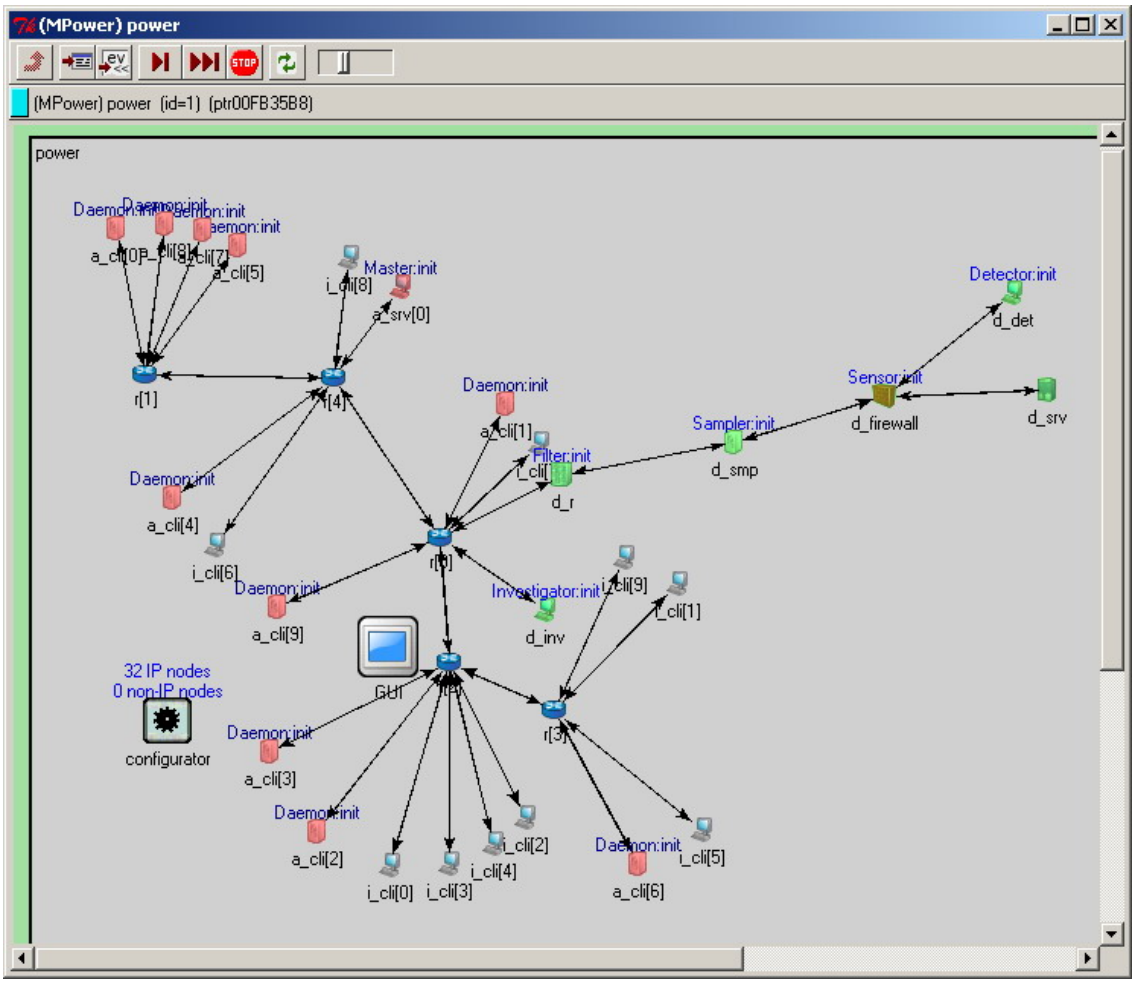

Рис.2. Пример компьютерной сети для проведения моделирования

6. На примере моделирования процессов реализации распределенных атак “отказ в обслуживании” и механизмов защиты от них проведен ряд 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. 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). Реализованы исследовательские прототипы менеджера верификации, управляющего процессом верификации, и трех модулей верификации: основанного на исчислении событий; базирующегося на технике проверки на модели (model checking); и использующего построение полурешеток действий.

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 делается 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.

Все результаты, полученные в процессе выполнения проекта в 2005 году, соответствуют мировому уровню. Авторы проекта апробировали и опубликовали в 2005 году 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.) и др.

В качестве начального 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).