На правах рукописи

Шоров
Андрей Владимирович

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ ОТ ИНФРАСТРУКТУРНЫХ АТАК НА ОСНОВЕ ПОДХОДА «НЕРВНАЯ СИСТЕМА СЕТИ»

Специальность:
05.13.19 — Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург
2012

Работа выполнена в Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН).

Научный руководитель:
доктор технических наук,
профессор — Котенко Игорь Витальевич

Официальные оппоненты:
доктор технических наук,
профессор — Воробьев Владимир Иванович

кандидат технических наук,
доцент — Авраменко Владимир Семенович

Ведущая организация: ЗАО «Институт сетевых технологий»

Защита состоится «17» апреля 2012 г. в 13.30 на заседании диссертационного совета Д.002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук по адресу: 199178, Санкт-Петербург, В.О., 14 линия, 39.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.

Автореферат разослан «16» марта 2012 г.

Ученый секретарь
диссертационного совета Д.002.199.01
кандидат технических наук Ф.Г. Нестерук

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации.

В последнее время наблюдается тенденция к увеличению количества и мощности компьютерных атак на инфраструктуру вычислительных сетей. Мощность распределенных атак типа «отказ в обслуживании» (DDoS-атак) значительно возросла, и преодолела барьер в 100 Гб/с. Также постоянно появляется информация о различных вирусных эпидемиях, провоцируемых сетевыми червями. Сетевые черви при распространении генерируют большие объемы трафика, вследствие чего перегружают каналы связи. Не менее опасны и другие типы инфраструктурных атак на компьютерные сети, такие как атаки на DNS-серверы и атаки на маршрутизаторы.

Все это говорит о необходимости исследований в области защиты компьютерных сетей от инфраструктурных атак. Одним из перспективных подходов к защите компьютерных сетей от инфраструктурных атак представляется подход «нервная система сети», являющийся примером биоинспирированного подхода. Подход «нервная система сети» является метафорой нервной системы человека. Концепция данного подхода была предложена Ю.Ченом и Х.Ченом. Система защиты, основанная на данном подходе, базируется на распределенном механизме сбора и обработки информации, который координирует действия основных устройств компьютерной сети, идентифицирует атаки и принимает контрмеры. Подобный подход, называемый «электронной нервной системой», описывал в своих книгах Б. Гейтс, где он предлагался в качестве механизма внутренних коммуникаций и координации работы предприятия. Механизм защиты компьютерных сетей, похожий на «нервную систему сети», предлагали в своих работах Ф.Дресслер и К.Анагностакис.

Для проектирования и реализации новых систем защиты, таких как «нервная система сети», необходимо иметь средства для их исследования, адаптации, разработки и тестирования. Исследование инфраструктурных атак и механизмов защиты от них на реальных сетях достаточно сложный и труднореализуемый процесс. Для выполнения инфраструктурных атак требуется огромное количество вычислительных узлов, объединенных в сеть. При этом сами инфраструктурные атаки являются очень опасным явлением, так как в случае их выполнения вычислительная сеть может выходить из строя из-за перегрузок, что может приводить к выходу эксперимента из-под контроля и даже распространению атак вне экспериментальных машин. В таком случае невозможно соблюсти такие важные условия научного эксперимента, как контролируемость и повторяемость.

Таким образом, применение методов имитационного моделирования для исследования инфраструктурных атак и механизмов защиты от них

представляется наиболее предпочтительным решением. Имитационное моделирование предоставляет гибкий механизм моделирования сложных динамических систем, что позволяет оперировать различными наборами параметров и сценариев, затрачивая намного меньше усилий, чем в реальных сетях.

Целью исследования является повышение защищенности компьютерных сетей, обусловленное совершенствованием моделей, методик и алгоритмов исследовательского моделирования механизмов защиты от инфраструктурных атак на основе подхода «нервная система сети».

Для достижения данной цели в диссертационной работе поставлены и решены следующие задачи:

1. Анализ инфраструктурных атак на компьютерные сети, механизмов защиты от них, биоподходов для защиты компьютерных сетей, включая подход «нервная система сети», и методов их моделирования.
2. Разработка моделей, реализующих инфраструктурные атаки, механизмов защиты от них и модели механизма защиты на основе подхода «нервная система сети».
3. Разработка модели компьютерной сети.
4. Построение архитектуры системы для имитационного моделирования инфраструктурных атак и механизмов защиты от них.
5. Разработка методики имитационного моделирования инфраструктурных атак и механизмов защиты от них на основе подхода «нервная система сети» с помощью представленных моделей и архитектуры.
6. Реализация системы имитационного моделирования инфраструктурных атак и механизмов защиты от них, проведение экспериментов.
7. Оценка разработанной методики и ее сравнение с существующими.

Методы исследования: Для проведения исследований использовались следующие научные методы: системного анализа, теории вероятности, объектно-ориентированного программирования, сравнения и аналогий, имитационного моделирования.

Объект исследования: инфраструктурные атаки на компьютерные сети и механизмы защиты от них, а также процессы моделирования компьютерных сетей, инфраструктурных атак и механизмов защиты от них.

Научная задача: разработка научно-методического аппарата (комплекса моделей, методик и алгоритмов) для исследовательского моделирования механизмов защиты компьютерных сетей от инфраструктурных атак на основе реализации подхода «нервная система сети».

Предмет исследования: модели и алгоритмы механизмов защиты компьютерной сети от инфраструктурных атак, основанные на подходе «нервная система» сети и методы их моделирования.

Результаты, выносимые на защиту:

1. Имитационные модели базовых механизмов реализации инфраструктурных атак на компьютерные сети и защиты от них.
2. Комбинированная модель и алгоритмы защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети».
3. Методика имитационного моделирования механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети».
4. Архитектура и программная реализация системы имитационного моделирования инфраструктурных атак на компьютерные сети на основе подхода «нервная система сети».

Научная новизна исследования заключается в следующем:

1. Разработанные имитационные модели реализации инфраструктурных атак на компьютерные сети в отличие от известных отражают реальные механизмы распространения компьютерных червей и выполнения распределенных атак типа «отказ в обслуживании» (DDoS-атак). При этом механизмы распространения сетевых червей используют дополнительные параметры, такие как вероятность успешного соединения, методики подмены IP-адреса, использование полезной нагрузки пакета, существенно повышающих адекватность модели. Кроме того, модель DDoS-атаки имеет широкий спектр подвидов атак, в т.ч. атаки типа DRDoS, и набор параметров, повышающих точность моделирования атак. В результате имитационные модели базовых механизмов защиты охватывают распространение сетевых червей и защиты от DDoS-атаки и учитывают особенности таких механизмов как Failed Connection (FC), Virus Throttling (VT), SAVE, SIM, Hop-count filtering (HCF), SYN detection и др., а также обеспечивают совместное использование комбинации нескольких механизмов, в т.ч. под управлением механизма защиты «нервная система сети».

2. Разработанные комбинированная модель и алгоритмы защиты компьютерной сети от инфраструктурных атак на основе подхода «нервная система сети» отличаются следующими аспектами: алгоритмами сбора информации, которые используют в качестве сенсоров базовые механизмы защиты; алгоритмами принятия решений, выполняемыми на основе данных, получаемых как с удаленных серверов, так и модулей, функционирующих в одной подсети, и позволяющими отследить и блокировать атаку у ее источника; протоколом и схемой обмена информацией, дающими возможность обмениваться данными о состоянии компьютерной сети между удаленными серверами и базовыми механизмами защиты.

3. Разработанная методика имитационного моделирования механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети» основана на предложенных в данной работе моделях

и алгоритмах для задач исследования инфраструктурных атак и механизмов защиты. В отличие от известных, данная методика использует единый подход к подготовке и моделированию различных типов инфраструктурных атак и механизмов защиты, а основные этапы методики автоматизированы с помощью разработанной системы имитационного моделирования. Методика учитывает основные параметры исследуемых процессов (параметры сети и ее узлов, параметры механизмов атаки и защиты, параметры механизма защиты «нервная система сети»).

4. Разработанные архитектура и программная реализация системы имитационного моделирования инфраструктурных атак на основе подхода «нервная система сети» отличаются наличием в своем составе предложенных моделей инфраструктурных атак и механизмов защиты, возможностью выполнять моделирование инфраструктурных атак и механизмов защиты от них на моделях больших компьютерных сетей, исследовать другие механизмы защиты, основанные на биологической метафоре.

Обоснованность и достоверность представленных в диссертационной работе научных положений обеспечивается проведением тщательного анализа состояния исследований в данной области, подтверждается согласованностью теоретических результатов с результатами, полученными при компьютерной реализации, а также апробацией основных теоретических положений в печатных трудах и докладах на научных конференциях.

Практическая значимость исследования. Разработанные модели, методики и алгоритмы могут быть использованы для решения большого класса задач, в частности позволят: исследовать инфраструктурные атаки на компьютерные сети; исследовать, проектировать и тестировать механизмы защиты от инфраструктурных атак, в т.ч. основанных на биологических подходах; повысить эффективность проектирования крупных вычислительных сетей; проводить оценивание производительности построенных вычислительных сетей; выявлять узкие места построенных вычислительных сетей и выполнять их оптимизацию; оценивать устойчивость построенных вычислительных сетей для различного вида атак; вырабатывать рекомендации для построения перспективных систем защиты.

Реализация результатов работы. Результаты, полученные в диссертационной работе, были использованы в рамках следующих научно-исследовательских работ: проект Седьмой рамочной программы (FP7) Европейского Сообщества «Проектирование безопасных и энергосберегающих встроенных систем для приложений будущего Интернет (SecFutur)», контракт № 256668, 2010-2013 гг.; проект Седьмой рамочной программы (FP7) Европейского Сообщества «Управление информацией и событиями безопасности в инфраструктурах услуг (MASSIF)», контракт № 257475, 2010-2013 гг.; «Математические модели и методы комплексной

защиты от сетевых атак и вредоносного ПО в компьютерных сетях и системах, основывающиеся на гибридном многоагентном моделировании компьютерного противоборства, верифицированных адаптивных политиках безопасности и проактивном мониторинге на базе интеллектуального анализа данных», грант РФФИ № 10-01-00826-а, 2010-2012 гг.; Проект по договору с компанией F-Secure, 2010-2011 гг.; «Математические модели, методы и алгоритмы проактивной защиты от вредоносного программного обеспечения в компьютерных сетях и системах», проект по программе фундаментальных исследований ОНИТ РАН «Архитектура, системные решения, программное обеспечение, стандартизация и информационная безопасность информационно-вычислительных комплексов новых поколений», 2009-2011 гг. и др.

Апробация результатов работы. Основные положения и результаты диссертационной работы докладывались на следующих научных конференциях: Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР, Санкт-Петербург, 2009, 2011)»; XIX Общероссийская научно-техническая конференция «Методы и технические средства обеспечения безопасности информации» (МТСОБИ, Санкт-Петербург, 2010, 2011); XII Санкт-Петербургская Международная Конференция «Региональная информатика-2010» («РИ-2010»); XII Национальная конференция по искусственному интеллекту с международным участием (Тверь, 2010); Международная конференция «РусКрипто» (2009, 2010, 2011); Conference on Cyber Conflict. Tallinn, Estonia, June 15-18, 2010; 4th International Symposium on Intelligent Distributed Computing - IDC'2010 (Tangier, Morocco, 2010); Девятая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2010, Москва); V Всероссийская научно-практическая конференция «Имитационное моделирование. Теория и практика» (ИММОД, Санкт-Петербург, 2011); 16-я Международная конференция по безопасным информационным системам (NordSec, Таллинн, Эстония, 2011); Конференция «Информационная безопасность: Невский диалог – 2011» (Санкт-Петербург, 2011 г) и др.

Публикации. По материалам диссертационной работы опубликовано 33 работы, в том числе 5 статей («Вопросы защиты информации», «Системы свободной доступности», «Изв. вузов. Приборостроение», «Труды СПИИРАН») из перечня ВАК на соискание ученой степени доктора и кандидата наук.

Структура и объем диссертационной работы. Диссертационная работа объемом 196 машинописных страниц, содержит введение, три главы и заключение, список литературы, содержащий 117 наименований, 7 таблиц, 36 рисунков.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована важность и актуальность темы диссертации, определена цель диссертационной работы и сформулированы задачи, решение которых необходимо для достижения данной цели, показана научная новизна и практическая значимость работы, дано кратное описание разработанных моделей, архитектуры разработанной системы имитационного моделирования, методики моделирования инфраструктурных атак и механизмов защиты от них, а также представлены основные результаты их реализации в научно-исследовательских проектах.

В первой главе диссертации определено место и роль имитационного моделирования в задаче защиты компьютерных сетей от инфраструктурных атак, проведен анализ инфраструктурных атак и механизмов защиты от них, анализ подхода к защите компьютерных сетей на основе реализации компонентов «нервная система сети» и методов моделирования механизмов защиты, выработаны требования к имитационному моделированию механизмов защиты компьютерных сетей от инфраструктурных атак.

Рассмотрены различные методы моделирования процессов защиты информации. Выявлены их преимущества, недостатки, обозначены особенности применения того или иного метода моделирования при моделировании компьютерных сетей, механизмов атак на них и методов защиты. В соответствии со спецификой моделирования процессов защиты информации в компьютерных сетях предложено использование имитационного моделирования, как эффективного метода имитации инфраструктурных атак и механизмов защиты от них, так как данный способ моделирования позволяет создавать масштабируемые модели компьютерных сетей, обладающих необходимой степенью адекватности представления реальных объектов компьютерной сети.

Проведен анализ инфраструктурных атак. Рассмотрены их основные типы и особенности реализации. Особое внимание было уделено таким инфраструктурным атакам как распространение сетевых червей и распределенная атака типа «отказ в обслуживании», так как они являются наиболее распространенными и опасными. В качестве методов защиты от инфраструктурных атак, рассматривалось множество различных подходов, предложена их классификация. Основное внимание уделено механизму защиты компьютерных сетей на основе биологического подхода «нервная система сети». Данный подход призван объединить существующие механизмы защиты, создавая среду для кооперативного взаимодействия.

Были проанализированы существующие системы имитационного и многоагентного моделирования: NS-3, Swarm, Java Swarm, Repast, OPNET, MASON, NetLogo, OMNeT++ и др.

Кроме того в работе рассматривается процесс разработки имитационных моделей компьютерной сети, механизмов атак и защиты, методика верификации и оценки созданных моделей, а также сложности, возникающие при имитационном моделировании процессов защиты информации.

Сформулирована задача исследования. Она заключается в разработке:

(1) модели N компьютерной сети (среды взаимодействия), моделей A инфраструктурных атак (распространение червей и DDoS), моделей D соответствующих механизмов защиты от них, модели NN механизма защиты на основе подхода «нервная система сети» и алгоритмов его работы,

(2) методики M моделирования, которая позволяет анализировать механизмы защиты и определять механизмы защиты, которые наилучшим образом соответствуют предъявляемым к ним требованиям; методика моделирования должна обеспечивать выполнение требований своевременности, обоснованности и ресурсопотребления процесса моделирования.

(3) при реализации методики M моделирования модель NN механизма защиты на основе подхода «нервная система сети» и алгоритмы его работы должны позволить улучшить показатели работы базовых механизмов защиты в соответствии с требованиями к количеству ошибок первого и второго рода, а также количеству правильно детектированных пакетов.

Во второй главе представлены следующие элементы моделирования: система имитационного моделирования, модель компьютерной сети, модели базовых механизмов реализации инфраструктурных атак и защиты от них, комбинированная модель и алгоритмы защиты от инфраструктурных атак на основе подхода «нервная система сети» и модели взаимодействия атак и механизмов защиты. Структура моделей описывается с помощью теоретико-множественного подхода, а функциональная часть моделей - с помощью псевдокода. В виду ограниченности объема в автореферате все модели специфицируются только на верхнем уровне представления.

Система имитационного моделирования задается в виде $MS = \langle Sc, En, Ev, T \rangle$, где Sc — планировщик; En — сущности; Ev — события; T — время. Планировщик Sc и время T входят в состав всех моделей и используются для обеспечения процесса моделирования. Модели инфраструктурных атак и механизмов защиты отличаются заданными сущностями En, описывающими их структуру моделей и событиями Ev, которые служат для описания алгоритмов функционирования моделей. События генерируются в соответствии с законами распределения, используемых конкретными типами моделей.

Модель компьютерной сети задается в виде кортежа $N = < T, TP, TR >$, где T — тип топологии; TP — топология сети; TR — трафик в сети. Тип

топологии сети может быть задан как $T \subseteq \langle Ln, Bs, St, Rn, Tr, Mh, Hbr \rangle$, специфицируя следующие типы топологий: Ln — линия, Bs — шина, St — звезда, Rn — кольцо, Tr — дерево, Mh — решетка, Hbr — гибридная. Топология сети $TP = \langle H, L \rangle$ включает в себя: H — узлы (хосты) вычислительной сети, L — связи между узлами вычислительной сети. Трафик TR определим в виде $TR = \cup p_i^P$, где p_i — пакеты трафика, P — протокол, который используется для передачи пакета p.

Модели базовых механизмов реализации инфраструктурных атак представляются в виде $A = \langle Sc, En_A, Ev_A, T \rangle$.

Раскроем основные элементы моделей инфраструктурных атак: $En_A = \langle TA, CA \rangle$, где TA — тип инфраструктурной атаки, CA — параметры реализации атаки.

Тип инфраструктурной атаки может задаваться в следующем виде: $TA = \langle Wrm_{n,m}, DDoS_{n,m}, AoR_{n,m}, AoDNS_{n,m} \rangle$, где $Wrm_{n,m}$ — распространение сетевых червей, $DDoS_{n,m}$ — распределенная атака типа «отказ в обслуживании», $AoR_{n,m}$ — атаки на маршрутизаторы, $AoDNS_{n,m}$ — атаки на серверы DNS; переменная n служит для идентификации типа атаки на верхнем уровне представления модели (например, название типа атаки), m определяет параметры заданного механизма атаки (например, источник атаки).

Представим верхний уровень модели сетевых червей (другие модели инфраструктурных атак используют подобный шаблон): $Wrm_{n,m} = \langle I, M_{ct}, f, Sprt, Dprt, M_{st}, P_{sc}, PS, M_{spoof} \rangle$, где I — идентификатор червя; M_{ct} — тип соединения, соединения могут быть на основе протокола TCP или на основе протокола UDP; f — частота генерации пакетов, число пакетов (соединений), генерируемых в секунду; $Sprt$ — сетевой порт, с которого отсылаются пакеты; $Dprt$ — сетевой порт, на который отсылаются пакеты; M_{st} — методика сканирования; P_{sc} — вероятность установления успешного TCP-соединения; Данный параметр имеет значение в случае распространения сетевых червей по протоколу TCP, в случае работы по UDP, параметр помечается как недоступный; PS — размер пакета передаваемого по сети; M_{spoof} — методики подмены сетевого адреса и порта.

События, генерируемые сетевыми червями, определяются в виде $Ev_{Wrm} = \langle nSpr, Vun \rangle$, где $nSpr$ — функция, отвечающая за начало

распространения сетевых червей, *Vun* — функция регламентирующая работу уязвимого узла. Функция *nSpr* определяется так:

if TIMER
  then NEWTIMER(*f*)
  if M_{ct} = TCP
    then TRYTOCONNECT(M_{st} (*trgIPaddr*))
    if connected
      then SENDPKTTO(M_{st} (*IPaddr*), *I* , *Sprt* , *Dprt* , M_{spoof})
  else SENDPKTTO(M_{st} (*IPaddr*), *I* , *Sprt* , *Dprt* , M_{spoof}),

где TIMER и NEWTIMER — функции описывающие срабатывание и планирование нового таймера соответственно, TRYTOCONNECT — функция выполняющая попытку осуществить трехэтапное рукопожатие в соответствии со спецификацией протокола TCP, SENDPKTTO — функция отправки пакетов с заданными параметрами.

Модели базовых механизмов защиты от инфраструктурных атак. Здесь и далее показан верхний уровень представления основных моделей без описания алгоритма из работы. Множество базовых механизмов защиты представляются в виде: $D = \langle Sc, En_D, Ev_D, T \rangle$. Представим сущности базовых механизмов защиты как $En_D = \langle TD, CD \rangle$, где TD — тип базового механизма защиты; CD — параметры механизма защиты.

Тип механизма защиты от инфраструктурных атак: $TD = \langle DWrm_{n,m}, DfDDoS_{n,m}, DAoR_{n,m}, DAoDNS_{n,m} \rangle$, где $DWrm_{n,m}$ — механизмы защиты от распространения сетевых червей; $DfDDoS_{n,m}$ — механизмы защиты от DDoS-атак; $DAoR_{n,m}$ — механизмы защиты от атак на маршрутизаторы; $DAoDNS_{n,m}$ — механизмы защиты от атак на серверы DNS.

Рассмотрим теоретико-множественные модели базовых механизмов защиты от распространения сетевых червей. Представим $DWrm_{n,m}$ как $DWrm_{n,m} = \{VT, FC, TRW, CB, ...\}$, где VT — механизм защиты на основе подхода «дросселирование вирусов» (VT); *FC* — механизм защиты на основе подхода «анализ неудачных соединений» (FC); *TRW* — механизм защиты на основе подхода «случайного порогового прохождения» (Threshold Random Walk); *CB* — механизм ограничения интенсивности соединений на основе кредитов доверия (Credit Base-based Rate Limiting).

Для примера, приведем события, с которыми работает механизм защиты *VT*: $Ev_{VT} = \{inPkt_{VT}, Tm_{VT}\}$, событие $inPkt_{VT}$ обозначает получение пакета из

сети и вызывает функцию PF_{VT}. Tm_{VT} — генерируется внутренним таймером модуля и вызывает функцию TF_{VT}, описывающую действия механизма защиты при срабатывании таймера.

Комбинированная модель и алгоритмы защиты от инфраструктурных атак на основе подхода «нервная система сети». В качестве компонента, обеспечивающего кооперацию базовых механизмов защиты, выступает механизм «нервная система сети». В каждой автономной системе имеется специальный сервер, который выполняет функции сбора и обработки информации, координации подключенных к нему узлов и обмена данными об атаках с серверами в других сетях. Узлы выполняют функции обнаружения и блокировки атак, а также передачи информации об обнаруженных атаках на сервер к которому они подключены.

Представим «нервную систему сети» в виде $NN = \langle Sc, En_{NN}, Ev_{NN}, T \rangle$, где объекты «нервной системы сети представлены следующим образом: $En_{NN} = \langle NS, NH \rangle$, где *NS* — сервера «нервной системы сети»; *NH* — узлы нервной системы сети, например маршрутизаторы.

Сервер «нервной сети» содержит в себе следующие модули: $NS = \langle IM, EM, DM, sDB \rangle$, где *IM* — блок обмена данными с узлами «нервной сети»; *EM* — блок обмена данными между серверами «нервной системы сети»; *DM* — блок принятия решений и определения ответной реакции; *sDB* — база данных.

Блок принятия решений и определения ответной реакции задается так: $DM = \langle PM, CM, dEE, dBE, dAD \rangle$, где *PM* — модуль приоритезации полученных данных; *CM* — модуль корреляции полученных данных; *dEE* — модуль обмена данными с другими серверами нервной системы сети и узлами локальной нервной системы сети; *dBE* — модуль обмена информацией с базой данных сервера; *dAD* — модуль принятия решений.

Представим узел «нервной сети» в следующем виде: $NH = \langle AG, TR, NT, HD \rangle$, где *AG* — модуль сбора информации с сенсоров; *TR* — модуль обмена данными с сервером «нервной системы сети»; *NT* — модуль обмена данными между узлами «нервной системы сети»; *HD* — модуль, реализующий обработку трафика.

Модуль обработки трафика определяется как $HD = \langle RP, CP, VD, nDB, RA \rangle$, где *RP* — блок перенаправления потоков, выполняющий разделение трафика на потоки согласно адресу отправителя и адресу получателя; *CP* — блок классификации пакетов, определяющий протокол и тип пакетов (запрос на соединение, пакет с данными и т.п.); *VD* — блок анализа и противодействия; *nDB* — база данных узла; *RA* — блок сдерживания атак.

Модели взаимодействия. Механизмы атаки и защиты находятся в состоянии антагонистического противоборства, так как преследуют противоположные цели. При этом механизмы взаимодействуют, воздействуя друг на друга с помощью компьютерной сети.

Модель взаимодействия определяется как $C = \{Ob, Tp\}$, где Ob — объекты взаимодействия, Tp — тип взаимодействия между объектами. В качестве объектов взаимодействия рассматриваются легитимные пользователи L, механизмы атак A и механизмы защиты D. Объекты могут, как кооперировать, так и противодействовать. Тип взаимодействия может быть следующим: cp — кооперация узлов, imp –противодействие узлов.

Третья глава посвящена представлению разработанной архитектуры системы моделирования и ее реализации, описанию прототипа системы моделирования инфраструктурных атак, механизмов защиты от них, в т.ч. механизма защиты на основе подхода «нервная система сети», реализации методики моделирования, оценке показателей ее применения и показателей механизма защиты на основе подхода «нервная система сети».

Предлагаемая архитектура системы моделирования имеет четыре основных компонента и отличается включением в ее состав базовых компонентов «нервной системы сети», имитационных моделей механизмов инфраструктурных атак и защиты от них в виде моделей приложений (рис.1).

На нижнем уровне располагается *базовая система имитационного моделирования*. Она представляет собой систему моделирования на основе дискретных событий. Для моделирования узлов и протоколов сети Интернет, используется *модуль имитации сети Интернет*. Он содержит компоненты для формирования сетевых топологий, модели сетевых приложений, и модели протоколов. Компонент использует библиотеку ReaSE, предназначенную для моделирования вычислительных сетей, реалистично представляющих сеть Интернет. Подсистема *базовых компонентов «нервной системы сети»* представляет собой библиотеку модулей, определяющую компоненты «нервной системы сети» и общие сценарии их поведения, реализованных в виде моделей сервисов и приложений, встраиваемых в модели узлов вычислительной сети. *Модуль процессов предметной области* включает компоненты механизмов атаки и механизмов защиты, а также модули, дополняющие функциональность узлов, включая таблицу фильтрации, анализатор пакетов, модели легитимных пользователей и т.д.

Система имитационного моделирования разработана на основе среды имитационного моделирования OMNeT++, библиотек INET Framework, ReaSE и разработанных компонент. Система включает в себя следующие основные функциональные подсистемы: подсистему имитации событий; интегрированную среду разработки; генератор моделей компьютерных сетей; модели легитимных пользователей; модели механизмов инфраструктурных

атак; модели механизмов защиты от инфраструктурных атак; модели взаимодействия механизмов атаки, защиты и легитимных пользователей; подсистему сбора выходных данных выполнения моделей; подсистему анализа данных.

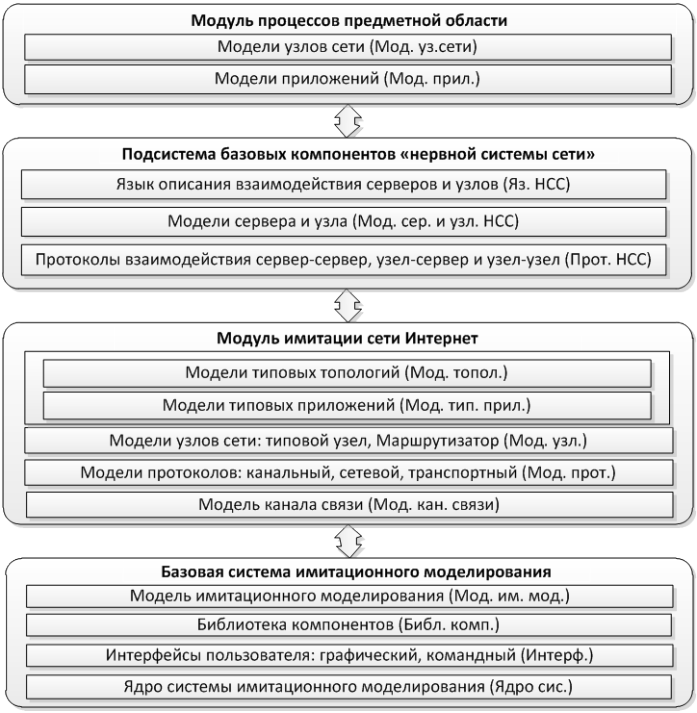

Рис. 1. Архитектура среды моделирования

С помощью разработанной программной среды для имитационного моделирования реализованы модели распространения сетевых червей (в т.ч. модель уязвимого узла), распределенной атаки типа «отказ в обслуживании», модели механизмов защиты на основе подходов FC, VT, HCF, SIM, SAVE, SYN detection, модель распределенного механизма защиты на основе подхода «нервная система сети».

Методика проведения имитационного моделирования инфраструктурных атак разделена на четыре основных этапа (рис.2). Рисунок содержит обобщенную методику имитационного моделирования, более подробно методика представлена в диссертационной работе.

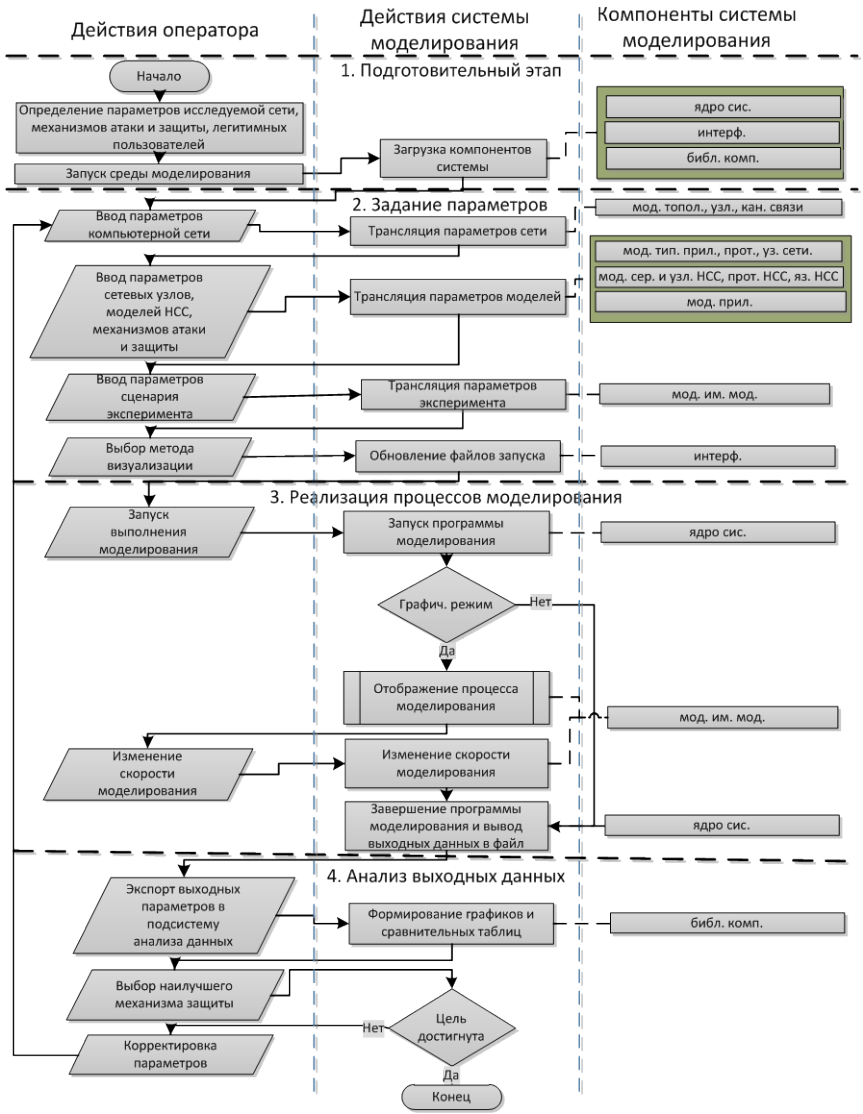

Рис. 2. Представление обобщенной методики имитационного моделирования

Методика позволяет исследовать механизмы реализации атак и защиты в зависимости от параметров моделей и сценария эксперимента. Используя лексико-графический метод, можно определять наилучшие стратегии выполнения расположения механизмов защиты и их параметров. С помощью

представленной методики и разработанной системы имитационного моделирования выполнено множество экспериментов по моделированию инфраструктурных атак и механизмов защиты от них.

Эксперименты по исследованию моделей защиты от инфраструктурных атак включают моделирование базовых механизмов защиты FC, VT, HCF, SIM, SAVE, SYN detection и механизма защиты «нервная система сети», работающего в кооперации с базовыми механизмами защиты. Для проведения экспериментов использовалась сеть, состоящая из 3652 узлов, 10 из которых являются серверными узлами, в состав которых входят: один DNS-сервер, три веб-сервера и шесть почтовых серверов. 1119 узлов (около 30% от общего количества) имеют уязвимости, необходимые для успешного осуществления распространения сетевых червей, эти же узлы выполняют DDoS-атаку, в случае ее моделирования.

В случае проведения экспериментов только с базовыми механизмами защиты они устанавливаются на 100% маршрутизаторов. При использовании подхода «нервная система сети», базовые механизмы защиты подключены к серверам «нервной системы сети». Для моделирования распространения сетевых червей, в компьютерной сети часть узлов имеет уязвимость, которую может эксплуатировать моделируемый червь. На рис. 3 показано количество зараженных хостов при выполнении механизма защиты Failed Connection установленного на 100% маршрутизаторов (FC-100%), механизма защиты Virus Throttling (VT-100%), механизма защиты на основе подхода «нервная система сети» в кооперации с механизмом защиты Failed Connection (НСС-100%) и распространении сетевых червей без защиты. Видно, что в случае координации механизма защиты FC «нервной системой сети», количество зараженных хостов снижается почти на 20% относительно механизма защиты FC и примерно на 10% относительно VT.

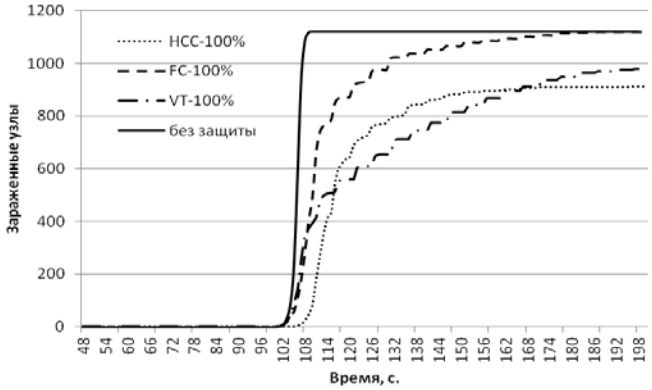

Рис. 3. Количество зараженных хостов относительно модельного времени

В экспериментах по моделированию DDoS-атак выполнялись атаки SYN Flooding, в половине экспериментов использовалась подмена IP-адреса отправителя. В качестве механизмов защиты от DDoS-атак использовались подходы SAVE, HCF и SIM.

В случае работы механизма защиты «нервная система сети», управление базовыми механизмами защиты выполнялось серверами «нервной системы». Эксперименты показали, что механизм защиты «нервная система сети» позволил снизить вредоносный трафик, поступающий на атакуемый узел, на 40% относительно базовых механизмов защиты, работающих без кооперации. Проведенные эксперименты продемонстрировали эффективность кооперации «нервной системы сети» с базовыми механизмами защиты в случае противодействия инфраструктурным атакам распространения сетевых червей и DDoS. Решающую роль здесь играет своевременная передача информации об обнаруженных атаках по всем серверам «нервной системы сети». Вследствие этого атакующий трафик, возникающий в различных сегментах сети, сразу же блокируется.

Производилась оценка отдельных свойств эффективности выполнения методики, таких как своевременность, обоснованность и ресурсопотребление. Показатели своевременности оценивались с помощью методов сетевого планирования. С помощью экспертно-аналитического метода были получены основные значения времени выполнения операций методики ($T^{ДОП}$ = 40 мин) при ее реализации на компьютерах с процессором Intel Core 2 Duo и 2ГБ оперативной памяти. Определено, что основным критерием, определяющим длительность выполнения эксперимента, является размерность моделируемой компьютерной сети. Были проведены эксперименты на моделях компьютерных сетей с количеством узлов равным 100, 1000, 3000. Получено минимальное и максимальное время выполнения моделирования механизмов защиты от инфраструктурных атак (от 45 до 445 секунд). Определено, что вероятность своевременного выполнения методики для сети размером до 1000 хостов при $T^{ДОП}$ = 40 мин, $P_{СВ}\left(t \le T^{ДОП}\right)$ составляет 0.9861, что соответствует предъявляемым требованиям к своевременности. Для оценки обоснованности использовались следующие показатели: полнота входных параметров, которая предполагает, что в методике N^{met} учитывались все входные параметры, представленные в таксономии инфраструктурных атак N_A и предложенной классификации механизмов защиты от инфраструктурных атак N_D, а также параметры работы легитимных пользователей N_L ($N^{met} = N_A + N_D + N_L$); полнота параметров методики N^{met} в сравнении с существующими системами N^k — $N^{met} \ge \max_{k \in K} N^k$, где K — множество этих систем; адекватность работы

механизмов инфраструктурных атак и механизмов защиты от них; адекватность моделирования протоколов работающих в сети Интернет. Показано, что эти требования выполняются.

Ресурсупотребление оценивалось с помощью разработанной системы имитационного моделирования. Входные параметры для моделирования аналогичны приведенным экспериментам. Данные, полученные в результате экспериментов, показали, что ресурсопотребление соответствуют предъявляемым требованиям.

Проводилось сравнение разработанной методики с методиками представленными другими исследователями. В результате анализа не было найдено систем, являющихся полными аналогами разработанной методики. Сравнение методик проводилось на качественном уровне по различным функциональным возможностям систем.

Проведена оценка эффективности работы механизма защиты «нервная система сети» относительно базовых механизмов защиты с помощью следующих показателей качества классификации трафика: ошибки первого и второго рода, полнота, точность, аккуратность, ошибка, F-мера. Для примера в табл. 1 приводится сравнение механизма защиты FC в случае самостоятельной работы и под управлением «нервной системы сети» (НСС).

Таблица 1. Сравнение механизмов защиты

	FP	FN	полнота	точность	аккуратн.	F-мера
FC	0.31	0.18	0.52	0.78	0.21	0.59
НСС	0.22	0.22	0.77	0.90	0.71	0.83

Верификация предложенных имитационных моделей проводилась на выделенном фрагменте компьютерной сети. Было выявлено соответствие средних значений основных характеристик (таких как потери пакетов, задержки, нагрузка на серверы и маршрутизаторы и т.п.) реализованных моделей и реальных процессов. Кроме того, производилось качественное сравнение механизма защиты «нервная система сети» с кооперативными механизмами COSSACK, DefCOM и другими подходами на основе данных о количестве вредоносного трафика поступающего на атакуемый узел. Механизм защиты «нервная система сети» показал большую эффективность по сравнению с другими кооперативными механизмами защиты.

ЗАКЛЮЧЕНИЕ

Данная работа предлагает модельно-методический аппарат для имитационного моделирования инфраструктурных атак и механизмов защиты от них, в т.ч. механизмов защиты, основанных на биологической метафоре.

1. Разработаны имитационные модели базовых механизмов реализации инфраструктурных атак на компьютерные сети и защиты от них. Предложена комбинированная модель и алгоритмы защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети». Определены модели взаимодействия механизмов атаки и защиты между собой и с моделью среды взаимодействия (компьютерная сеть). Представляемые модели и процессы взаимодействия между ними были формализованы.
2. Разработана архитектура системы имитационного моделирования инфраструктурных атак и механизмов защиты от них. Архитектура состоит из четырех компонентов: базовой системы имитационного моделирования, модуля моделирования процессов сети Интернет, подсистемы базовых компонентов «нервной системы сети» и библиотеки имитации процессов предметной области.
3. Разработана методика имитационного моделирования инфраструктурных атак и механизмов защиты от них. Представленная методика позволяет повысить эффективность анализа механизмов защиты от инфраструктурных атак на компьютерные сети, в т.ч. механизмов защиты основанных на биологической метафоре.
4. С помощью представленной архитектуры и методики реализована система имитационного моделирования инфраструктурных атак и механизмов защиты от них. Данная система моделирования использовалась для реализации экспериментов с использованием предложенных моделей и методики, что позволило провести анализ данных моделей и показать эффективность их работы.

Полученные в работе результаты можно использовать для исследования инфраструктурных атак на компьютерные сети; исследования, проектирования и тестирования механизмов защиты от инфраструктурных атак, в т.ч. основанных на биологических подходах; повышения эффективности проектирования защищенных компьютерных сетей; определения проблем и узких мест существующих компьютерных сетей и выполнения их оптимизации; оценивания устойчивости компьютерных сетей в условиях воздействия различных инфраструктурных атак.

СПИСОК ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в ведущих рецензируемых научных журналах и изданиях из списка ВАК:

1) Котенко И.В., Коновалов А.М., Шоров А.В. Исследование бот-сетей и механизмов защиты от них на основе методов имитационного моделирования // Изв. вузов. Приборостроение, Т.53, № 11, 2010. С. 42-45. ISSN 0021-3454.

2) Котенко И.В., Коновалов А.М., Шоров А.В. Моделирование бот-сетей и механизмов защиты от них // Системы высокой доступности, № 2, Т.7, 2011. С. 107-111.
3) Котенко И.В., Коновалов А.М., Шоров А.В. Агентно-ориентированное моделирование бот-сетей и механизмов защиты от них // Вопросы защиты информации, № 3, 2011. С. 24-29.
4) Котенко И.В., Коновалов А.М., Шоров А.В. Имитационное моделирование механизмов защиты от бот-сетей // Труды СПИИРАН. Вып. 19., 2011. С. 7–33.
5) Котенко И.В., Шоров А.В., Нестерук Ф.Г. Анализ биоинспирированных подходов для защиты компьютерных систем и сетей // Труды СПИИРАН. Вып. 18, 2011. С.19–73.

Остальные публикации:

6) Kotenko I., Konovalov A., Shorov A. Agent-based simulation of cooperative defence against botnets // Concurrency and Computation: Practice and Experience, Vol. 24, Issue 6, 25 April 2012. P. 573-588.
7) Kotenko I., Konovalov A., Shorov A. Simulation of Botnets: Agent-based approach // Intelligent Distributed Computing IV. Studies in Computational Intelligence. Springer-Verlag, Vol.315. Proceedings of 4th International Symposium on Intelligent Distributed Computing - IDC'2010. September 16-18, 2010. Tangier, Morocco. Springer. P. 247–252.
8) Kotenko I., Konovalov A., Shorov A. Agent-based Modeling and Simulation of Botnets and Botnet Defense // Conference on Cyber Conflict. Proceedings 2010. CCD COE Publications. Tallinn, Estonia, June 15-18, 2010. P.21-44. ISBN 978-9949-9040-1-3.
9) Kotenko I., Konovalov A., Shorov A. Simulation of botnets and protection mechanisms against them: software environment and experiments // 16th Nordic Conference on Secure IT-Systems. October 26th-28th, 2011. Tallinn, Estonia, Preproceedings, Cybernetica, 2011. P. 119-126.
10) Котенко И.В., Коновалов А.М., Шоров А.В. Исследовательское моделирование бот-сетей и механизмов защиты от них. Приложение к журналу «Информационные технологии». Москва: Издательство Новые технологии, 2012, № 1. 32 с. ISSN 1684-6400.
11) Котенко И.В., Коновалов А.М., Шоров А.В. Агентно-ориентированное моделирование функционирования бот-сетей и механизмов защиты от них // Защита информации. Инсайд, 2010. № 4, С.36-45. № 5, С.56-61.
12) Шоров А.В. Анализ биологических подходов для защиты компьютерных сетей от инфраструктурных атак // VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009). 28-30 октября 2009 г. Материалы конференции. СПб, 2009. С.145.

13) Шоров А.В. Архитектура механизма защиты от инфраструктурных атак на основе подхода «нервная система сети» // VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2011). 26-28 октября 2011 г. Материалы конференции / СПОИСУ. - СПб., 2011. С. 157-158.
14) Котенко И.В., Шоров А.В. Использование биологической метафоры для защиты компьютерных систем и сетей: предварительный анализ базовых подходов // Защита информации. Инсайд, 2011. № 1, С.52-57. № 2, С.66-75.
15) Шоров А.В. Анализ DDoS-атак и механизмов защиты от них и требования к их моделированию // XII Санкт-Петербургская Международная Конференция “Региональная информатика-2010” (“РИ-2010”). Материалы конференции. СПб., 2010.
16) Шоров А.В. Анализ биоинспирированных подходов в области защиты компьютерных систем // XII Санкт-Петербургская Международная Конференция “Региональная информатика-2010” (“РИ-2010”). Материалы конференции. СПб., 2010.
17) Шоров А.В. Моделирование стадии формирования и сдерживания распространения бот-сети // Методы и технические средства обеспечения безопасности информации. Материалы XIX Общероссийской научно-технической конференции. СПб: Издательство Политехнического университета, 2010. С.50-51.
18) Шоров А.В., Котенко И.В. Теоретико-множественное представление имитационных моделей инфраструктурных атак и механизмов защиты от них // Пятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2011). Санкт-Петербург, 19-21 октября 2011 г. Сборник докладов. СПб.: ОАО “Центр технологии судостроения и судоремонта”. 2011. С.306-310.
19) Шоров А.В. Теоретико-множественные модели для имитационного моделирования инфраструктурных атак на компьютерные сети и механизмов защиты от них // Материалы Юбилейной 20-ой научно-технической конференции 27 июня-01 июля 2011 года. Спб.: Издательство Политехнического университета, 2011. С. 196.
20) Коновалов А.М., Шоров А.В. Моделирование противодействия бот-сетей и механизмов защиты от них // Тринадцатая Международная конференция “РусКрипто’2011”. Московская область, г.Солнечногорск, 30 марта-2 апреля 2011 г. http://www.ruscrypto.ru/