Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.056.57

На правах рукописи

ДАВИДОВСКИЙ
Артём Олегович

МОДЕЛИ И АЛГОРИТМЫ РЕАЛИЗАЦИИ ИНФРАСТРУКТУРНЫХ АТАК НА КОМПЬЮТЕРНЫЕ СЕТИ И МЕХАНИЗМОВ ЗАЩИТЫ ОТ НИХ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра техники и технологий

по специальности 1-39 81 01 – Компьютерные технологии
проектирования электронных систем

Минск 2017

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **ЦЫРЕЛЬЧУК Игорь Николаевич,**
кандидат технических наук, доцент, декан факультета непрерывного и дистанционного обучения, заведующий кафедрой проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **НОВИКОВ Сергей Олегович,**
кандидат технических наук, доцент, доцент кафедры электрические системы учреждения образования «Белорусский национальный технический университет»

Защита диссертации состоится «26» января 2017 г. года в $11^{\underline{00}}$ часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, e-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

СОГЛАСОВАНО:
Научный руководитель
декан ФНиДО, заведующий
кафедрой ПИКС
канд.техн.наук, доцент И.Н. Цырельчук

ВВЕДЕНИЕ

Современное общество уже не может обойтись без информационных технологий, которые проникли во все сферы жизни человека. Их неотъемлемой частью является глобальная сеть Интернет. В связи с этим одной из главных задач является обеспечение безопасности обращения информации внутри сети, которая подвержена инфраструктурным атакам на компьютерные сети.

Для организации коммуникаций в неоднородной сетевой среде применяются набор протоколов *TCP/IP*, обеспечивая совместимость между компьютерами разных типов. Данный набор протоколов завоевал популярность благодаря совместимости и предоставлению доступа к ресурсам глобальной сети Интернет и стал стандартом для межсетевого взаимодействия. Однако повсеместное распространение стека протоколов *TCP/IP* обнажило и его слабые стороны. В особенности из-за этого инфраструктурным атакам подвержены распределённые системы, поскольку их компоненты обычно используют открытые каналы передачи данных, и нарушитель может не только проводить пассивное прослушивание передаваемой информации, но и модифицировать передаваемый трафик.

Трудность выявления проведения инфраструктурных атаки и относительная простота проведения(из-за избыточной функциональности современных систем) выводит этот вид неправомерных действий на первое место по степени опасности и препятствует своевременному реагированию на осуществлённую угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки.

Все это говорит о необходимости исследований в области защиты компьютерных сетей от инфраструктурных атак. Таким образом, необходимо знать модели и алгоритмы реализации инфраструктурных атак на компьютерные сети, а также механизмы защиты от них.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В настоящее время наблюдается тенденция к увеличению количества и мощности компьютерных атак на инфраструктуру вычислительных сетей. 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 серверы и атаки на маршрутизаторы. Все это говорит о необходимости исследований в области защиты компьютерных сетей от инфраструктурных атак.

Степень разработанности проблемы

Исследование моделей и алгоритмов реализации инфраструктурных атак на компьютерные сети и механизмов защиты от них осуществлялось на основе построения теоретических моделей с использованием работ российских и белорусских ученых: А.В. Шоров, И.В. Котенко, В.В. Воронцов, А.В. Уланов, А.Е. Боршевников и др.

Одним из недостатков исследований, представленных в современной технической литературе, является неполное рассмотрение особенностей и условий для моделирования инфраструктурных атак на компьютерные сети и механизмов защиты от них.

Предложенное исследование направлено на устранение этого недостатка на основе модификации алгоритма моделирования инфраструктурных атак на компьютерные сети и механизмов защиты от них.

Цель и задачи исследования

Целью диссертации является повышение защищенности компьютерных сетей, обусловленное совершенствованием моделей, алгоритмов и механизмов защиты от инфраструктурных атак.

Для выполнения поставленной цели в работе были сформулированы следующие задачи:

1. Проанализировать инфраструктурные атаки на компьютерные сети и механизмы защиты от них.

2. Разработать модели, реализующие инфраструктурные атаки и механизмы защиты от них.

3. Разработать методику имитационного моделирования инфраструктурных атак и механизмов защиты от них с помощью представленных моделей и архитектуры.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) ОСВО 1-39 81 01-2012 специальности 1-39 81 01 «Компьютерные технологии проектирования электронных систем».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в области разработки моделей и алгоритмов инфраструктурных атак на компьютерные сети и механизмов защиты от, а также анализ технических нормативных правовых актов по рассматриваемой тематике.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна работы заключается в рассмотрении моделей алгоритмов реализации инфраструктурных атак на компьютерные сети и механизмов защиты от них. 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.

Теоретическая значимость диссертации состоит в том, что имея представления о том, что такое инфраструктурная атака и зная механизмы защиты можно предотвратить атаки на компьютерные сети.

Практическая значимость работы заключается в том, что 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.

Основные положения, выносимые на защиту

1. Систематизация информации об инфраструктурных атаках на компьютерные сети и механизмов защиты от них, основанная на вредоносном воздействии, позволившая разработать модели инфраструктурных атак на компьютерные сети и механизмы защиты от них.

2. Модели реализующие инфраструктурные атаки и механизмы защиты от них, разработанные в специализированном программном продукте, позволяющие построить методику имитационного моделирования инфраструктурных атак и механизмов защиты от них.

3. Методика имитационного моделирования инфраструктурных атак и механизмов защиты от них, основанная на разработанных моделях, позволяющая анализировать системы защиты существующих сетей и для выработки рекомендаций по созданию перспективных систем защиты.

Апробация диссертации и информация об использовании ее результатов

Результаты работы по теме диссертации были представлены на 52-й научной конференции аспирантов, магистрантов и студентов БГУИР (г. Минск, Республика Беларусь, 2016 г.) и Международной научно-практической интернет-конференции молодых ученых и студентов «Акту-

альные проблемы автоматизации и управления (г. Луцк, Украина, 2016 г.).

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 6 печатных работах. В их числе 2 статьи в сборнике материалов научной конференции, 3 тезиса докладов на научных конференциях, 1 статья в научном журнале.

Общий объем публикаций по теме диссертации составляет 18 страниц.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения и библиографического списка.

В первой главе были рассмотрены инфраструктурные атаки и их виды. Рассмотрены механизмы защиты от инфраструктурных атак.

Во второй главе были разработаны модели, реализующие инфраструктурные атаки и механизмы защиты от них.

В третьей главе была разработана методика имитационного моделирования инфраструктурных атак и механизмов защиты от них.

В приложении представлены публикации автора и акт внедрения.

Общий объем диссертационной работы составляет 99 страниц. Из них 55 страниц основного текста, 6 иллюстраций, библиографический список из 51 наименований, список собственных публикаций соискателя из 6 наименований, 3 приложения на 36 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** описана трудность выявления проведения инфраструктурных атаки и относительная простота проведения, из-за избыточной функциональности современных систем. Обоснована необходимость знания моделей и алгоритмов реализации инфраструктурных атак на компьютерные сети, а также механизмы защиты от них, то есть актуальность темы диссертационной работы.

В **общей характеристике работы** рассмотрены инфраструктурные компоненты, компьютерной сети представлена актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимости исследований, а также апробация работы.

В **первой главе** рассматриваются инфраструктурные компоненты компьютерной сети (рисунок 1). Выделяются четыре типа инфраструктурных атак: атака типа «отказ в обслуживании» (*DoS*), сетевые черви, атаки на *DNS*-сервер и атаки на маршрутизатор.

DoS-атаки используют множество систем для нападения на один или

несколько сайтов, цель которых — добиться отказа в обслуживании. Высокий уровень автоматизации в инструментальных средствах организации атак позволяет одному злоумышленнику установить свой инструментарий и контролировать десятки тысяч промежуточных систем, используемых для нападения.

Сетевой червь — это самотиражирующийся вредоносный код, который в состоянии распространять себя сам. Самый серьезный вред от сетевых червей состоит в том, что благодаря своему активному распространению они создают возможности организации *DoS*-атак из-за огромного объема трафика, который они генерируют.

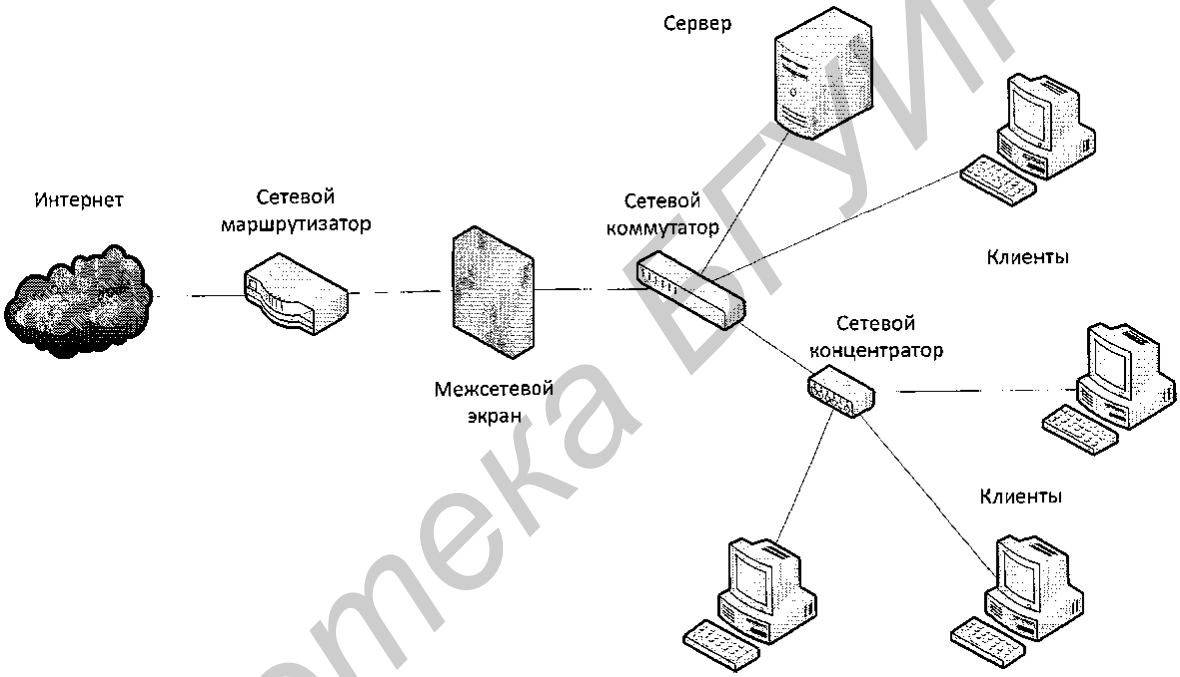

Рисунок 1 — Обобщенная компьютерная сеть

Атаки на DNS-сервер. *DNS* — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения *IP*-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (*SRV*-запись).

Распределённая база данных *DNS* поддерживается с помощью иерархии *DNS*-серверов, взаимодействующих по определённому протоколу.

Основой *DNS* является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени. Среди потенциальных угроз *DNS* — искажение кэша, фальсификация данных, отказ в обслуживании и кража доменов.

Атаки на маршрутизаторы. Потенциальные угрозы для маршрутизаторов разделяются на следующие категории:

— отказ в обслуживании. Хотя маршрутизаторы рассчитаны на передачу больших объемов трафика, они зачастую не способны обрабатывать те же объемы трафика, адресуемые им самим;

— использование доверительных отношений между маршрутизаторами. Чтобы маршрутизаторы могли выполнять возложенные на них обязанности, они должны знать, куда переслать трафик, который они получают. Они делают это путем обмена друг с другом информацией о маршрутизации, в силу чего маршрутизаторы вынуждены доверять данным, которые они получают друг от друга. В результате, злоумышленник может изменить, удалить или добавить маршруты в глобальные таблицы маршрутизации таким образом, чтобы перенаправить предназначенный для одной сети трафик в другую сеть.

Во второй главе представлены разработки моделей, реализующие инфраструктурные атаки, механизмы защиты от них.

Основными компонентами для проведения имитационного моделирования выполнения инфраструктурных атак и механизмов защиты от них являются: модель компьютерной сети, в т.ч. модели легитимных пользователей, модели инфраструктурных атак, модели механизмов защиты.

Модель компьютерной сети определяется топологией, типами узлов, трафиком циркулирующем в сети. Основным типом топологии использующемся при моделировании компьютерной сети является «дерево». Для генерации топологий используется библиотека *ReaSE*, которая позволяет создавать топологии близкие к существующим, в настоящее время, в компьютерных сетях. Также библиотека *ReaSE* используется для генерации реалистичного трафика создаваемого легитимными узлами в сети. Легитимный трафик включает в себя обмен данными между пользовательскими узлами, а также работу пользователей с серверами, в пропорциях типичных для корпоративных сетей. Трафик состоит из пакетов, которые обрабатываются на основных уровнях модели *OSI*. Это позволяет использовать его для исследования большинства методов защиты от инфраструктурных атак.

Генерация топологии на уровне роутеров более сложна и основывается на данных коммерческих провайдеров, которые публикуют информацию о структуре своих сетей. Для генерации используется подход, предложенный в , названный «эвристически-оптимальной топологией» (*HOT, Heuristically Optimal Topology*). Данный подход учитывает ограничения каналов связи, аппаратной части маршрутизаторов и хостов. Таким образом строится иерархическая топология, на верхнем уровне которой находятся небольшое количество главных маршрутизаторов (*core routers*), которые перенаправляют трафик на промежуточный уровень (шлюзы), с которого трафик попадает на конечные маршрутизаторы к которым присоединены хосты (рисунок 2) . Пропускная способность каналов связи между главными маршрутизаторами, шлюзами, и конечными маршрутизаторами также различается и падает в зависимости от уровня передающего устройства.

Модели инфраструктурных атак включают в себя модели выполняющие атаки «распространение сетевых червей» и распределенная атака типа «отказ в обслуживании». Модель, выполняющая атаку типа «распространение сетевых червей» состоит из двух модулей. Первый компонент отвечает за сканирование компьютерной сети и рассылку специально сформированных пакетов содержащих «вредоносный» код на удаленные узлы. Второй модуль «сетевых червей» выполняет функцию уязвимого сервиса, который при получении специально сформированного пакета от зараженного узла. Механизм распространения сетевых червей, в качестве уязвимого узла использует стандартный легитимный хост, который может функционировать до и после заражения. Компонент, отвечающий за выполнении атак, используется для реализации атак на уровне транспортных протоколов.

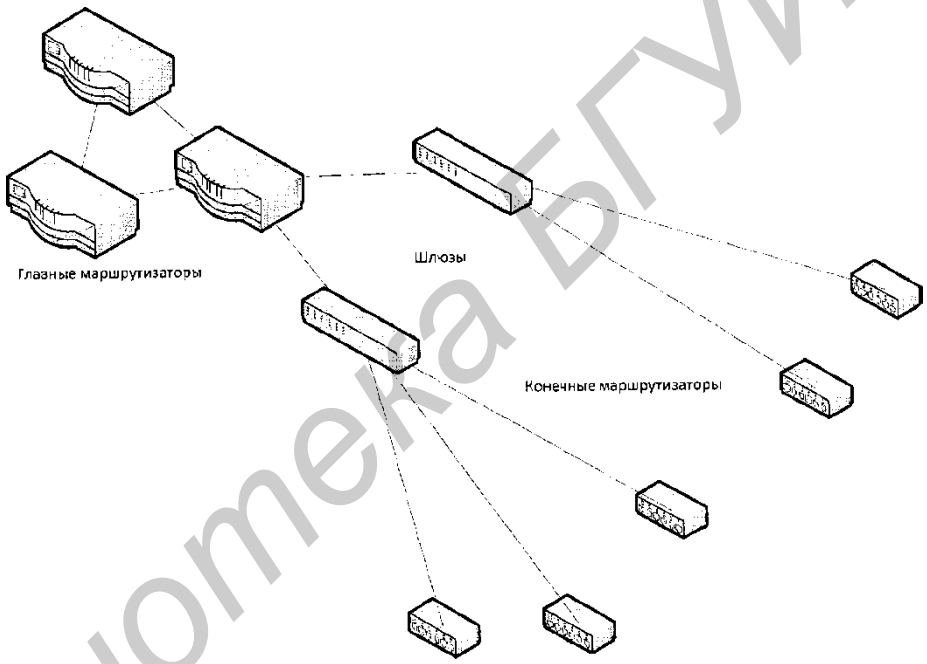

Рисунок 2 — Иерархия модели компьютерной сети на уровне маршрутизаторов

Приведены структурные и функциональные модели механизмов атак и механизмов защиты от них. Описаны параметры, необходимые для реализации представленных моделей.

В третьей главе представлена разработка методики имитационного моделирования механизмов защиты от инфраструктурных атак с помощью представленных моделей.

Для моделирования любой ситуации или системы, а также процессов защиты информации, в основном применяются методы физического (аппаратные полигоны) моделирования, методы эмуляции, аналитического (математического) моделирования, а так же имитационного моделирования.

Прототип системы моделирования включает в себя множество функциональных подсистем. Подсистема имитации событий является основным

компонентом системы моделирования. С ее помощью происходят все процессы моделирования. Содержит в себе планировщик, список сущностей (моделей), список событий выполняемых для каждой модели, временную ось. Интегрированная среда разработки включает в себя основные инструменты разработчика, такие как редактор исходных кодов, компилятор исходных кодов, отладчик и др. Модели легитимных пользователей представляют собой сложные модели узлов, состоящие из различных компонентов служащих для: функционирования модели в соответствии с уровнями эталонной модели *OSI*; выполнение процесса легитимной деятельности; эксплуатации уязвимостей при распространении сетевых червей; атакующие модули, активирующиеся в случае выполнения атаки. В качестве механизмов выполняющих атаки на инфраструктуру компьютерной сети используются простые модули, входящие в состав моделей легитимных пользователей и подключающихся к интерфейсу передачи данных. Модели механизмов выполнены в виде простых модулей, которые с помощью специального интерфейса имеют возможность подключаться к моделям различных узлов. Подсистема сбора выходных данных состоит из модуля статистики, который получает данные от различных моделей посредством специального интерфейса. Подсистема анализа данных используется для оценки результатов моделирования используется подсистема анализа данных.

Параметры инфраструктурных атак:

1. Распространение сетевых червей. Модуль распространения сетевых червей включает в себя параметры:

— диапазон адресов. Служит для указания *IP*-адресов узлов, которые будут сканироваться червем при поиске уязвимых хостов. Диапазон адресов может указываться вручную, либо использовать диапазон адресов используемых в моделируемой сети;

— тип сканирования. Адреса могут сканироваться в случайном порядке или на основе какого-либо алгоритма;

— порт получателя. Указывается порт, на котором висит уязвимое приложение;

— порт отправителя. Необходим для трехэтапного рукопожатия в случае использования протокола *TCP*;

— тип атаки: распространение червя осуществляется по протоколу *TCP* или *UDP*;

— общее количество попыток установления соединения атакующим узлом;

— начало атаки. Обозначает время начала выполнения распространения сетевых червей относительно к общему времени выполнения моделирования;

— смещение времени атаки. Используется для изменения времени начала атаки, вследствие чего узлы включаться в атаку через какой- либо определенный интервал времени;

— интервал между отправлением пакетов. Используется для определения скорости отправки пакетов. Интервал может быть статичным или изме-

няться в пределах определенной величины;

— размер пакета. Определяет размер отправляемого пакета в байтах;

— подмена адреса отправителя. В случае распространения сетевых червей посредством протокола *UDP* может использоваться подмена *IP*-адреса отправителя;

— вероятность начала или завершения атакующих действий со стороны узла. Используется для изменения количества атакующих узлов с течением времени.

2. Выполение *DDoS*-атак:

— цель атаки. Указывается *IP*-адрес жертвы;

— порт цели атаки. Указывается порт цели атаки;

— тип атаки: *TCP SYN flood*, *TCP RST flood*, *UDP flood*, *ICMP flood*;

— общее количество отправляемых пакетов каждым атакующим узлом;

— начало атаки. Задается время начала выполнения *DDoS*-атаки относительно к общему времени выполнения моделирования;

— смещение времени атаки. Определяет начать ли атаку одновременно всеми узлами или узлы будут включаться в атаку последовательно в течение определенного интервала;

— интервал между отправлением пакетов. Используется для определения скорости отправки пакетов. Интервал может быть статичным или изменяться в пределах определенной величины;

— размер пакета. Задается в байтах;

— подмена адреса отправителя. Для проведения *DDoS*-атак может использоваться подмена *IP*-адреса отправителя. Адреса для подмены могут браться из *IP*-адресов подсетей или можно вручную определить их диапазон;

— вероятность начала или завершения атакующих действий со стороны узла. Используется для изменения количества атакующих узлов с течением времени.

Данные параметры должен иметь модуль выполнения *DDoS*-атак.

Параметры механизмов защиты. Определены основные параметры механизмов защиты от инфраструктурных атак:

1. Общие для всех механизмов защиты:

— типы механизмов защиты. Выбираются механизмы защиты, которые будут устанавливаться на узлы;

— место установки. Определяет узлы, на которые устанавливаются механизмы защиты;

— степень кооперации.

2. Базовые механизмы защиты:

— место подключения. Механизмы защиты, в зависимости от типа, могут подключаться к различным модулям, отвечающим за обработку трафика моделью узла;

— буфер адресов. Задается количество адресов, с которыми может работать механизм защиты. Адреса, в различных случаях, могут принадлежать источникам или получателям трафика;

— пороговые значения. Большинство механизмов защиты имеют пороговые значения, которые используются для детектирования атак;

— период обновления счетчиков. Механизмы защиты используют таймеры, с помощью которых происходит обновление пороговых значений, буферов адресов и т.п.

Представленная методика имитационного моделирования инфраструктурных атак и механизмов защиты от них определяет, как задавать параметры модели сети, параметры атаки, параметры защиты, параметры моделей легитимных пользователей. Методика описывает, какую информацию требуется подать на вход и как получить и обработать выходные данные, для проведения исследований в области защиты от инфраструктурных атак. Методика проведения имитационного моделирования инфраструктурных атак разделена на четыре основных этапа: подготовительный, этап задания параметров, этап реализации процессов моделирования, этап анализа выходных параметров. Методика позволяет исследовать механизмы атаки и защиты в зависимости от параметров моделей и сценария эксперимента и с помощью лексико-графического метода определять наилучшие стратегии расположения механизмов защиты и набора их параметров.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Проведен системный анализ задачи имитационного моделирования механизмов защиты от инфраструктурных атак. Выполнены обзор атак на инфраструктуру компьютерных сетей, механизмов защиты от них и их классификации.

2. Разработаны модели и алгоритмы, с помощью которых реализуются атаки на инфраструктуру компьютерных сетей и модели механизмов защиты от них.

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.

Рекомендации по практическому использованию результатов

Полученные в работе результаты позволяют описывать инфраструктурные атаки и системы защиты, используя множество параметров атаки и защиты, проводить моделирование в соответствии с предложенной методикой и оценить эффективность анализируемых механизмов защиты. Это может быть использовано для анализа систем защиты существующих сетей, а также для выработки рекомендаций по созданию перспективных систем защиты.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в рецензируемых журналах

1. Давидовский А.О. Сложности создания имитационных моделей / А.О. Давидовский // Научно-методический журнал издательства «Проблемы науки» – «Научный журнал» – Москва, 2016. – в печати.

Статьи в сборниках научных трудов

2. Давидовский А.О. Технология BIM в системах автоматизированного проектирования / А.О. Давидовский, С.И. Петров // материалы международной научно-практической интернет-конференции молодых ученых и «Актуальные проблемы автоматизации и управления», Луцк, Украина, 26 ноября 2016г. – С. 80–84.

3. Давидовский А.О. Проблемы, методы и задачи математического моделирования и оптимизации тепловых процессов в микроэлектронных структурах / С.И. Петров, А.О. Давидовский // материалы международной научно-практической интернет-конференции молодых ученых и «Актуальные проблемы автоматизации и управления», Луцк, Украина, 26 ноября 2016г. – С. 105–109.

Тезисы конференций

4. Давидовский А.О. Механизмы защиты от инфраструктурных DDoS-атак / А.О. Давидовский, А.В. Рытова, А.И. Якубашко, // материалы 52-ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно-компьютерных систем», Минск, Респ. Беларусь, 25–30 апреля 2016 г. / УО «БГУИР». – Минск, 2016. – в печати.

5. Давидовский А.О. Data loss prevention системы. Выбор DLP-системы / А.В. Рытова, А.О. Давидовский // материалы 52-ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно-компьютерных систем», Минск, Респ. Беларусь, 25–30 апреля 2016 г. / УО «БГУИР». – Минск, 2016. – в печати.

6. Давидовский А.О. Разработка модели конфликтного взаимодействия программных средств защиты информации и динамических библиотек / А.И. Якубашко, А.О. Давидовский // материалы 52-ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно-компьютерных систем», Минск, Респ. Беларусь, 25–30 апреля 2016 г. / УО «БГУИР». – Минск, 2016. – в печати

РЭЗЮМЭ

Давідоўскі Арцём Алегавіч

Мадэлі і алгарытмы рэалізацы інфраструктурных нападаў на кампўтарные сеткі і механізмы абароны ад іх

Ключавыя словы: інфраструктурныя атакі, кампутарныя сеткі, механізмы абароны.

Мэта працы: мэтай дысертацыі з'яўляецца павышэнне абароненасці камп'ютэрных сетак, абумоўленае удасканаленнем мадэляў, методык і алгарытмаў даследчага мадэлявання механізмаў абароны ад інфраструктурных нападаў.

Атрыманыя вынікі і іх навізна: распрацаваны мадэлі і алгарытмы, з дапамогай якіх рэалізуюцца атакі на інфраструктуру кампутарных сетак і мадэлі механізмаў абароны ад іх. Вызначаны мадэлі ўзаемадзеяння механізмаў атакі і абароны паміж сабой і з мадэллю асяроддзя ўзаемадзеяння (кампутарная сетка). Прадстаўляюцца мадэлі і працэсы ўзаемадзеяння паміж імі былі фармалізаваны.

Распрацавана методыка імітацыйнага мадэлявання інфраструктурных нападаў і механізмаў абароны ад іх. Прадстаўленая методыка дазваляе павысіць эфектыўнасць аналізу механізмаў абароны ад інфраструктурных нападаў на кампутарныя сеткі.

Атрыманыя ў рабоце вынікі дазваляюць апісваць інфраструктурныя атакі і сістэмы абароны, выкарыстоўваючы мноства параметраў атакі і абароны, праводзіць мадэляванне ў адпаведнасці з прапанаванай методыкай і ацаніць эфектыўнасць аналізаваных механізмаў абароны. Гэта можа быць выкарыстана для аналізу сістэм абароны існуючых сетак, а таксама для выпрацоўкі рэкамендацый па стварэнні перспектыўных сістэм абароны.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс на ка-Федра праектавання інфармацыйна-камп'ютэрных сістэм ўстановы адукацыі «Беларускі дзяржаўны універсітэт інфарматыкі і радыёэлектронікі».

Вобласць прымянення: абарона кампутарных сетак ад інфраструктурных нападаў.

РЕЗЮМЕ

Давидовский Артём Олегович

Модели и алгоритмы реализации инфраструктурных атак на компьютерные сети и механизмов защиты от них

***Ключевые слова*:** инфраструктурные атаки, компьютерные сети, механизмы защиты.

***Цель работы*:** целью диссертации является повышение защищенности компьютерных сетей, обусловленное совершенствованием моделей, методик и алгоритмов исследовательского моделирования механизмов защиты от инфраструктурных атак.

***Полученные результаты и их новизна*:** разработаны модели и алгоритмы, с помощью которых реализуются атаки на инфраструктуру компьютерных сетей и модели механизмов защиты от них. 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.

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.

Полученные в работе результаты позволяют описывать инфраструктурные атаки и системы защиты, используя множество параметров атаки и защиты, проводить моделирование в соответствии с предложенной методикой и оценить эффективность анализируемых механизмов защиты. Это может быть использовано для анализа систем защиты существующих сетей, а также для выработки рекомендаций по созданию перспективных систем защиты.

***Степень использования*:** результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

***Область применения*:** защита компьютерных сетей от инфраструктурных атак.

SUMMARY

Davidovsky Artyom Olegovich

Models and algorithms for the implementation of infrastructure attacks on computer networks and mechanisms of protection against them

Keywords: infrastructure attack, computer network defense mechanisms.

Objective: The aim of the thesis is to improve the security of computer networks, due to the improvement of the models, methods and algorithms for the simulation research of protection against infrastructure attacks mechanisms.

The results and their novelty: models and algorithms, which are implemented via attack on computer networks and infrastructure model defense mechanisms. Defined model of interaction between the attack and defense mechanisms among themselves and with the model of the interaction of the environment (computer network). The presented models and processes were formalized interaction between them.

The technique of simulation infrastructure attacks and defense mechanisms against them. The presented method allows to increase the efficiency of the analysis of mechanisms for the protection of the infrastructure of computer network attacks.

The results obtained allow us to describe infrastructure attack and defense system, using a variety of attack and defense parameters, to carry out simulation in accordance with the proposed methodology and analyzed to evaluate the effectiveness of protection mechanisms. This can be used for analysis of protection systems of existing networks, as well as to make recommendations on the development of advanced security systems.

Use level: the results implemented in the educational process at the department of design information and computer systems educational institution "Belarusian State University of Informatics and Radio Electronics."

Application: protection of computer networks from infrastructure attacks.