1 Название проекта/ Номер годового отчета

Проект 1994Р: Формальные методы защиты информации в компьютерных сетях

Задача 1: Разработка математической модели, архитектуры и программного прототипа системы моделирования удаленных атак на компьютерные сети.
Отчет №3

2. Головной институт

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

3. Институты-участники

Нет

4. Руководитель , номер телефона, факса, адрес электронной почты

Котенко Игорь Витальевич, (812)-323-3570, (812)-328-0685, ivkote@iias.spb.su

5. Дата начала осуществления, продолжительность проекта

1 декабря 2000, 27 месяцев

6. Краткое описание плана работ: цель, предполагаемые результаты, научно-технический подход

Краткий план работ

А-1. Разработка концептуальных описаний представительного множества распределенных атак на макро уровне и их моделей.	1-3 кварталы
Промежуточный отчет #1, представляющий результаты исследований по задаче А-1.	3 квартал
А-2. Разработка формальных моделей сетевых атак.	2-3 кварталы
Промежуточный отчет #2, представляющий результаты исследований по задачам А-1 и А-2.	4 квартал
А-3. Разработка объектно-ориентированного проекта программного прототипа системы “Симулятор атак”.	4-6 кварталы
Представление статьи в международный журнал.	5 квартал
Промежуточный отчет # 3, представляющий результаты исследований по задаче А-3.	6 квартал
А-4. Разработка объектно-ориентированного проекта программного прототипа системы “Симулятор сетевых атак”.	6-9 кварталы
Демонстрация программных компонент, которые будут использованы в прототипе Симулятора атак (По согласованию с US AFRL/ID.).	9 квартал
Итоговый отчет и общее заключение по задаче 1	9 квартал

Примечание: Строки таблицы, показанные серым цветом, отвечают исследованиям, запланированным на третий год работы.

Цель проекта

Целью задачи 1 проекта является разработка формальной модели и программного обеспечения для моделирования широкого спектра распределенных атак, а также исследование ее возможностей и полезности применительно к решению задач защиты компьютерных сетей.

Ожидаемые результаты

Основным ожидаемым результатом будет формальный подход, модель, архитектура и программный прототип системы моделирования атак на компьютерные сети. Детализация этих результатов может быть представлена следующим образом:

1. Спецификация представительного множества удаленных атак, основанная на сценариях;
2. Методики и алгоритмы восстановления формальных грамматик, задающих модели атак различных классов;
3. Стохастические модели фрагментов атак на микро-уровне;
4. Объектно-ориентированный проект программного прототипа системы моделирования атак;
5. Программный прототип системы моделирования атак и результаты исследования на основе компьютерного моделирования его работы с оценкой полезности его практического использования.

Научно-технический подход

Распределенная атака планируется на макро-уровне в виде частично упорядоченного множества шагов, задающих сценарий. Каждый шаг направлен на достижение частной цели и соответствует некоторой частной атаке. При реализации конкретной атаки некоторые шаги выбранного сценария могут быть успешными, а другие – нет. Эти шаги могут быть реализованы в различном порядке, многократно повторяться и выполняться с различных удаленных компьютеров. Они могут быть направлены на различные ресурсы компьютерной сети. Для реализации каждого шага сценария атаки используются операции нижнего уровня в виде последовательности команд.

В соответствии с названными особенностями приложения, используется следующий подход.

На макро-уровне используется формализация сценариев в терминах структуры формальных грамматик, связанных операцией подстановки. Каждая реализация сценария рассматривается как последовательность шагов атаки на макро уровне. Каждая такая последовательность рассматривается как “слово”, принадлежащее формальному языку, который формально задается посредством формальной грамматики. Множество “слов” такого “языка” может быть использовано для регенерации (восстановления) грамматики формальными методами. Однако в настоящее время используется экспертный метод восстановления грамматики, что обусловлено недостатком экспериментальных данных и наличием информации о структуре атак, полученной экспертным путем. Проведенный анализ и полученные результаты показывают, что адекватное описание сценариев атак может быть выполнено в терминах стохастических (атрибутных) *LL2* право-рекурсивных грамматик.

Второй уровень моделирования соответствует спецификации атак на микро уровне. Каждый шаг сценария, заданный на макро уровне, состоит из последовательности различных событий (например, системных вызовов) микро уровня. Событие в этой последовательности реализует некоторое конкретное действие или команду злоумышленника, которое в разрабатываемой модели относится к микро уровню. Моделирование этого уровня также может быть выполнено в терминах формальных грамматик с подстановкой в листьях дерева вывода последовательностей, отвечающих низкоуровневому описанию действий злоумышленника.

7. Ход выполнения технических работ за второй год

Ход выполнения работ второго года исследований полностью соответствовал плану работ, как по содержанию, так и по срокам завершения предусмотренных этапов работ.

Основные достижения за второй год исследований

Основные достижения связаны с решением запланированных задач. Эти задачи и полученные по ним результаты перечисляются ниже.

1. Разработка объектно-ориентированного проекта программного прототипа системы “Симулятор атак” (системы моделирования атак).

2. Разработка программного прототипа системы “Симулятор атак” (системы моделирования атак).

Основные результаты, полученные в течение второго года исследований, таковы.

1. *Уточнен используемый подход к моделированию атак на компьютерные сети.*

Концептуальное исследование атак позволило выявить следующие *особенности планирования и выполнения атак*, влияющие на выбор формальной модели атак и проектирование системы моделирования атак: атака направлена на конкретный объект и, как правило, имеет вполне

определенную цель; намерение атакующего может быть представлено в терминах частично упорядоченного множества намерений более низкого уровня и действий, которые могут быть реализованы различными способами; развитие атаки в значительной степени определяется реакцией атакуемой компьютерной сети, выбор продолжения атаки почти всегда недетерминирован; сценарий развития атаки не может быть задан заранее, так как любая атака зависит от множества неопределенностей: неопределенности выбора намерения атакующего и объекта атаки; неопределенности выбора сценария атаки, реализующего выбранное намерение; неопределенности реакции на атаку компьютерной сети и др. *Отличительными чертами разработанного подхода*, влияющими на выполнение объектно-ориентированного проекта системы моделирования атак, являются следующие: моделирование атаки основывается на задании намерений злоумышленника и спецификации объектов атаки; многоуровневая спецификация атаки представляется в следующей последовательности (от верхнего к нижним уровням): "задача атаки (цель) и объект атаки $\rightarrow$ структурированные намерения злоумышленников $\rightarrow$ действия злоумышленников $\rightarrow$ реакция атакуемой компьютерной сети"; структурирование модели атаки базируется на использовании онтологии предметной области; для формальной спецификации сценариев атаки и ее компонент ("простых атак") используются атрибутные стохастические *LL*(*2*) контекстно-свободные грамматики, что означает, что цепочки грамматик генерируются слева направо, сверху вниз с неопределенностью выбора подстановки для второго символа включительно; для задания многоуровневой структуры атак используются операции подстановки формальных грамматик; интерпретация формальных грамматик осуществляется на основе автоматов; генерация действий злоумышленников происходит в зависимости от реакции атакуемой сети в реальном масштабе времени.

Более точно определенная концептуальная модель атак на компьютерные сети позволила разработать объектно-ориентированный проект программного прототипа системы моделирования атак на компьютерные сети.

2. В целях разработки объектно-ориентированного проекта программного прототипа системы моделирования атак на компьютерные сети и его реализации *разработаны и использованы технология и программный инструментарий, названный Multi-agent System Development Kit (MAS DK)*. Этот инструментарий реализован на базе Visual C++ 6.0, JAVA1.3 и XML.

3. *Разработан объектно-ориентированный проект программного прототипа системы "Симулятор атак" (системы моделирования атак).*

Программный прототип системы моделирования атак реализован в виде двух взаимодействующих агентов – агента *MainHack* (агента-хакера) и агента *MainNet* (агента, задающего атакуемую компьютерную сеть).

В основу агента-хакера *MainHack* положена автоматная вероятностная модель переходов от одного атакующего действия к другому. Эта модель является интерпретацией предложенного авторами проекта подхода к генерации атак, основанного на аппарате формальных грамматик. Информационной базой агента-хакера *MainHack* является хранилище информации, полученной от агента *MainNet*.

Агент *MainNet* базируется на вероятностно-атрибутной схеме реакции на действия агента-хакера *MainHack*. В зависимости от конфигурации хоста (сети), запущенных приложений, версий и типов операционной системы, а также от настроек сетевой безопасности агент *MainNet* выдает информацию о сети (хосте) агенту-хакеру в ответ на его сообщение с той или иной вероятностью. Вероятность успеха на стороне агента *MainNet* рассчитывается только в случае удовлетворения всех условий для данного действия хакера, направленного на конкретный атакуемый хост (если целью является один хост) или совокупность хостов (если атака направлена на сеть).

Коммуникация между агентами *MainHack* и *MainNet* в программном прототипе базируется на использовании понятия "Attack" онтологии "Атаки на компьютерные сети". Всего в текущей версии программного прототипа системы моделирования атак используется 27 атрибутов атаки, в том числе и атрибуты, отражающие результат атак на DNS-сервер.

Приходящие сообщения обрабатываются с использованием соответствующих скриптов. Обработка осуществляется как на стороне агента-хакера *MainHack*, так и на стороне агента *MainNet*. При этом агент-хакер *MainHack* выполняет регистрацию выполненного действия и вычисление последующего действия. После получения входного сообщения (пакета входных сообщений) агент *MainNet* производит его обработку и формирование отклика, направляемого агенту-хакеру.

Для отдельных классов атак (а, следовательно, и сообщений) как на стороне агента-хакера *MainHack*, так и на стороне агента *MainNet* были реализованы специализированные автоматы (с именами “класс/подкласс атаки + _MSG”). Эти автоматы ответственны только за коммуникацию между агентами.

При переходе на двухагентную архитектуру прототипа обработка условий выполнения атакующих действий была исключена из скриптов агента *MainHack*. Она была реализована в отдельной программной компоненте агента *MainNet*. Таким образом, в настоящей версии прототипа при реализации атаки агент-хакер обладает только двумя типами данных об атакуемой сети: (1) спецификация цели атаки; (2) результаты предыдущих атак.

8. Ход выполнения технических работ за рассматриваемый год

Ход выполнения работ за рассматриваемый год полностью соответствует плану работ как по содержанию, так и по срокам завершения предусмотренных этапов работ.

Основные достижения за рассматриваемый год

Основные достижения за рассматриваемый год связаны с решением запланированных задач. Эти задачи и полученные по ним результаты перечисляются ниже.

1. Разработка программного прототипа системы “Симулятор атак” (системы моделирования атак).

2. Исследование разработанного прототипа системы “Симулятор атак” на основе компьютерного моделирования, оценка возможностей его использования при проектировании систем защиты.

Основные результаты, полученные в течение текущего года исследований, таковы.

1. *Модифицирован разработанный программный прототип системы “Симулятор атак”.*

Программный прототип “Симулятора атак” (системы моделирования атак на компьютерные сети) построен как многоагентная система, в которой используется два класса агентов. Агент первого класса моделирует атакуемую компьютерную сеть и систему защиты сети (агент-сеть). Агент второго типа моделирует действия хакера против компьютерной сети (агент-хакер). В разработанном прототипе каждый класс агента имеет единственный экземпляр, хотя разработанная технология позволяет моделировать действия команды хакеров и команды агентов, ответственных за защиту компьютерной сети.

Агенты реализованы на основе применения технологии, обеспечиваемой инструментарием разработки многоагентных систем Multi-Agent System Development Kit (MASDK). Это программное средство, предназначенное для поддержки проектирования и реализации широкого класса многоагентных систем. Спроектированный и реализованный Симулятор Атак включает множество повторно используемых компонент, сгенерированных посредством использования стандартных функций MASDK, а также дополнительных программных компонент, разработанных в среде MS Visual C++ 6.0 SP 5.

Каждый из агентов использует свой фрагмент общей онтологии предметной области, описанной и поддерживаемой программно средствами MASDK. Взаимодействие агентов в процессе генерации атаки происходит посредством коммуникационного компонента, проектирование и реализация которого также осуществлена с использованием MASDK.

Необходимо отметить, что предыдущая версия прототипа была реализована в виде системы, состоящей из одного агента, моделирующего действия хакера, в то время как система защиты компьютерной сети имитировалась как реактивная система в рамках этого агента. При задействовании такой архитектуры не было необходимости в использовании коммуникационного компонента агентом-хакером и системой защиты компьютерной сети. В текущей версии прототипа, коммуникационный компонент играет очень важную роль. Действительно, в этой версии базы знаний агента-сети и агента-хакера разнесены. Такое представление знаний делает возможным моделировать взаимодействия нескольких соперничающих сторон. При использовании такой архитектуры при моделировании атак для того, чтобы или получить какую-либо информацию от агента-сети (на стадии разведки) или выполнить то или иное атакующее действие (на стадии реализации угрозы), агент-хакер отправляет соответствующее сообщение агенту-сети. Агент-сеть, как и при реальном взаимодействии, анализирует полученное сообщение и формирует ответное сообщение. Это сообщение формируется на основе базы знаний агента-сети, содержащей информацию о конфигурации сети и параметрах всех хостов сети, а также данные об атаках и возможных реакциях на них хостов сети.

Ключевым компонентом обоих агентов является их ядро. Каждое ядро представляет собой модуль, написанный на языке C++ и откомпилированный в dll. Данные компоненты связывают между собой программную часть, написанную на языке C++, с компонентами, выполненными в среде MASDK. Посредством соответствующих функций ядра агент работает с фрагментом онтологии предметной области, инициализирует автоматную модель, которая в свою очередь запускает на выполнение скрипты.

В *состав агента-хакера* входят следующие основные компоненты: (1) ядро агента-хакера; (2) используемый фрагмент онтологии предметной области; (3) компонент реализации автоматных моделей; (4) компонент скриптов; (5) компонент спецификации задачи атаки; (6) вероятностная (стохастическая) модель принятия решения о дальнейших действиях; (7) компонент генерации сетевого трафика; (8) компонент визуализации хода реализации атаки.

Ядро агента хакера (Hacker.dll) содержит стандартный набор функций для работы с онтологией и автоматной моделью, а также функцию вызова программного компонента спецификации задачи атаки, функцию вычисления следующего перехода, функцию инициализации визуализации хода выполнения атаки и функцию визуализации хода генерации атаки.

Фрагмент онтологии предметной области задает набор понятий и атрибутов, используемых агентом-хакером.

Компонент реализации автоматных моделей служит для описания поведения агента-хакера, в том числе частично логики принятия решения о выборе дальнейших действий агента-хакера. Автоматная модель агента-хакера построена на базе атрибутных стохастических грамматик и представляет собой порядка 50 вложенных автоматов.

Компонент скриптов определяет множество всех скриптов, вызываемых из автоматной модели агента-хакера.

Компонент спецификации задачи атаки предназначен для обеспечения пользовательского интерфейса для задания всех необходимых параметров атаки.

Вероятностная модель принятия решения используется для определения дальнейших действий агента-хакера в процессе генерации атаки.

Компонент генерации сетевого трафика предназначен для формирования реальных сетевых пакетов для некоторых классов атак, направленных на указанные в спецификации задачи атаки хосты. Компонент инициируется посредством вызова соответствующей функции ядра из скриптов тех состояний, для которых необходимо генерировать сетевой трафик.

Компонент визуализации хода реализации атаки служит для отображения хода выполнения атаки с указанием каждого сгенерированного действия и ответной реакции на него агента-сети. Ответная реакция может быть положительной (атакующее действие реализовано частично или полностью), отрицательной (отсутствует ответное сообщение или сообщение о блокировании атаки межсетевым экраном (МЭ)).

Основными компонентами агента-сети являются: 1) ядро агента-сети; (2) используемый фрагмент онтологии предметной области; (3) компонент реализации автоматных моделей; (4) компонент скриптов; (5) компонент задания конфигурации сети; (6) компонент реализации модели МЭ; (7) компонент формирования отклика (реакции) сети на атакующее действие.

Ядро агента-сети (NetAgent.dll) содержит стандартный набор функций для работы с онтологией и автоматной моделью, а также функции вызова пользовательского интерфейса конфигурирования сети, вызова модели МЭ и формирования отклика сети на атакующее действие.

Фрагмент онтологии предметной области определяет набор понятий и атрибутов, используемых агентом-сетью.

Компонент реализации автоматных моделей служит для описания поведения агента-сети. Автоматная модель агента-сети состоит из одного автомата, который по своей функциональности является коммуникационным. Этот автомат задает действия по приему входных сообщений, их классификации, обработке и отправке ответного сообщения.

Компонент скриптов задает множество скриптов, вызываемых из автоматной модели агента-сети.

Компонент задания конфигурации сети служит для задания набора пользовательских интерфейсов, посредством которых происходит описание и настройка сети, на которую будет осуществляться генерация атак. Все те понятия и атрибуты, которые относятся к хостам и сети, в том числе понятия и атрибуты, описывающие МЭ, означиваются с использованием данного интерфейса.

Компонент реализации модели МЭ предназначен для определения отклика МЭ на генерируемые агентом-хакером действия. Каждое входное сообщение от агента-хакера, представляющее собой атакующее действие, подается на вход модели МЭ, которая закреплена за всей сетью (при имитации сетевого МЭ) и (или) атакуемым хостом (при моделировании персонального МЭ). При блокировке атаки МЭ содержание ответного сообщения, формируемого агентом-сетью, включает лишь информацию о самом факте блокировки атаки тем или иным МЭ.

Компонент формирования отклика сети служит для генерации ответной реакции сети на атакующее действие. Он вызывается посредством соответствующей функции, экспортируемой ядром агента, после успешного преодоления агентом-хакером МЭ.

2. *Выполнено основанное на компьютерном моделировании исследование разработанного прототипа системы "Симулятор атак".*

Основная цель *экспериментов*, проведенных с прототипом Симулятора атак, состояла в демонстрации работоспособности симулятора атак для различных параметров спецификации атак и конфигурации атакуемой сети. Авторами проекта ставилась цель исследования возможностей симулятора атак для реализации двух следующих задач:

(1) *проверки политики безопасности защищаемой компьютерной сети на этапах концептуального и логического проектирования системы защиты*. Эта задача может решаться путем имитационного моделирования (симуляции) атак на макро-уровне и исследования откликов модели проектируемой (анализируемой) сети;

(2) *проверки политики безопасности (в том числе уязвимостей) защищаемой реально существующей компьютерной сети*. Эта задача может решаться посредством имитации атак на микро-уровне, т.е. за счет генерации сетевого трафика, соответствующего реальной деятельности злоумышленников по реализации различных угроз безопасности.

Поэтому все проведенные эксперименты были разбиты на два класса:

(1) *Эксперименты по моделированию атак на макро-уровне*. В этих экспериментах осуществлялась генерация и исследование злонамеренных действий против модели компьютерной сети;

(2) *Эксперименты по моделированию атак на микро-уровне*. В этих экспериментах выполнялась генерация злонамеренного сетевого трафика против реальной компьютерной сети.

В экспериментах по моделированию атак на макро-уровне проводились исследования атак для всех реализуемых Симулятором атак намерений злоумышленника. Причем эксперименты осуществлялись при различных параметрах спецификации задачи атаки и конфигурации атакуемой компьютерной сети.

Кроме намерения злоумышленника, при проведении экспериментов исследовалось влияние на результативность атак следующих входных параметров:

- степень защиты сетевого и персонального МЭ,
- степень защиты атакуемого хоста (например, насколько строгим является пароль, имеет ли хост разделяемые файлы, принтеры и другие ресурсы, используются ли доверяемые хосты и др.), и
- уровень знаний злоумышленника о сети.

Для исследования возможностей Симулятора атак были выбраны следующие параметры результата реализации атаки:

- количество шагов атаки (терминальных действий на макро-уровне),
- процент намерений злоумышленника, реализованных успешно,
- процент "успешных" откликов сети на атакующие действия,
- процент блокировок МЭ атакующих действий,
- процент "неэффективных" результатов атакующих действий (когда атака не привела к ожидаемому результату).

Во всех экспериментах с Симулятором атак были получены ясно интерпретируемые результаты.

Учитывая ограниченность объема итогового отчета, представлены результаты экспериментов только для двух классов намерений, относящихся к каждому из высокоуровневых намерений *Reconnaissance* (*R*) и *Implantation and threat realization* (*I*).

Для высокоуровневого намерения *R* представлены результаты экспериментов для намерений *Identification of the host Services* (IS) и *Applications and Banners Enumeration* (ABE), а для

высокоуровневого намерения *I* – результаты экспериментов для намерений *Gaining Access to Resources* (GAR) и *Confidentiality Violation Realization or Confidentiality destruction* (CVR).

При выполнении атак, реализующих намерения *IS* и *ABE*, предполагалось, что сетевой МЭ может защищать атакуемую сеть с тремя градациями степени защиты ("Strong", "Medium" и "None"), в зависимости от полноты атак терминального уровня, которые могут быть распознаны МЭ. Для намерений *IS* и *ABE* были построены графики зависимостей параметров результата реализации атаки от степени защиты сетевого МЭ.

При выполнении атак, реализующих намерения *GAR* и *CVR*, атаки осуществлялись для следующих изменяемых условиях:

(1) для двух значений степени защиты сетевого МЭ (1 – "Strong"; 2 – "None");

(2) для двух значений степени защиты персонального МЭ (1 – "Strong"; 2 – "None");

(3) для двух значений степени защиты атакуемого хоста (1 – "Strong"; 2 – " Weak");

(4) для двух значений уровня знаний хакера о сети (1 – "Good"; 2 – "Nothing").

Для намерений *GAR* и *CVR*, были построены графики зависимостей параметров результата реализации атаки от различных значений входных параметров.

В текущей версии прототипа генерация сетевого трафика реализована только для определенных типов атак. Эти атаки выбраны из различных классов атак и намерений злоумышленника, заданных в онтологии предметной области. Авторы не ставили перед собой задачу реализации всех атакующих действий на нижнем уровне. Основной упор был сделан на разработку общего подхода к генерации сетевого трафика посредством использования прототипа Симулятора атак и оценивания его возможностей и эффективности.

Для оценки результативности прототипа Симулятора атак на микро-уровне генерировались сетевые пакеты для атак классов "*Port scanning*", "*Denial of service*", и "*Password Guessing*". Модель сети, использованная в экспериментах с Симулятором атак, соответствовала реальной компьютерной сети, на которую были направлены атаки на микро-уровне.

Основанное на имитационном моделировании экспериментальное исследование разработанного Симулятора Атак продемонстрировало его эффективность для осуществления различных сценариев атак против компьютерных сетей с различной структурой и политиками безопасности.

Кроме того, был подготовлен *итоговый отчет* по задаче 1.

9. Существующее положение дел с выполнением технических работ

Ход выполнения работ полностью соответствует предусмотренному плану и в коррекции не нуждается.

10. Сотрудничество с зарубежными партнерами

В соответствии с планом работ партнеру представлен итоговый отчет (1 марта 2003), в котором представлены соответствующие результаты исследований.

В данном отчете полученные в рамках проекта результаты были представлены в двух главах и приложениях.

Глава 1 описывает предлагаемый подход к моделированию атак на компьютерные сети, разработанную технологию и программный инструментарий для проектирования и реализации основанных на знаниях многоагентных систем, объектно-ориентированный проект Симулятора Атак, а также содержит обзор релевантных исследований.

В главе 2 представлены результаты исследований по задаче А-4. В главе описывается архитектура и основные компоненты прототипа Симулятора Атак, а также его функциональные возможности и специфические особенности реализации. В главе также представлены результаты основанного на имитационном моделировании экспериментального исследования разработанного Симулятора Атак.

11. Выявленные проблемы и предложения относительно их устранения

Нет

12. Перспективы дальнейшего развития разработанной технологии/научного исследования

Перспективы дальнейшего сотрудничества будут обсуждаться на встрече с представителями Партнера и Министерства обороны США ориентировочно в апреле 2003. Предложения по дальнейшему сотрудничеству были представлены Партнеру в сентябре 2002.

Приложение 1. Наглядные материалы, прилагаемые к основному тексту

Нет

Приложение 2. Другая дополнительная информация к основному тексту

Краткое содержание *итогового отчета*, представленного партнеру

Приложение 3. Резюме статей и докладов, опубликованных за рассматриваемый год

1. Городецкий В.И., Котенко И.В., Карсаев О.В. Многоагентные технологии для обеспечения безопасности компьютерных сетей: имитация атак, обнаружение вторжений и обучение обнаружению вторжений. International Journal of Computer Systems Science and Engineering. vol.18, No.4, July 2003, pp.191-200.

   Abstract. В статье представлен опыт применения многоагентной технологии для проектирования и реализации многоагентных систем (МАС), предназначенных для кооперативного решения наиболее актуальных в настоящее время задач в области защиты компьютерных сетей. Рассматриваемые МАС – это базирующийся на агентах Симулятор атак против компьютерных сетей, многоагентная система обнаружения вторжений и многоагентная система обучения обнаружению вторжений. Каждая из этих МАС базируется на строгих формальных подходах, предложенных авторами, создана и реализована в виде программных прототипов на основе типовой агентской технологии, поддерживаемой инструментарием разработки МАС (MASDK), разработанным с участием авторов. В статье описаны перечисленные МАС и проведен анализ преимуществ применения многоагентных технологий для решения проблем защиты информации в компьютерных сетях.

2. Котенко И.В., Маньков Е.В. Агентно-ориентированное моделирование атак на компьютерные сети. Proceedings of Fourth International Workshop “Agent-Based Simulation 4 (ABS 4)”. Jean-Pierre Muller, Martina-M.Seidel (Editors). April 28-3. Montpellier, France, 2003, pp.121-126.

   Abstract. В статье представлен базирующийся на агентских технологиях подход и программная система (Симулятор атак), предназначенные для моделирования удаленных атак на компьютерные сети и активной оценки уязвимостей защиты компьютерных сетей. Предложенный подход реализуется за счет автоматической имитации распределенных хакерских атак различной сложности. Модель атак рассматривается как сложный процесс противоборства антагонистических объектов (команд злоумышленников) и системы защиты сети. Разработанный базирующийся на агентских технологиях Симулятор атак построен на

основе моделирования намерений злоумышленника, структурирования атак на основе онтологии, использования атрибутной стохастической грамматики для спецификации сценариев атак, ее интерпретации, базирующейся на конечных автоматах, и генерации в реальном времени действий злоумышленника, как отклика на реакцию атакованной системы защиты.

3. I. Kotenko. Командная работа хакеров: Формальное описание и компьютерное моделирование координированных распределенных атак на компьютерные сети. Proceedings of The 3rd International/Central and Eastern European Conference on Multi-Agent Systems (CEEMAS 2003). Prague, Czech Republic. June 16 – 18, 2003. "Multi-Agent Systems and Applications III". V.Marik, J.Muller, M.Pechoucek (Editors), Lecture Notes in Artificial Intelligence, Springer-Verlag, vol.2691, pp.464-474.

   Abstract. В статье рассматривается подход к реализации командной работы агентов. Этот подход описывается на примере моделирования скоординированных распределенных атак на компьютерные сети, выполняемых группой агентов-хакеров. Подход основан на базовых положениях теории “совместных намерений” и теории “общих планов”. Предлагаемая технология создания команды агентов включает следующие стадии: (1) формирование онтологии предметной области; (2) определение структуры команды агентов и механизмов их взаимодействия и координации; (3) спецификация планов действий агентов как иерархии атрибутных стохастических формальных грамматик; (4) назначение ролей и распределение планов между агентами; (5) автоматная интерпретация командной работы агентов-хакеров. Рассматриваются стадии создания онтологии, спецификации планов агентов и автоматной интерпретации генерации атаки. Описывается программный прототип Симулятора атак и результаты его оценки.

4. В.И.Городецкий, И.В.Котенко, Б.Дж.Майкл. Многоагентное моделирование распределенных атак “Отказ в обслуживании” на компьютерные сети. Proceedings of Third International Conference “NAVY AND SHIPBUILDING NOWADAYS” (NSN’2003). St. Petersburg, Russia, June 26 – 28, 2003, pp.38-47.

   Abstract. Переход к реализации военно-морских операций, базирующихся на современной парадигме использования информационно-телекоммуникационного пространства, имеет несомненное преимущество, связанное с применением распределенной компьютерной обработки информации для получения превосходства над противником. Однако, противник будет пытаться атаковать информационные инфраструктуры, используемые силами флотов для выполнения военно-морских операций. Одно из действенных средств, приводящих к нарушению работы этих инфраструктур, — это распределенные компьютерные атаки типа “Отказ в обслуживании” (DDoS-атаки). Основная цель таких атак состоит в нарушении или снижении возможностей доступа авторизованных пользователей к распределенным вычислительным ресурсам, а также их компрометации. Повышение живучести информационных систем и инфраструктур в условиях реализации противником таких атак требует разработки адекватного теоретического и практического фундамента. Одной из важных составляющих такого фундамента является наличие средств моделирования DDoS-атак. Формальный подход к моделированию полного спектра атак данного класса, ключевыми элементами которого является онтология DDoS-атак, механизмы командной работы программных агентов, реализующих DDoS-атаки, а также программный инструментарий для разработки многоагентных систем MASDK, используемый для построения системы моделирования атак, составляют основное содержание данной работы.

5. И.В.Котенко., Е.В.Маньков. Эксперименты по моделированию атак против компьютерных сетей. Lecture Notes in Computer Science, Springer-Verlag, vol.2776. Theory and Practice of Computer Network Security. Proceedings of the International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security, St. Petersburg, Russia, September 21–23, 2003, pp.187-198.

   Abstract. В статье описываются вопросы реализации и проведения экспериментов с программным средством “Симулятор атак”, предназначенным для активной оценки уязвимостей компьютерных сетей на стадиях проектирования и развертывания. Предложенный подход основан на моделировании намерений злоумышленника, базирующемся на онтологии структурировании атак и автоматной спецификации сценариев атак. В статье представлена обобщенная многоагентная архитектура Симулятора атак. Анализируются процессы генерации атак против модели компьютерной сети и реальной компьютерной сети. Рассматриваются эксперименты, демонстрирующие эффективность

Симулятора атак по генерации сценариев атак на компьютерные сети, имеющие различную конфигурацию и реализующие различные политики безопасности.

6. Котенко И.В., Алексеев А.С., Маньков Е.В. Формальный подход к моделированию и имитации DDoS-атак, основанный на командной работе агентов-хакеров. Proceedings of 2003 IEEE/WIC International Conference on Intelligent Agent Technology, Halifax, Canada, October 13-16, 2003, IEEE Computer Society. 2003, pp.507-510.

   Abstract. Современный Internet находится на довольно опасной стадии жизненного цикла. Принимая во внимание сегодняшний уровень защиты компьютерных сетей, Internet может просто прекратить работать, если продолжится текущая тенденция роста числа и мощности атак "Распределенный отказ в обслуживании" (DDoS) на корневые серверы. В статье обсуждается, что для защиты от DDoS-атак компьютерное сообщество должно разработать строгий теоретический фундамент, позволяющий так укрепить информационные системы и инфраструктуры, чтобы они смогли преодолевать такие атаки. Основное содержание статьи - базирующийся на агентских технологиях подход к моделированию и имитации DDoS-атак. Разработанный подход и программное средство могут использоваться для проведения экспериментов, направленных на анализ уязвимостей компьютерных сетей и оценки результативности и эффективности используемой политики безопасности.

7. Котенко И.В.. Активный анализ уязвимостей компьютерных сетей на основе имитации сложных распределенных атак. Proceedings of 2003 International Conference on Computer Networks and Mobile Computing (ICCNMC-03). Shanghai, China, October 20-23, 2003. IEEE Computer Society, 2003, pp.40-47.

   Abstract. В статье рассматривается формальный подход и программный инструмент "Симулятор атак", предназначенные для активной оценки уязвимостей реализованной политики безопасности компьютерной сети на стадиях проектирования и развертывания систем защиты компьютерных сетей. Предложенный подход основан на моделях атак, заданных на основе стохастических формальных грамматик, и реализован посредством автоматической имитации удаленных атак на компьютерные сети различной сложности. В статье охарактеризованы архитектура Симулятора атак и процессы генерации злонамеренных действий против модели компьютерной сети и реальной компьютерной сети. Детально описываются результаты экспериментов с Симулятором атак, которые демонстрируют его эффективность.