Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.421:621.391

МОХАММЕД

Файсал Осман Мохаммед

АДАПТИВНОЕ УПРАВЛЕНИЕ МЕЖСЕТЕВЫМИ ЭКРАНАМИ В ИНФОТЕЛЕКОММУНИКАЦИЯХ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты

информации, информационная безопасность

Минск, 2012

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Научный руководитель: **Бобов Михаил Никитич**, доктор технических наук, профессор, начальник отдела Управления высоких технологий ОАО «Агат-системы управления» – управляющая компания холдинга «Геоинформационные системы управления»

Официальные оппоненты: **Кучинский Пётр Васильевич**, доктор физико-математических наук, директор НИУ «НИИ прикладных физических проблем им. А.Н. Севченко БГУ»

Утин Леонид Львович, кандидат технических наук, доцент, ведущий научный сотрудник «Научно- исследовательского института Вооруженных Сил Республики Беларусь»

Оппонирующая организация: Учреждение образования «Высший государственный колледж связи»

Защита состоится 7 июня 2012 года в 14:00 на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники», по адресу 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232, e-mail: dissovet@bsuir.by, тел.: 293-89-89.

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

КРАТКОЕ ВВЕДЕНИЕ

Использование современных компьютерных сетей и информационных технологий в настоящее время в большинстве своем связано с подключением к глобальной сети Интернет. Однако при подключении ИТС к Интернет возникают серьезные проблемы с обеспечением безопасности информации. Решение задач по защите ИТС от наиболее вероятных атак через Интернет возлагается на межсетевые экраны (МСЭ). МСЭ обеспечивают барьер между сетями и предотвращают или блокируют нежелательный несанкционированный трафик. Являясь защитным барьером между Интернет и внутренней ИТС, МСЭ тем самым замыкают весь информационный поток на себя, что может негативно сказаться на пропускной способности защищаемой сети. Поэтому актуальной задачей является совершенствование МСЭ путем повышения их производительности. Данная задача решается в двух направлениях: повышение быстродействия функций проверки путем совершенствования их алгоритмов и создание алгоритмов адаптивного управления работки МСЭ в зависимости от сетевой нагрузки. Данная диссертационная работа посвящена решению задачи повышения производительности МСЭ по второму направлению исследований.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами и темами

Исследования проводились в рамках следующих научно-технических программ:

1. Государственная программа информатизации Республики Беларусь на 2003 - 2005 гг. и на перспективу 2010 г. «Электронная Беларусь», утвержденная Постановлением Совета Министров Республики Беларусь от 27 декабря 2002 г. № 1819. Задание 55 «Разработать и внедрить интегрированную автоматизированную систему контрольной (надзорной) деятельности в Республике Беларусь».

2. Госбюджетная тема ГБ 11-2033 «Разработка и исследование методов и технологий построения мультисервисных локальных кабельных сетей».

Цели и задачи исследования

Целью диссертационной работы является разработка алгоритмов адаптивного управления межсетевым экранированием информационно-телекоммуникационных сетей в условиях воздействия сетевых атак.

Для достижения поставленной цели необходимо решить следующие задачи:

– провести анализ алгоритмов работы межсетевых экранов и их возможностей по предотвращению сетевых атак;

– разработать математическую модель межсетевого экрана с адаптивным управлением и провести исследования её показателей;

– синтезировать алгоритмы адаптивного управления межсетевым экраном в условиях воздействия сетевых атак;

– разработать методику адаптивного управления межсетевым экраном и программное средство для её реализации.

Объектом исследования являются межсетевые экраны, функционирующие в составе информационно-телекоммуникационных сетей.

Предметом исследования являются алгоритмы адаптивного управления межсетевыми экранами в условиях воздействия сетевых атак.

Положения, выносимые на защиту

1. Результаты исследований (полунатурное моделирование) процессов проверки трафика в МСЭ, образующих демилитаризованную зону, определяющие вид функций времени проверки трафика и устанавливающие, что время выполнения контроля целостности и инспектирования состояния зависит от длины проверяемых пакетов, а время выполнения трансляции адреса, контроля соединения и управления доступом зависит от размеров соответствующих таблиц.

2. Рекомендации по наиболее предпочтительным вариантам перераспределения функций проверки трафика между МСЭ на границе демилитаризованной зоны за счёт организации области адаптации и выбора необходимых точек переключения функций, позволяющих в 1,7 раза увеличить пропускную способность МСЭ.

3. Методика адаптивного управления МСЭ, образующих демилитаризованную зону, основанная на анализе функционального состава МСЭ, определении временных значений выполнения функций проверки, определении границ области адаптации и выборе необходимых точек переключения функций, что позволило разработать программное средство адаптивного управления любыми типами МСЭ.

Личный вклад соискателя

Все результаты были получены автором самостоятельно. Научный руководитель, доктор технических наук М.Н. Бобов принимал участие в постановке задач, определении возможных решений, оценке результатов, организации внедрения.

Апробация результатов диссертации

Результаты диссертации докладывались и обсуждались на следующих конференциях: Международная научно-практическая конференция «Теоретические и прикладные проблемы информационной безопасности в Республике Беларусь» (Академия МВД, Минск, Беларусь, 2010 г.); Международный научно-технический семинар «Телекоммуникации: сети и

технологии, алгебраическое кодирование и безопасность данных» (БГУИР, Минск, Беларусь, 2010 г.); IX Белорусско-российская научно-техническая конференция «Технические средства защиты информации» (БГУИР, Минск, Беларусь,
2010 г.); Международный научно-технический семинар «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных» (БГУИР, Минск, Беларусь, 2011 г.).

Опубликованность результатов диссертации

По материалам исследований, представленных в диссертации, опубликовано 10 печатных работ, в том числе: 5 статей в научных журналах общим объемом 2,9 авторских листа; 5 статей и тезисов в сборниках и материалов конференций.

Структура и объём диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырёх глав, заключения, библиографического списка и приложений.

В первой главе представлен анализ предметной области, выявлены существующие проблемы в рамках тематики исследования, показаны направления их решения. Во второй главе проведен анализ алгоритмов работы межсетевых экранов и определены их возможности по предотвращению сетевых атак на информационно-коммуникационные сети. Разработана математическая модель межсетевого экрана с адаптивным управлением при его функционировании в составе информационно-коммуникационной сети. В третьей главе исследованы показатели адаптивного управления межсетевым экраном, разработана полунатурная модель информационно-коммуникационной сети, защищённой межсетевым экраном. Разработана постановка экспериментальных исследований характеристик межсетевого экрана на полунатурной модели. Определены количественные значения параметров адаптивного управления межсетевым экраном. В четвёртой главе представлены результаты практической реализации алгоритма адаптивного управления межсетевым экраном в виде разработанного программного средства оценки критичности трафика и автоматической перенастройки межсетевого экрана. Представлена методика адаптивного управления межсетевым экраном в составе информационно-коммуникационной сети и приведены сравнительные оценки результатов моделирования и натурных испытаний.

Общий объем диссертационной работы составляет 138 страниц, из которых 85 страниц текста, 47 рисунков на 23 страницах, 9 таблиц на 4 страницах, 6 приложений на 19 страницах, библиография из 90 источников на 7 страницах, включая 10 собственных публикаций.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во *введении* показана необходимость повышения пропускной способности МСЭ как основного средства защиты внутренних ИТС от наиболее вероятных атак через Интернет. Обоснована актуальность темы диссертации и определена область исследований.

В *первой главе* анализируется архитектура защищенных ИТС и показывается, что защищённая ЛВС как элемент ИТС содержит три зоны безопасности, одна из которых отделяется от остальных двух внешним и внутренним МСЭ и называется демилитаризованной зоной.

Рассмотрены различные классы сетевых атак, относящиеся к различным уровням модели взаимосвязи открытых систем. Констатировано, что подавляющее большинство атак и их возможностей по нарушению конфиденциальности, целостности и доступности информации в ИТС может быть предотвращено межсетевыми экранами. Анализ различных классов МСЭ показал, что они способны обеспечивать необходимый уровень защищенности ИТС, однако являются транспортно узким местом, что может приводить к блокированию проходящего трафика.

Актуальность диссертационной работы связана с необходимостью повышения пропускной способности МСЭ, эффективным подходом к решению которой является его адаптивное управление с учётом структуры защищаемой ИТС. В условиях наличия ДМЗ представляется целесообразным переключать проверку установленных правил с внешнего на внутренний МСЭ в зависимости от сетевой нагрузки, что позволяет увеличить пропускную способность и снизить вероятность блокировки трафика.

Целью диссертационной работы является разработка алгоритмов адаптивного управления межсетевым экранированием ИТС в условиях воздействия сетевых атак. Поставлены задачи исследований, определяющие необходимость разработки модели адаптивного управления функционированием МСЭ и проведения исследований ее показателей; синтезирования алгоритмов адаптивного управления МСЭ и условиях сетевых атак; разработки методики адаптивного управления МСЭ и программного средства для ее реализации.

Во *второй главе* рассмотрена модель МСЭ с традиционным контуром управления. Структура МСЭ с традиционным контуром управления представлена на рисунке 1.

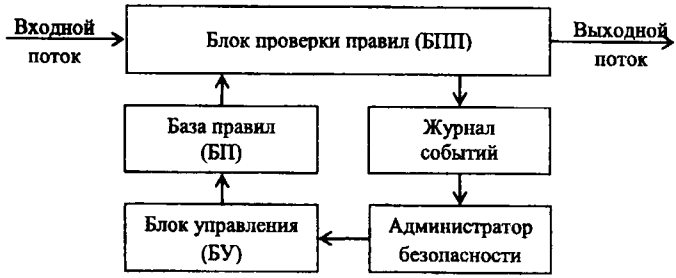


Рисунок 1 – МСЭ с традиционным контуром управления

Модель МСЭ с традиционным контуром управления представляет собой одноканальную СМО с отказами, вероятность отказа (блокировки) которой, определяется по формуле

$$p_{\text{отк}} = \frac{\lambda}{\lambda+\mu}.$$

Параметр μ является неизвестным и зависит от свойств МСЭ. Анализ алгоритма функционирования МСЭ показал, что он анализирует график путем последовательного выполнения функций, включающих в себя контроль целостности, трансляцию адреса, ведение таблицы соединений, управление доступом, инспектирование соединения и проверку контента. Поэтому процесс обслуживания МСЭ каждого пакета можно изобразить в виде схемы, приведенной на рисунке 2.

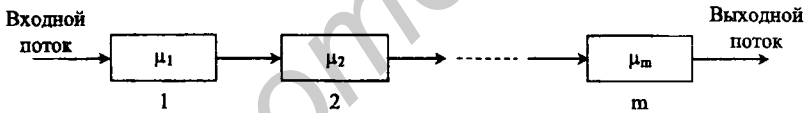


Рисунок 2 – Схема обслуживания пакетов МСЭ

Функция распределения длительности обслуживания на m последовательно соединённых однолинейных этапах называется распределением Эрланга m-го порядка и для $\mu_1 = \mu_2 = \ldots = \mu$ имеет вид

$$F(t) = 1 - e^{m\mu t} \sum_{j=0}^{m-1} \frac{(m\mu t)^j}{j!}. \quad (1)$$

Указанная функция распределения представляет собой сумму m независимых случайных величин, каждая из которых распределена по экспоненциальному закону с параметром mμ. Причём длительность обслуживания на каждом этапе имеет экспоненциальное распределение с параметром μ. В нашем случае время обслуживания, а следовательно, и параметр μ на каждом этапе обработки пакета имеет различные значения, поэтому формулу (1) непосредственно использовать нельзя. Определим

посредством $F_j(t)$ и $F_k(t)$ функции распределения времени обслуживания с параметрами μ_j и μ_k, представляющих сумму времён обслуживания пакетов МСЭ на первых j и последних k этапах соответственно.

В этом случае

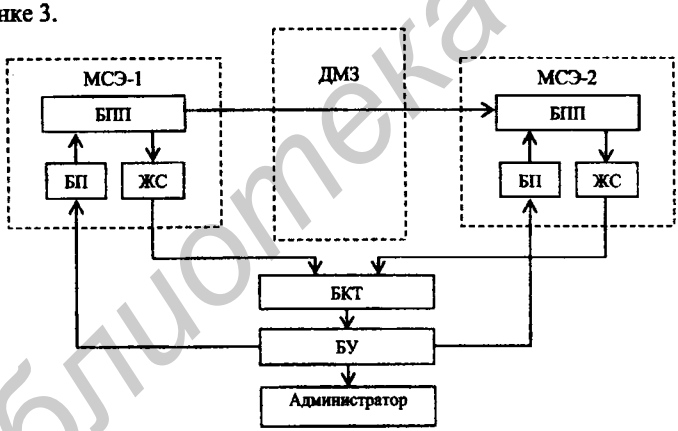
$$\mu_j = \frac{1}{\sum_{i=1}^{j} t_i}, \quad j = \overline{m-1,1} \quad ; \quad \mu_k = \frac{1}{\sum_{i=m-(k-1)}^{m} t_i}, \quad k = \overline{1,m-1}.$$

где m – общее количество функций.

Тогда вероятность блокировки пакета с учётом числа включённых в обработку этапов, начиная с первого и последнего соответственно равны

$$P_{бл}^{j} = \frac{\lambda}{\mu_j + \lambda}, \quad P_{бл}^{k} = \frac{\lambda}{\mu_k + \lambda}.$$

В традиционном контуре управления МСЭ присутствует администратор безопасности, который осуществляет настройку правил проверки пакетов. Если его функции по управлению МСЭ в случае обнаружения аномалий реализовать программными средствами, то устранение возникшей угрозы можно осуществлять автоматически, путём изменения базы правил. С учётом архитектуры защищённой ИТС, в структуре которой присутствует ДМЗ, модель МСЭ с адаптивным контуром управления можно изобразить, как показано на рисунке 3.



БКТ – блок контроля трафика

Рисунок 3 – МСЭ с адаптивным контуром управления

Блокировка в МСЭ с адаптивным контуром управления может наступить в следующих случаях:

– МСЭ-1 заблокирован, МСЭ-2 свободен;

– МСЭ-1 свободен, МСЭ-2 заблокирован;

Тогда вероятность блокировки адаптивного контура МСЭ будет равна

$$P_{бл} = \frac{\lambda(\mu_j + \mu_k)}{\lambda^2 + \lambda(\mu_j + \mu_k) + \mu_j \mu_k}.$$

В третьей главе для исследования параметров μ_i и μ_k разработана полунатурная модель ИТС, схема которой представлена на рисунке 4.

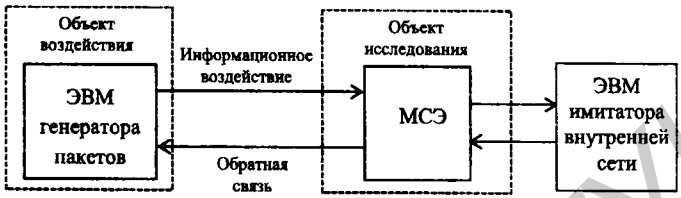


Рисунок 4 – Схема полунатурной модели ИТС

Полунатурная модель обеспечивает решение следующих задач:

1) определение продолжительности обработки пакетов каждого типа сетевой атаки, поступающей от объекта воздействия в защищаемую сеть;

2) определение продолжительности выполнения каждого вида проверки входящего пакета испытуемым МСЭ.

Генератор пакетов реализован в виде свободно распространяемого пакета программ Colasoft Packet Builder (CPB) и обеспечивает набор функций формирования пакетов различных форматов и протоколов.

МСЭ с соответствующими настройками представляет собой объект исследования. В рассматриваемой полунатурной модели использовался МСЭ Cisco ASA 5520, функционирующий под управлением операционной системы Cisco IOS.

Рабочая схема полунатурной модели ИТС представлена на рисунке 5.

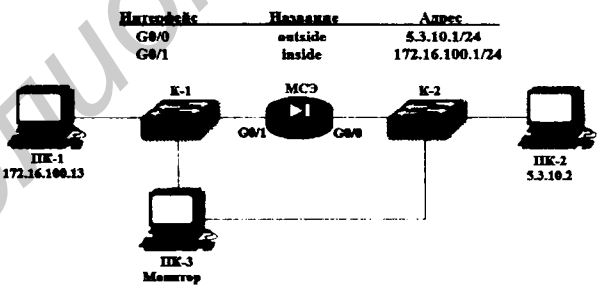


Рисунок 5 – Рабочая схема полунатурной модели ИТС

Схема полунатурной модели ИТС включает в себя персональный компьютер ПК-1, играющий роль получателя; коммутатор внутренней сети К-1, который соединяет ПК-1 с МСЭ через внутренний интерфейс (G0/1); персональный компьютер ПК-3, играющий роль монитора; межсетевой экран

Cisco ASA 5520; коммутатор внешней сети К-2, который соединяет ПК-2 с МСЭ через внешний интерфейс (G0/0) и персональный компьютер ПК-2, играющий роль источника трафика. В ПК-2 установлен программный генератор пакетов CPB, в ПК-1 и ПК-3 установлена программа Wireshark, которая выполняет функцию сниффера, показывает и сохраняет все пакеты и их параметры. В коммутаторах К-1 и К-2 включена функция SPAN, которая обеспечивает копирование всех пакетов, проходящих через определенный интерфейс в указанный интерфейс.

Экспериментальные исследования характеристик МСЭ проводились по следующему сценарию:

1) для каждой из 6 исследуемых функций производилось конфигурирование генератора пакетов таким образом, чтобы в нём формировался трафик определённого протокола, содержащий как правильные, так и ложные пакеты для исследуемой функции контроля;

2) правила МСЭ и его интерфейсы настраивались таким образом, чтобы активизировалась только одна исследуемая функция проверки, а остальные функции были бы заглушены;

3) в течение каждых 30 с генерировались потоки правильных и ложных пакетов с последовательным изменением длин пакетов в диапазоне от 100 до 1500 байт и интенсивностью их поступления в диапазоне от 1000 до 4000 пакет/с;

4) осуществлялась регистрация моментов времени поступления пакетов в МСЭ и моментов их отправки из МСЭ;

5) осуществлялась обработка полученных результатов и расчёт среднего времени выполнения выбранной функции контроля пакетов в МСЭ.

Для задания модели потока атак на МСЭ проведен анализ структуры пакетов исследуемых протоколов и содержания полей их заголовков. Установлено, что для задания потока атак для исследования функций контроля целостности, трансляции адреса и управления доступом необходимо использовать пакеты протокола ICMP, а для исследования функций ведения таблицы соединений и инспектора состояний - пакеты протокола TCP.

Время выполнения функций трансляции адреса, ведения таблицы соединения и управления доступом зависит от числа входов соответствующих таблиц, а время выполнения функций контроля целостности, проверки контента и инспектора состояний зависит от длины проверяемого пакета, т.е.

$$t_j = F_j(k) \quad \text{и} \quad t_j = F_j(L). \qquad (2)$$

где j – функция проверки,

k – количество входов таблицы,

L – длина пакета.

Так как вид функций (2) является неизвестным, они также определялись в процессе моделирования.

В результате проведенного моделирования получены значения времени и соответственно интенсивности обслуживания для каждой из функций МСЭ, которые представлены в таблице 1.

Таблица 1 – Время обработки и интенсивность обслуживания функций МСЭ

№	Наименование функции	t_i (мкс)	μ_i
1	Контроль целостности	1,133	$883 \cdot 10^3$
2	Трансляция адресов	12,5	$80 \cdot 10^3$
3	Ведение таблицы соединения	1,256	$679 \cdot 10^3$
4	Управление доступом	6,00	$167 \cdot 10^3$
5	Инспектор состояния	1,338	$747 \cdot 10^3$
6	Проверка контента	5,42	$190{,}84 \cdot 10^3$

Как было определено, параметрами адаптивного управления МСЭ являются вероятность его блокировки в зависимости от нагрузки λ, числа включенных в обработку на МСЭ функций контроля, распределения функций контроля по двум МСЭ, образующим ДМЗ.

Количество вариантов перегруппирования перемененных функций в таблице 1 равно

$$N = \sum_{i=1}^{3} C_6^i = 41.$$

Однако проведенный анализ алгоритмов выполнения функций проверки показал, что между ними существует определённая зависимость. Так, функции ведения таблицы соединения и управления доступом взаимно влияют друг на друга, а функции инспектора состояния и ведения таблицы соединения связаны друг с другом. Таким образом, для осуществления адаптации перегруппирование этих функций нельзя осуществлять в произвольном порядке. Так как функция ведения таблицы соединения связана с функциями управления доступом и инспектора состояния, то при осуществлении адаптации они всегда должны быть вместе. Остальные функции не связаны друг с другом и могут работать автономно. С учетом вышеизложенного в таблице 2 приведены варианты возможного перегруппирования функций между двумя МСЭ.

Таблица 2 – Варианты возможного группирования функций между двумя МСЭ

№ варианта	Функции МСЭ-1	Функции МСЭ-2
1	1,2,3,4,5	6
2	2,3,4,5	1,6
3	1,3,4,5	2,6
4	3,4,5	1,2,6
5	3,4,5,6	1,2
6	1,2	3,4,5,6

В таблицах 3 и 4 представлены значения интенсивности обслуживания МСЭ в зависимости от включенных в обработку функций.

Таблица 3 – Интенсивности обслуживания МСЭ в зависимости от j

№ варианта	t_j (мкс)	μ_j
1	22,228	44988
2	21,094	47407
3	9,728	102796
4	8,594	116360
5	13,834	72286

Таблица 4 – Интенсивности обслуживания МСЭ в зависимости от k

№ варианта	t_k (мкс)	μ_k
1	5,42	19084
2	6,36	15689
3	17,74	5637
4	18,87	5298
5	13,63	7335

Полученные вероятности блокировки МСЭ в конфигурации с ДМЗ представлены на рисунке 6.

Как следует из полученных графиков, самым худшим вариантом с точки зрения пропускной способности является вариант 1, а самым лучшим – вариант 5. На рисунке 7 показаны графики вероятностей блокировки МСЭ с адаптивным управлением и зонами адаптации. Анализ результатов имитационного моделирования процессов защиты от сетевых атак с использованием МСЭ Cisco ASA 5520, образующих демилитаризованную зону, показывает следующее.

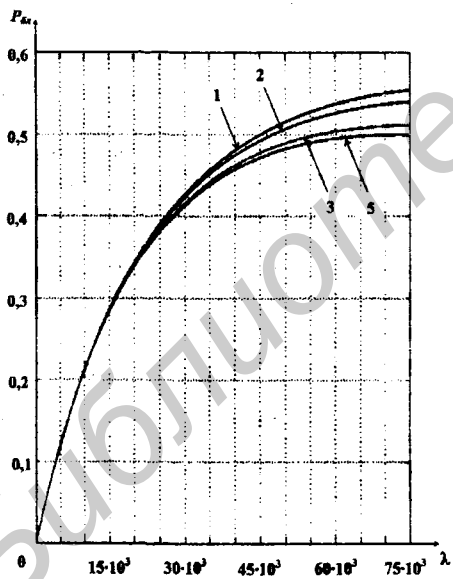


Рисунок 6 – График вероятностей блокировки сдвоенного МСЭ

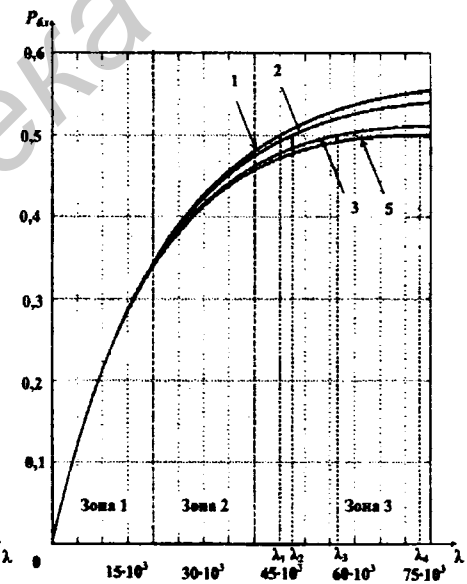


Рисунок 7 – Графики вероятностей блокировки сдвоенного МСЭ с адаптивным управлением

При входящей нагрузке λ, сравнимой с интенсивностью обслуживания потока пакетов μ_j и μ_k, вероятность блокировки практически не зависит от перераспределения функций между МСЭ-1 и МСЭ-2. В данном случае это интервал $0 < \lambda < 20 \cdot 10^3$ (зона 1 на рисунке 7). Вместе с тем МСЭ-1, являясь внешним средством защиты, должен обеспечивать защиту ЛВС от атак извне, и следовательно, в исходном состоянии выполнять функции 1 – 5. Внутренний МСЭ (МСЭ-2) служит для контроля информационных потоков между внутренними сетями и поэтому выполнение функции проверки контента (функция 6) в исходном состоянии для него является наиболее приемлемым. Поэтому начальным адаптивным вариантом распределения функций между МСЭ-1 и МСЭ-2 при организации демилитаризованный зоны является вариант, когда МСЭ-1 выполняет функции 1 – 5, а МСЭ-2 осуществляет проверку контента пакетов, т.е. выполняет функцию 6. Вариант с распределением функций j=5, k=1 является наиболее предпочтительным при нагрузке в переделах от $20 \cdot 10^3 \le \lambda \le 40 \cdot 10^3$ (зона 2 на рис. 7), когда вероятность блокировки обслуживания $P_{бл} \le 0{,}5$.

Приняв вероятность $P_{бл} \le 0{,}5$ в качестве нормы, видим, что в интервале $40 \cdot 10^3 < \lambda < 75 \cdot 10^3$ необходимо адаптировать МСЭ, переключая функцию контроля целостности от МСЭ-1 на МСЭ-2. В нашем случае это второй вариант с распределением функций $j = 4$, $k = 2$ (зона 3 на рисунке 7).

Если число заявок в секунду продолжает нарастать, то вероятность блокировки ($P_{бл}$) тоже растет, и при $P_{бл} \ge 0{,}5$ снова необходимо адаптировать МСЭ, переключая функцию трансляции адресов от МСЭ-1 на МСЭ-2, а функцию контроля целостности от МСЭ-2 на МСЭ-1. В нашем случае это третий вариант с распределением функций $j = 4$, $k = 2$.

Если число заявок в секунду достигает $\lambda = 60 \cdot 10^3$, то $P_{бл} \ge 0{,}5$ то МСЭ снова необходимо адаптировать, переключая функцию контроля целостности от МСЭ-1 на МСЭ-2, а функцию проверки контента от МСЭ-2 на МСЭ-1. В нашем случае это четвертый вариант с распределением функций $j = 4$, $k = 2$.

Ввиду того, что процесс перенастройки МСЭ требует некоторых временных затрат, а значения λ_1 и λ_2 достаточно близкие величины, является целесообразным адаптацию МСЭ производить не в четыре, а в три этапа, как это показано на рисунке 8.

На рисунке 8 область адаптации – диапазон значений нагрузки трафика, в котором осуществляется переключение функции от МСЭ-1 на МСЭ-2. Организация области адаптации поясняется следующими отношениями:

$0 < \lambda < \lambda_1 \longrightarrow$ Вариант № 1 (j=5, k=1),

$\lambda_1 \le \lambda < \lambda_3 \longrightarrow$ Вариант № 3 (j=4, k=2),

$\lambda_3 \le \lambda < \lambda_4 \longrightarrow$ Вариант № 5 (j=4, k=2).

$\lambda \ge \lambda_4 \longrightarrow$ Звуковая сигнализация администратору.

(Варианты конфигурации МСЭ-1 и МСЭ-2 приведены в таблице 2).

Как видно на рис. 8, предложенные правила переключения функций проверки в зоне адаптации позволяют в 1,7 раза увеличить пропускную способность МСЭ.

Четвёртая глава посвящена разработке алгоритма адаптивного управления МСЭ и соответствующего ему программного средства. Алгоритм адаптации МСЭ должен выполнять две основные функции:

– контроль трафика, проходящего через МСЭ;

– переключение функций в зоне адаптации МСЭ.

На рисунке 9 представлен алгоритм работы программы адаптации МСЭ в составе ДМЗ.

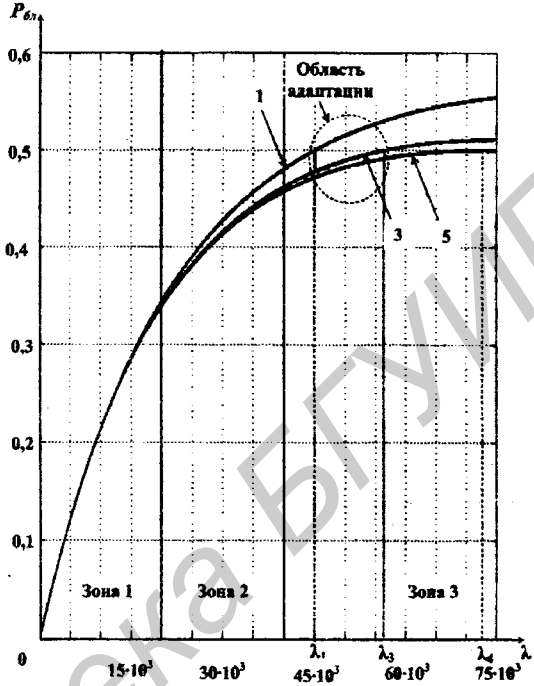


Рисунок 8 – Графики вероятностей блокировки сдвоенного МСЭ с адаптивным управлением

Адаптация МСЭ выполняется переключением определенных функций между МСЭ-1 и МСЭ-2 в зависимости от расчетной величины вероятности блокировки МСЭ, которая зависит от нагрузки поступающего трафика (число заявок в секунду).

Разработанная в соответствии с алгоритмом программа адаптации «MSA» написана в среде «MATLAB» V.7, работает в программной среде Windows и инсталлируется на рабочее место администратора, которое имеет связь с МСЭ.

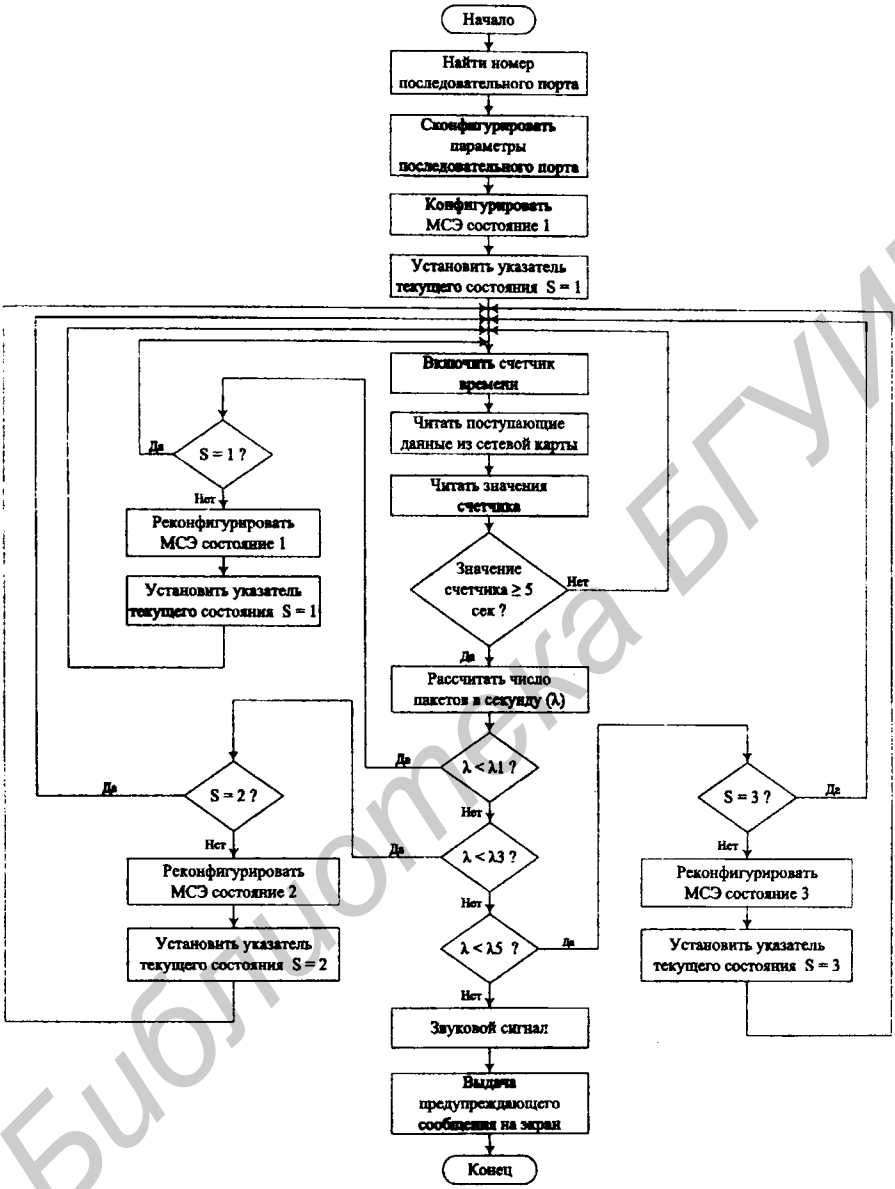


Рисунок 9 – Алгоритм работы программы адаптации МСЭ

Структура программы «MSA» представлена на рисунке 10.

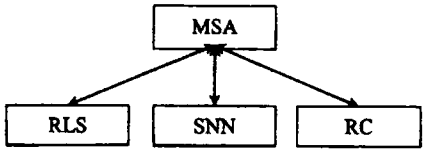


Рисунок 10 – Структура связи между главной программой и подпрограммами адаптации МСЭ

Она включает в себе головную программу «MSA.exe» и три подпрограммы «RLS.exe», «SNN.exe» и «RC.exe».

Программа «MSA» с помощью подпрограмм реализует следующие функции:

– контролирует поступающую нагрузку текущего трафика. Эта функция выполняется подпрограммой «RLS.exe»;

– сравнивает назначения поступающей нагрузки с определенными нормами λ_1, λ_2 и λ_3. Эта функция выполняется подпрограммой «SNN.exe»;

– реконфигурирует МСЭ. Эта функция выполняется подпрограммой «RC.exe»;

– регистрирует данные события (время включения и выключения программы, число, время, нагрузка трафика в момент адаптации и т. д.) в текстовом файле «C:\\ASA_Adaptation\Adaptation_events.doc».

С целью подтверждения разработанных алгоритма и методики адаптивного управления МСЭ, а также проверки полученных при моделировании значений вероятности блокировки МСЭ в зависимости от нагрузки в рамках диссертационных исследований были проведены натурные испытания.

Натурные испытания проводились в условиях обработки трех типов трафиков: поток пакетов без сетевых атак; поток пакетов с сетевой атакой на преодоление функции трансляции адресов; поток пакетов с сетевой атакой на преодоление функции ACL, относящейся к классу атак «отказ в обслуживании». Натурные испытания проводились на сегменте ЛВС БГУИР, отконфигурированном в соответствии со схемой, приведенной на рисунке 11.

Результаты натурных испытаний приведены на графиках (рисунки 12, 13), где рисунок 12 иллюстрирует график расчетной и практической вероятностей блокировки МСЭ, а рисунок 13 иллюстрирует расчетную и практическую вероятности блокировки МСЭ в зоне адаптации.

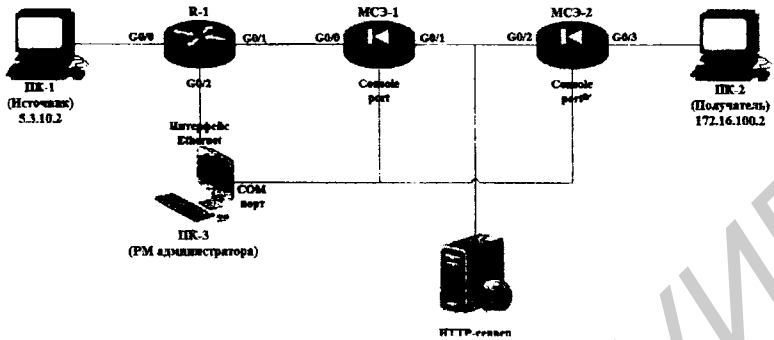


Рисунок 11 – Схема натурных испытаний программы адаптации

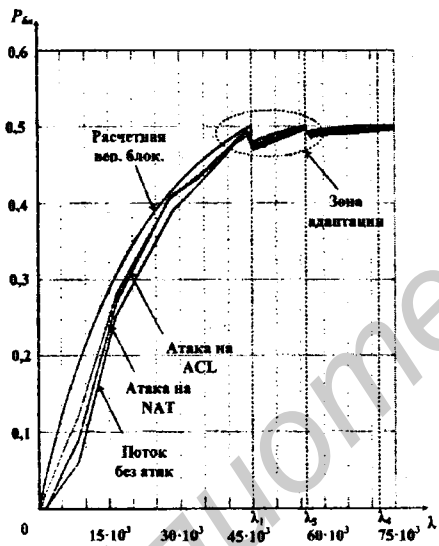


Рисунок 12 – График расчетной и практической вероятностей блокировки МСЭ

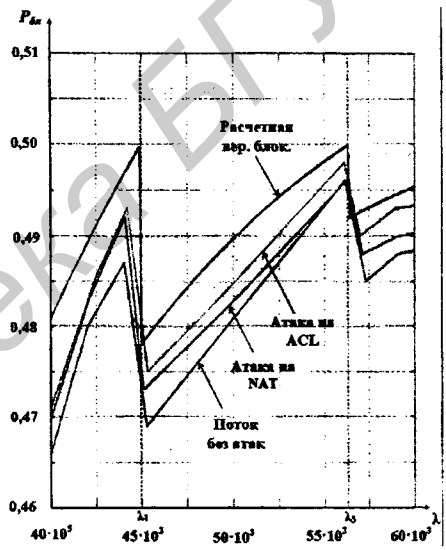


Рисунок 13 – Зона адаптации расчетной и практической вероятностей блокировки МСЭ

На основании проведенных ранее исследований можно сделать вывод, что в общем виде методика адаптации управления МСЭ в условиях реализации демилитаризованной зоны должна иметь следующие основные этапы: анализ МСЭ, определение временных значений, выбор вариантов распределения функций, определение границы зоны адаптации.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Рассмотрены различные классы МСЭ и показано, что существующие средства защиты способны обеспечивать необходимый уровень защищенности ИТС, однако являются транспортно узким местом, что может приводить к блокированию проходящего трафика. Установлено, что известные методы повышения пропускной способности МСЭ заключаются в прямом увеличении производительности его интерфейсов и функций без использования алгоритмов адаптации. Исследованы алгоритмы функционирования МСЭ и установлено, что МСЭ анализирует трафик путем последовательного выполнения функций, включающих в себя контроль целостности, трансляцию адреса, ведение таблицы соединений, управление доступом, инспектирование соединения и проверку контента [1–А, 2–А, 7–А].

2. Исследованы алгоритмы функций, выполняемых МСЭ при проверке пакетов, и получено, что время выполнения функций контроля целостности и инспектирования соединения зависит от длины пакета, а время выполнения функций трансляции адреса, ведения таблицы соединений и управлений доступом зависит от размеров соответствующих таблиц. Разработана модель МСЭ с адаптивным контуром управления. Показано, что модель МСЭ с адаптивным управлением представляет собой модель одноканальной многоэтапной СМО, в которой каждый этап является реализацией соответствующей функции проверки. Установлено, что для определения вероятности блокировки МСЭ необходимо исследовать зависимость интенсивности обслуживания пакетов от числа задействованных функций проверки. Разработана схема контура адаптации МСЭ с учетом архитектуры защищенной ИТС, в структуре которой присутствует демилитаризованная зона. Для разработанного контура адаптации получены математические выражения по определению вероятности его блокировки в зависимости от комбинации распределения функций и поступающей нагрузки [3–А, 4–А, 6–А].

3. В качестве концептуальной основы исследования интенсивности обслуживания пакетов от числа задействованных функций проверки предложена полунатурная модель ИТС. Разработана рабочая схема полунатурной модели ИТС и сценарий экспериментальных исследований характеристик МСЭ. Сформированы тесты для задания потоков атак на МСЭ, настройки коммутаторов и интерфейсов МСЭ, конфигурирования МСЭ применительно к каждой функции проверки пакетов. Для задания модели потока атак на МСЭ проведен анализ структуры пакетов исследуемых протоколов и содержания полей их заголовков. Установлено, что формирование потока атак для исследования функций контроля целостности, трансляции адреса и управления доступом необходимо осуществлять с использованием пакетов протокола ICMP, а для исследования функций ведения

таблицы соединений и инспектора состояний – с использованием пакетов протокола TCP [4–А, 6–А, 8–А, 10–А].

4. На основе проведенных исследований определен вид функций времени обслуживания в зависимости от объемов таблиц и размера пакетов для каждой функции МСЭ. Осуществлен поиск и проведено обоснование наиболее предпочтительных вариантов распределения функций между МСЭ, образующих демилитаризованную зону. Установлена область реконфигурирования МСЭ, называемая зоной адаптации, и получены отношения, описывающие правила перераспределения функций проверки между МСЭ. Показано, что реализация правил переключения функций в зоне адаптации позволяет в 1,7 увеличить пропускную способность МСЭ для заданной вероятности его блокировки 0,5 [5–А, 9–А].

5. Разработана методика адаптивного управления МСЭ, образующих демилитаризованную зону, основанная на анализе функционального состава МСЭ, определении временных значений выполнения функций проверки, определении границ области адаптации и выборе необходимых точек переключения функций. Предложено определять временные значения выполнения функций проверки на полунатурной модели ИТС с заданием потока пакетов, в котором 50 % пакетов относятся к потоку атак, что позволяет получить значения интенсивности обслуживания конкретной исследуемой функции проверки [5–А].

Рекомендации по практическому использованию результатов

1. Разработан алгоритм программного средства адаптации МСЭ, предусматривающий контроль проходящего трафика и переключение функций в зоне адаптации МСЭ. В алгоритме предусмотрена установка и смена значений переменных, влияющих на процесс адаптации МСЭ, а именно: интервала контроля проходящего трафика (в секундах) и величин нагрузки трафика (в пакетах в секунду) для каждой точки переключения функций. Разработано программное средство адаптации, функционирующее в среде Windows, которое устанавливается на рабочее место администратора и управляет работой МСЭ. Использование программного средства адаптации позволяет в 1,7 увеличить пропускную способность МСЭ для заданной вероятности его блокировки 0,5.

2. Проведены экспериментальные исследования адаптивного контура управления МСЭ, образующих демилитаризованную зону, на выделенном сегменте ЛВС БГУИР при поступлении различных видов трафика: без сетевых атак, с атакой на NAT, с атакой на ACL. Получено, что результаты экспериментальных исследований хорошо согласуются с теоретическими расчетами и имеют расхождение от 0,5 % до 1 %, что свидетельствует о перспективности использования методики адаптивного управления для различных классов МСЭ.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в научных рецензируемых изданиях

1–А. Мохаммед, Ф.О. Межсетевые экраны / Ф.О. Мохаммед // Доклады БГУИР. – 2009. – № 5 (43). – С. 70–76.

2–А. Мохаммед, Ф.О. Методы использования механизма поиска обратного маршрута для защиты локальных сетей от атаки спуфинга / М.Н. Бобов, Ф.О. Мохаммед // Доклады БГУИР. – 2010. – № 5 (51). – С. 72–75.

3–А. Мохаммед, Ф.О. Реализация функции контроля соединения в межсетевом экране / М.Н. Бобов, Ф.О. Мохаммед // Доклады БГУИР. – 2011. – № 5 (59). – С. 83–87.

4–А. Мохаммед, Ф.О. Оценка влияния функции контроля соединения на пропускную способность межсетевого экрана / М.Н. Бобов, Ф.О. Мохаммед // Доклады БГУИР. – 2011. – № 6 (60). – С. 44–48.

5–А. Мохаммед, Ф. О. Адаптивное управление межсетевым экраном / М.Н. Бобов, Ф.О. Мохаммед // Доклады БГУИР. – 2012. – №3 (65). – С. 5–11.

Материалы конференций

6–А. Мохаммед, Ф.О. Мониторинг безопасности в информационных системах Web-сервисной архитектуры / М.Н. Бобов, Ф.О. Мохаммед // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: тез. докл. Междунар. науч.-техн. семинара, Браслав, 20–24 сент. 2010 г. / БГУИР. – Минск, 2010. – С. 70–73.

7–А. Мохаммед, Ф.О. Принципы функционирования межсетевых экранов / М.Н. Бобов, Ф.О. Мохаммед // Теоретические и прикладные проблемы информационной безопасности в Республике Беларусь: Минск, 31 марта 2010 г. / Академия МВД Респ. Беларусь. – Минск, 2011. – С. 64–69.

8–А. Мохаммед, Ф.О. Защита TCP-пакетов на основе случайной замены их порядковых номеров в межсетевом экране / Ф.О. Мохаммед // Технические средства защиты информации: тез. докл. IX Белорус.-российск. науч.-техн. конф. (Минск, 28–29 июня 2011 г.) / БГУИР. – Минск, 2011. – С. 45–46.

9–А. Мохаммед, Ф.О. Обеспечение фильтрации Java-аплетов ActiveX-скриптов в межсетевом экране / Ф.О. Мохаммед // Технические средства защиты информации: тез. докл. IX Белорус.-российск. науч.-техн. конф. (Минск, 28–29 июня 2011 г.) / БГУИР. – Минск, 2011. – С. 46.

10–А. Мохаммед, Ф.О. Инспектирование состояния соединений в межсетевом экране / М.Н. Бобов, Ф.О. Мохаммед // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы докл. Междунар. науч.-техн. семинара (Минск, янв.–дек. 2011 г.) / БГУИР. – Минск, 2011. – С. 11–16.

РЭЗЮМЭ

Махамед Файсал Асман Махамед

Адаптыўнае кіраванне міжсеткавых экранаў у інфатэлекамунікацыях

Ключавыя словы: міжсеткавы экран, функцыі кантролю пакетаў, прапускная здольнасць, зона адаптацыі, адаптыўнае кіраванне.

Мэта працы: распрацоўка алгарытмаў адаптыўнага кіравання міжсеткавым экранаваннем інфармацыйна-тэлекамунікацыйных сетак ва ўмовах уздзеяння сеткавых нападаў.

Метады даследавання: мадэляванне паводзін міжсеткавых экранаў, якія ўтвараюць дэмілітарызаваную зону ва ўмовах уздзеяння сеткавых нападаў у паступаючым трафіку на полунатуральнай мадэлі.

Атрыманыя вынікі і іх навізна: даследаваны працэсы праверкі трафіку ў МСЭ, якія ўтвараюць дэмілітарызаваную зону і ўсталявана, што час выканання функцый кантролю цэласнасці і інспектаванні стану залежыць ад даўжыні правяраемых пакетаў, а час выканання функцый трансляцыі адрасу, кантролю злучэння і кіравання доступам залежыць ад памераў адпаведных табліц. Вызначаны найбольш пераважныя варыянты пераразмеркавання функцый праверкі трафіку паміж МСЭ на мяжы дэмілітарызаванай зоны за кошт арганізацыі вобласці адаптацыі і выбару неабходных кропак пераключэння функцый, якія дазваляюць у 1,7 разоў павялічыць прапускную здольнасць МСЭ. Распрацавана методыка адаптыўнага кіравання МСЭ, заснаваная на аналізе функцыянальнага складу МСЭ, вызначэнні часавых значэнняў выканання функцый праверкі, вызначэнні меж вобласці адаптацыі і выбары неабходных кропак пераключэння функцый, што дазволіла распрацаваць праграмны сродак адаптыўнага кіравання любымі тыпамі МСЭ.

Ступень выкарыстання: скарыстаны пры стварэнні аўтаматызаваных інфармацыйных сістэм у ААТ «АГАТ – сістэмы кіравання» г. Мінск і ўкаранёныя ў навучальны працэс у Беларускім дзяржаўным універсітэце інфарматыкі і радыёэлектронікі.

Вобласць ужывання: сістэмы абароны інфармацыі ў інфакамунікацыйных сетках.

РЕЗЮМЕ

Мохаммед Файсал Осман Мохаммед

Адаптивное управление межсетевыми экранами в инфотелекоммуникациях

Ключевые слова: межсетевой экран, функции контроля пакетов, пропускная способность, зона адаптации, адаптивное управление.

Цель работы: разработка алгоритмов адаптивного управления межсетевым экранированием информационно-телекоммуникационных сетей в условиях воздействия сетевых атак.

Методы исследования: моделирование поведения межсетевых экранов, образующих демилитаризованную зону в условиях воздействия сетевых атак в поступающем трафике на полунатурной модели.

Полученные результаты и их новизна: Исследованы процессы проверки трафика в МСЭ, образующих демилитаризованную зону, и установлено, что время выполнения функций контроля целостности и инспектирования состояния зависит от длины проверяемых пакетов, а время выполнения функций трансляции адреса, контроля соединения и управления доступом зависит от размеров соответствующих таблиц. Определены наиболее предпочтительные варианты перераспределения функций проверки трафика между МСЭ на границе демилитаризованной зоны за счёт организации области адаптации и выбора необходимых точек переключения функций, позволяющие в 1,7 раза увеличить пропускную способность МСЭ. Разработана методика адаптивного управления МСЭ, основанная на анализе функционального состава МСЭ, определении временных значений выполнения функций проверки, определении границ области адаптации и выборе необходимых точек переключения функций, что позволило разработать программное средство адаптивного управления любыми типами МСЭ.

Степень использования: использованы при создании автоматизированных информационных систем в ОАО «АГАТ – системы управления» г. Минск и внедрены в учебный процесс в Белорусском государственном университете информатики и радиоэлектроники.

Область применения: системы защиты информации в инфокоммуникационных сетях.

SUMMAY

Mohammed Faisal Osman Mohammed

Adaptive control of firewalls in infotelecommunications

Keywords: firewall, packet processing functions, throughput, adaptation zone, adaptive management.

Objective: algorithms development for firewall screening adaptive control of information and telecommunications network under the impact of network attacks.

Research Methods: simulation of firewall's behavior that forming a demilitarized zone under the impact of incoming traffic network attacks in the scaled-down model.

Obtained results and their novelty: the traffic checking processes in firewall that forms and configures a demilitarized zone are found that the processing time of initial checking and inspection engine functions depends on the size of packet under check, and the processing time of the xlate lookup (network address translation), connection lookup and access list lookup functions depends on the size of the corresponded table. It is identified the most preferred choice to distribute the checking traffic functions between the two firewalls at the border of the demilitarized zone, by calculating the adaptation zone and selecting the required functions of the switching points, allows 1.7 times more firewall's bandwidth. A method for firewall adaptive control, based on analyzing the functional of the firewall, defining the processing times for the checking functions, defining the boundaries of the adaptation zone and selecting the required functions switching points, that allowed to development adaptive software tool to control any type of firewall is prepared.

Extent of Usage: the study has been used for constructing automated information systems at JSC «AGAT – Control Systems» Minsk city, and introduced into the curriculum of the Belarusian State University of Informatics and Radio Electronics.

Application field: information protection systems applied in information and communication networks.

Научное издание

МОХАММЕД ФАЙСАЛ ОСМАН МОХАММЕД

АДАПТИВНОЕ УПРАВЛЕНИЕ МЕЖСЕТЕВЫМИ ЭКРАНАМИ В ИНФОТЕЛЕКОММУНИКАЦИЯХ

Специальность – Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени кандидата технических наук

Подписано в печать 25.04.2012.	Формат 60×84 1/16.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л. 1,65.
Уч.-изд. л. 1,4.	Тираж 60 экз.	Заказ 199.

Издатель и полиграфическое исполнение: учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2012.

220013, Минск, П. Бровки, 6