На правах рукописи

ЛАПИН Андрей Анатольевич

ОБЕСПЕЧЕНИЕ СКРЫТНОЙ ФИЛЬТРАЦИИ ТРАФИКА СЕТЕВЫМИ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург - 2007

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования «Санкт-Петербургский государственный политехнический университет»

Научный руководитель:

Доктор технических наук, профессор Заборовский Владимир Сергеевич

Официальные оппоненты:

доктор технических наук, профессор Макаров Сергей Борисович

кандидат технических наук Скиба Владимир Юрьевич

Ведущая организация:

Институт проблем информационной безопасности МГУ им. М.В. Ломоносова (ИПИБ МГУ) г. Москва

Защита состоится «____ » _____2007 г. в ____ часов на заседании диссертационного совета Д 212.229.27 при ГОУ ВПО “Санкт-Петербургский государственный политехнический университет” по адресу 195251, Санкт-Петербург, ул. Политехническая 29, ауд. 175 главного здания.

С диссертацией можно ознакомиться в фундаментальной библиотеке ГОУ ВПО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан «____»_____ 2007 г.

Ученый секретарь диссертационного совета Платонов В.В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

Средства обеспечения информационной безопасности являются важнейшей составляющей современных информационных систем. Повсеместное внедрение персональных компьютеров, локальных и глобальных вычислительных сетей, связанных в единую инфраструктуру передачи данных, обостряет проблему использования сетевых средств защиты информации. Для обеспечения информационной безопасности в современных высокоскоростных компьютерных сетях широкое распространение получили методы защиты, использующие межсетевые экраны (МЭ). Основная функция МЭ реализуется на основе контроля параметров заголовков сетевых пакетов или состояния виртуальных соединений с целью принятия решения об их пропуске или удалении.

Исследованию проблем обеспечения безопасности информации, выработки новых подходов к построению защищенных информационных систем и способов организации средств защиты в компьютерных сетях посвящены работы А.Я. Городецкого, В.С. Заборовского, Д.П. Зегжды, Л.М. Ухлинова, А.Ю. Щербакова и других.

Одной из угроз, рассматриваемой при создании информационных систем, является несанкционированное воздействие на устройства защиты, в частности атаки на МЭ. Для отражения угроз такого типа в компьютерных сетях применяется режим скрытного функционирования устройств защиты. Применимо к МЭ скрытность функционирования достигается за счет того, что фильтрующие интерфейсы не имеют сетевых (IP–адресов) и физических (MAC) адресов. Отсутствие адресов позволяет защитить МЭ от несанкционированных воздействий, основанных на использовании адресной информации. При этом локализация МЭ возможна по косвенным признакам, связанным с анализом особенностей их функционирования. К таким признакам, например, относятся статистические характеристики потоков пакетов, которые проходят через МЭ и доступны для непосредственного измерения. Более высокого уровня безопасности МЭ можно

достичь, если в процессе работы будет обеспечиваться скрытность его функционирования не только на уровне адресной информации, но и на уровне доступных для измерения статистических характеристик сетевых процессов (трафика).

Реализация такого режима функционирования МЭ определяется возможностями влияния на статистические и динамические характеристики сетевых процессов, связанных с организацией виртуальных транспортных TCP соединений. Во многих исследованиях для описания свойств сетевых процессов предлагается использовать характеристики статистического самоподобия или масштабной инвариантности трафика, которые в современной литературе принято называть фрактальными. Одной из таких характеристик является показатель Херста H, с помощью которого описывается отличная от марковских процессов статистическая зависимость между отсчетами значений сетевого трафика в различные моменты времени. Из результатов большого числа исследований известно, что для современных компьютерных сетей значение H соответствует диапазону 0,6÷0,8. Это обстоятельство указывает на то, что для описания сетевых процессов непосредственное использование моделей, разработанных в рамках теории систем массового обслуживания (СМО), невозможно, поскольку для них H=0,5.

Актуальной научно-технической задачей, от решения которой зависит возможность реализации режима скрытной фильтрации, является разработка моделей трафика, позволяющих выбирать параметры МЭ, при которых значение H для потока пакетов на входе и на выходе МЭ остается неизменным. Решение этой задачи позволит идентифицировать фрактальные характеристики трафика и осуществить выбор параметров МЭ, при которых обеспечивается его функционирование в скрытном режиме, что повышает надежность функционирования и уровень безопасности информационных систем в целом.

Цель диссертации

Целью диссертации является обеспечение скрытной фильтрации трафика сетевыми средствами защиты информации на основе разработки и исследования

моделей сетевых процессов, используемых для идентификации фрактальных характеристик трафика и позволяющих выбрать параметры МЭ, при которых обеспечивается его функционирование в режиме скрытной фильтрации.

Для достижения поставленной цели решались следующие основные задачи:

1. Разработка методов описания процессов в компьютерных сетях, используемых для построения моделей трафика с учетом свойств масштабной инвариантности.
2. Разработка модели транспортного TCP соединения, используемой для идентификации параметров состояния сетевой среды и исследования влияния алгоритма управления передачей пакетов на фрактальные характеристики трафика.
3. Разработка метода выбора параметров МЭ, для реализации режима полной скрытной фильтрации с учетом фрактальных характеристик трафика.
4. Разработка архитектуры программного комплекса идентификации трафика и анализа регистрируемой информации МЭ с целью выбора параметров его настройки.

Методы исследований

В работе использованы методы статистической обработки данных, теории случайных процессов, математического моделирования, процедурного и объектно-ориентированного программирования.

Основные научные результаты и их новизна

В диссертации получены следующие основные научные и практические результаты:

1. Предложен метод описания процессов на уровне виртуальных транспортных соединений с учетом фрактальных свойств потока пакетов.
2. Разработана модель TCP соединения, которая позволяет рассчитывать статистические характеристики временных задержек передачи данных и

определить причины возникновения фрактальных свойств сетевых процессов.

3. Разработан метод параметрической настройки МЭ, осуществляющих фильтрацию трафика в скрытном режиме, с учетом фрактальных характеристик трафика.
4. Разработана архитектура и реализованы основные компоненты программного комплекса идентификации и анализа регистрируемой информации для обеспечения скрытной фильтрации трафика сетевыми средствами защиты, в частности МЭ.

Положения, выносимые на защиту

На основе результатов диссертационного исследования сформулированы следующие положения, выносимые на защиту:

1. Модель транспортного TCP соединения, которая позволяет рассчитывать статистические характеристики временных задержек передачи данных и определить причину возникновения фрактальных свойств сетевых процессов.
2. Метод выбора параметров МЭ, для реализации фильтрации трафика в скрытном режиме с учетом фрактальных характеристик сетевых потоков.
3. Архитектура программных средств идентификации и анализа регистрируемой информации МЭ, а также структура используемой базы данных, соответствующая иерархической связанности сетевых протоколов.

Практическая ценность работы заключается в том, что разработанные модели и методы описания процессов возможно использовать как для создания сетевых средств защиты информации, так и для оценки влияния фрактальных свойств процессов на производительность протоколов транспортного уровня. В основу диссертационной работы положены результаты, полученные автором в период с 2004 по 2007 год, в ходе выполнения научно-исследовательских и опытно-

конструкторских работ на кафедре «Телематика» факультета при ЦНИИ РТК ГОУ ВПО «СПбГПУ» и при разработке программного обеспечения анализа регистрируемых данных МЭ, осуществляющих фильтрацию трафика в скрытном режиме и используемых в Федеральной таможенной службе РФ, Министерстве образования и науки, а также в других учреждениях.

Внедрение результатов

Результаты проведенных исследований нашли практическое применение в разработках, в которых автор принимал личное участие:

1. Разработанное программное обеспечение используется в таможенных органах РФ в рамках проекта «Сопровождение средств сетевой безопасности при интеграции локальных сетей таможенных органов».

2. Разработанные программные средства анализа параметров трафика при использовании МЭ внедрены в эксплуатацию в Федеральной таможенной службе РФ, ФГУ ГНИИ ИТТ «Информика», ОАО «Ленэнерго», правительстве Ленинградской области.

Апробация и публикация результатов работы

Результаты, полученные в диссертационной работе, докладывались на семинаре «Проблемы современных информационно-вычислительных систем» в МГУ им. М.В. Ломоносова, а также на всероссийских и межвузовских научно-технических конференциях. По теме диссертации опубликовано 7 статей, в том числе 2 на международных конференциях.

Структура и объем диссертации

Диссертационная работа общим объемом 153 стр. состоит из введения, четырех глав, заключения и списка литературы (включая 59 рисунков, 3 таблицы и списка литературы из 64 наименований)

СОДЕРЖАНИЕ РАБОТЫ

Во введении показана актуальность темы, сформулирована цель и постановка задачи исследования, перечислены основные научные результаты и положения,

выносимые на защиту, а также представлены сведения о внедрении результатов, апробации, публикациях и дана краткая характеристика содержания работы.

В первой главе рассмотрены угрозы безопасности характерные для современных информационных систем, методы и средства защиты информации в компьютерных сетях и проведен анализ актуальных вопросов, связанных с исследованием сетевых процессов.

Показано, что различные средства защиты информации в компьютерных сетях, такие как системы обнаружения и предотвращения вторжений, виртуальные частные сети, серверы-посредники, способы трансляции адресов и межсетевые экраны условно можно разделить на два типа: устройства, при функционировании которых существенно используется информация об адресах сетевых интерфейсов и устройства, функционирование которых не связано с использованием этой информации. Средства защиты второго типа, в частности МЭ, могут функционировать в скрытном режиме. Отсутствие адресов позволяет использовать для защиты таких устройств специальные высокоэффективные средства и методы, среди которых особо следует выделить те, которые обеспечивают невозможность их локализации в сети по характеристикам процессов, доступных для измерений. В этой главе определен круг научно-технических задач, решение которых позволяет обеспечить скрытность функционирования МЭ не только на уровне адресов, но и на уровне доступных для измерения статистических характеристик трафика.

Отмечается, что при решении сформулированных задач важно учитывать фрактальные свойства сетевых процессов, которые проявляются в виде свойства самоподобия корреляционных характеристик трафика на разных масштабах измерения, т.е. для различных интервалов времени, в течение которых фиксируются результаты измерений, связанные с количеством пакетов, количеством байт, интервалами времени между поступлением пакетов и др. Показано, что для создания моделей, учитывающих фрактальные свойства трафика, можно использовать специальные решения в классе задач СМО.

При этом среди факторов, влияющих на результаты измерений и синтез моделей необходимо учитывать следующие:

- измерения трафика в МЭ изменяют состояния пакетов (TTL, контрольные суммы и др.);
- каждое измерение пакета «возмущает сеть», что оказывает влияние на процессы в сети, добавляя задержки при передаче пакета, и в ряде случаев приводит к появлению фрактальных свойств;
- измеряемые характеристики трафика можно получить на интервале времени, который связан с минимальным размером пакета и временем жизни виртуального TCP соединения.

С учетом отмеченных особенностей для построения моделей сетевых процессов предлагается рассмотрение на различных уровнях.

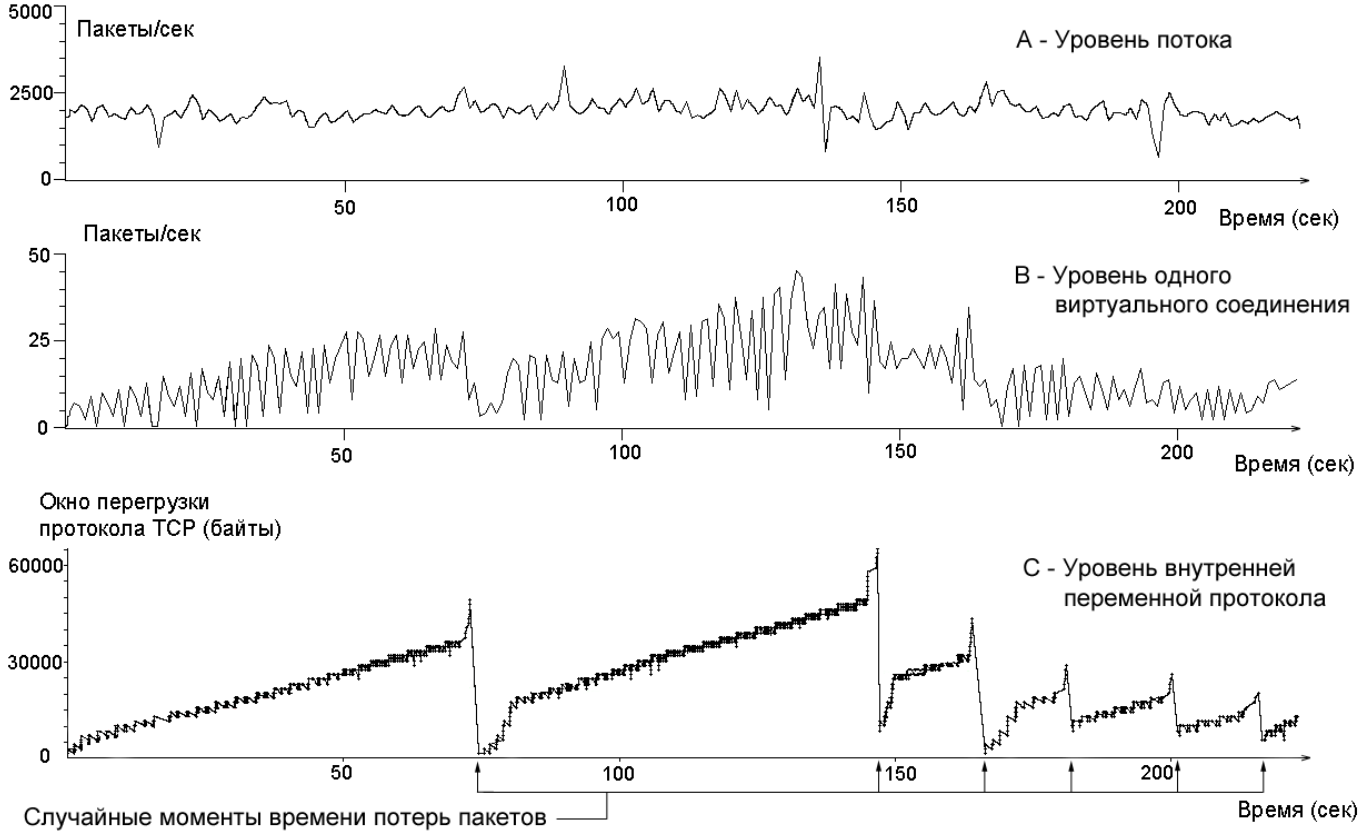

Рис. 1. Уровни рассмотрения процессов, порождающих пакетный трафик в компьютерных сетях

На рис. 1 зависимость A описывает трафик потока, проходящий через сетевой интерфейс МЭ, который формируется как совокупность пакетов от различных

транспортных соединений. В этом потоке возможно выделить отдельное TCP соединение (зависимость B), динамика которого определяется окном перегрузки протокола TCP или внутренней переменной управления передачей для данного соединения, зависящей от случайных моментов времени потерь пакетов (зависимость C).

Из представленных на рис.1 зависимостей следует, что характеристики сетевых процессов имеют разную степень сложности и предсказуемости, связанную с характером «возмущения сети». Для решения сформулированных задач модели сетевых процессов предложено синтезировать на уровне внутренней переменной протокола TCP, изменение которой представлено на рис. 1.C, а свойства определяются характером распределения моментов потерь и повторных передач пакетов.

Во второй главе рассмотрено влияние фрактальных свойств, связанных со свойством статистического самоподобия вторых моментов трафика. Определены количественные и качественные характеристики трафика, при этом модель МЭ представлена в виде СМО с фрактальным входным потоком, а модель транспортного TCP соединения использована для описания его фрактальных свойств.

Показано, что при осуществлении фильтрации пакетного трафика фактором, ограничивающим производительность МЭ, является производительность системы обработки пакетов, функционирующей в соответствии с правилами фильтрации. Для описания интенсивности входного и выходного потока, предложено использовать интегральную характеристику производительности МЭ, измеряемую в количестве пакетов в единицу времени и рассчитанную для фиксированного размера пакетов.

В результате, функционирование МЭ с одним входным и одним выходным интерфейсами может быть представлено в виде СМО типа G/D/1. В условиях высокой интенсивности трафика для описания СМО предложена модель, основанная на диффузионной аппроксимации входного потока G. В этом случае, входной трафик $N(t)$ аппроксимируется выражением $N(t) \approx \lambda t + \sqrt{\lambda} W_H(t)$, где λ – интенсивность, $W_H(t)$ – фрактальное броуновское движение с функцией распределения

$f(w;t) = \frac{1}{t^H \sqrt{2\pi}} e^{-\frac{w^2}{2t^{2H}}}$, где H – показатель Херста. Поскольку производительность центрального процессора МЭ много больше производительности сетевых интерфейсов, т.е. время обработки пакетов является постоянной величиной, в модели МЭ процедура обслуживания D аппроксимируется детерминированным законом. В разработанной модели на рис. 2 приняты следующие обозначения: M – суммарная интенсивность обработки всех TCP соединений (пакет/сек), $\rho = \lambda / M$ – коэффициент использования, q – размер буфера (количество пакетов), C – количество TCP соединений, время существования которых позволяет оценить показатели H, $H_{вх}$ и $H_{вых}$ – показатели Херста на входе и на выходе МЭ для разрешенных TCP соединений, λ_i – интенсивность входного потока для i-го разрешенного TCP соединения, q_i – размер буфера, выделяемый для i-го TCP соединения и m_i – интенсивность обработки i-го TCP соединения.

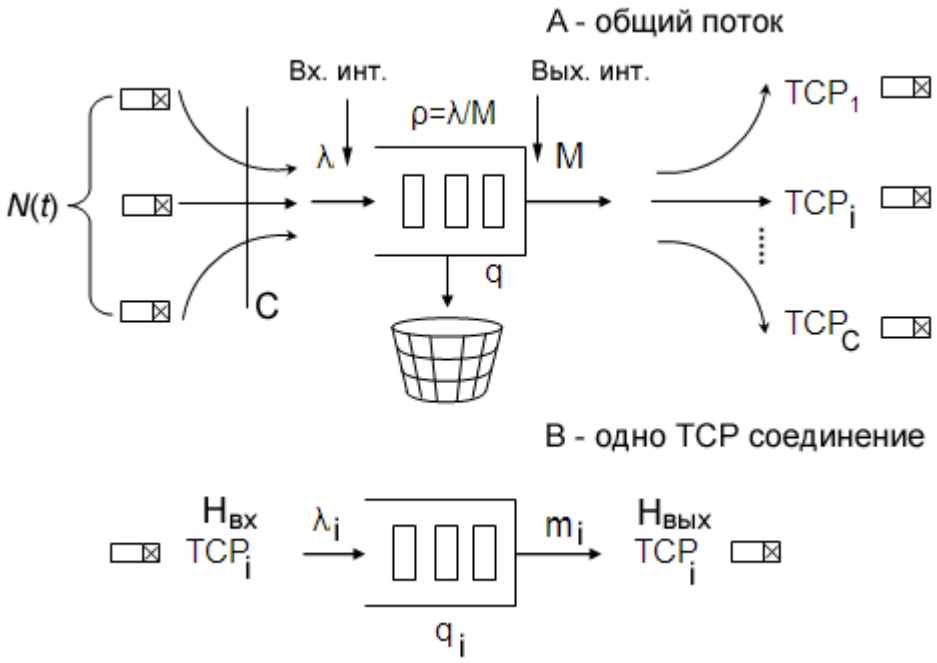

Рис. 2. Обобщенная модель МЭ с двумя физическими интерфейсами:
A – общий поток, B – одно TCP соединение

В случае, когда поток пакетов удовлетворяет разрешающим прохождение пакетов правилам фильтрации, МЭ не осуществляет их удаление, поэтому для характеризации разрешенного TCP соединения возможно использовать результаты

измерений, позволяющие получить оценки статистических моментов: математического ожидания и дисперсии, а также показателя Херста *H*. В отличие от статистических моментов, показатель Херста *H* является инвариантным к масштабу измерения, поэтому обеспечение неизменности этого показателя для потока пакетов разрешенного TCP соединения до и после прохождения МЭ рассматривается как критерий реализации режима скрытной фильтрации.

В терминах, принятых для описания протоколов, разработана модель транспортного TCP соединения, учитывающая изменения состояния сетевой среды. Показано, что потери пакетов являются доминирующим фактором, влияющим на динамику трафика и его статистические свойства. Для оценки влияния потерь в сети между источником и приемником получены гистограммы распределения количества повторных передач пакетов для разрешенных TCP соединений за интервалы агрегирования от 1 до 10 сек. На рис. 3 ось Y соответствует относительной частоте событий повторных передач, а ось X – номеру интервала агрегирования.

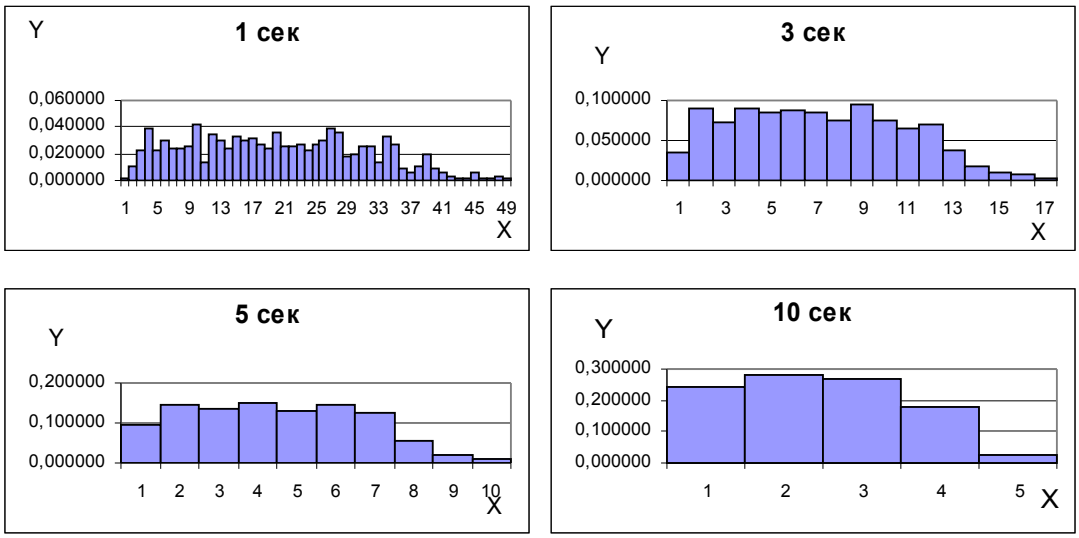

Рис. 3. Гистограммы распределения количества повторных передач протокола TCP для различных интервалов агрегирования измерений

На основании анализа экспериментальных данных показано, что потери пакетов в сетях характеризуются временной однородностью и статистической равномерностью в широком диапазоне интервалов измерений, что позволяет описать

случайный процесс возникновения потерь пакетов равномерным законом распределения.

С учетом влияния потерь пакетов на фрактальные характеристики процессов разработана модель, в которой размер окна перегрузки в режиме быстрой повторной передачи аппроксимируется линейным законом увеличения числа посланных пакетов с интенсивностью один пакет в условную единицу времени до достижения уровня окна приемника. На рис. 4 τ_1, τ_2, τ_3 и т. д. определяют случайные моменты времени наступления потерь пакетов в сети, а величины τ_0, τ_{10}, τ_{20}, τ_{30} и т. д. обозначают возможные моменты времени благоприятных исходов достижения уровня окна приемника в отдельных сериях передачи данных.

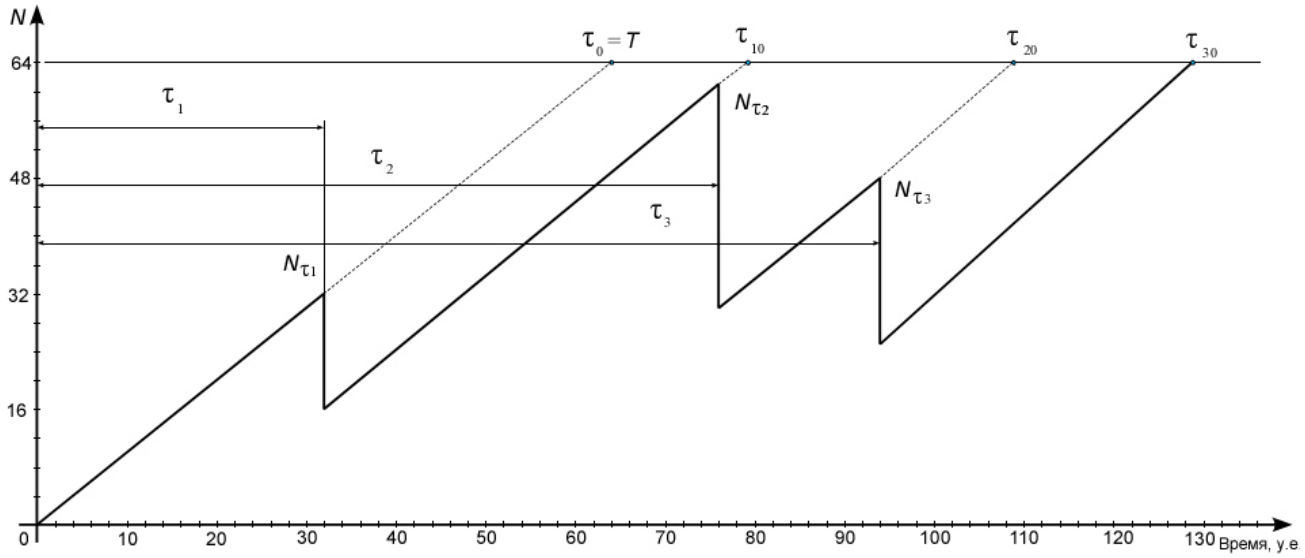

Рис. 4. Эволюция размера окна перегрузки

Выражения, связывающие временные задержки со случайными величинами τ_1, τ_2, τ_3 получены из анализа кусочно-линейной аппроксимации рассматриваемого режима с помощью следующих формул:

$$\tau_{10} = T + \frac{\tau_1}{2}, \quad \tau_{20} = T + \frac{\tau_1}{4} + \frac{\tau_2}{2}, \quad \tau_{30} = T + \frac{\tau_1}{8} + \frac{\tau_2}{4} + \frac{\tau_3}{2},$$

где τ_1 – равномерно распределенная случайная величина с плотностью вероятностей $1/T$; τ_2 – равномерно распределенная случайная величина с плотностью вероятностей $1/(\tau_{10} - \tau_1)$; τ_3 – равномерно распределенная случайная величина с плотностью вероятностей $1/(\tau_{20} - \tau_2)$. Полученные соотношения позволяют

рассчитать зависимость дисперсии от математического ожидания задержек благоприятных исходов, которая имеет нелинейный характер и аппроксимируется формулой: $D(t) = K(t - 64)^{1+\alpha}$ при $t \geq 64$; $D(t)=0$ при $t < 64$; $K=1{,}17$; $\alpha=0{,}52$. Данная зависимость свидетельствует о том, что реакция протокола TCP на потери пакетов в режиме быстрой повторной передачи приводит к коррелированности трафика. Полученная модель позволяет оценить характер влияния свойств протокола TCP на фрактальные характеристики трафика и учесть эти свойства при описании МЭ в режиме скрытной фильтрации.

В третьей главе представлен метод параметрической настройки, обеспечивающий функционирование МЭ в режиме скрытной фильтрации и учитывающий фрактальные свойства процессов.

Метод основан на модели МЭ как СМО типа G/D/1. При обработке входного фрактального процесса сетевым устройством с коэффициентом использования ρ и показателем Херста H существует уровень размера буфера q, при котором не будут происходить отбрасывания пакетов и показатель Херста H на входе и на выходе МЭ сохраняется неизменным. Показано, что в СМО, учитывающих фрактальные свойства сетевых процессов, имеют место повышенные требования к буферу (рис. 5), поэтому для расчета его размера используется соотношение, полученное с учетом диффузионной аппроксимации входного потока заявок. Это соотношение имеет следующий вид: $q = \frac{\rho^{1/2(1-H)}}{(1-\rho)^{H/(1-H)}}$, где q– размер буфера, ρ – коэффициент использования, H – показатель Херста.

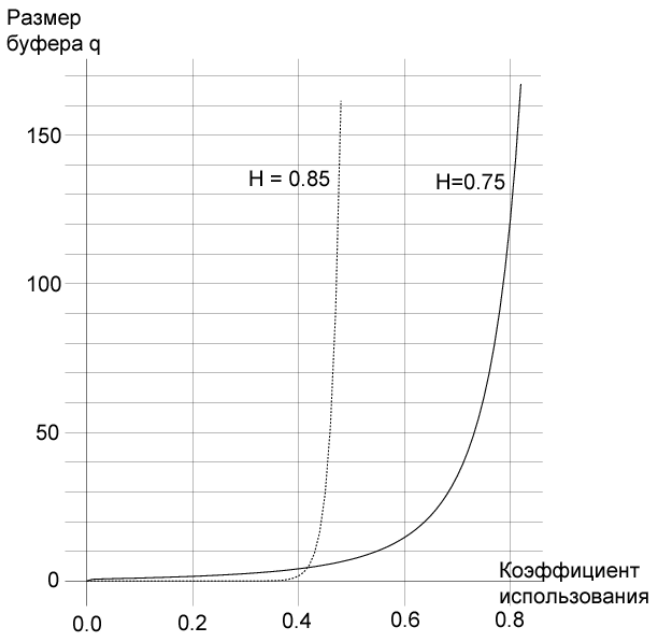

Рис. 5. Зависимость размера буфера от коэффициента использования для модели G/D/1

Учитывая, что трафик, обрабатываемый МЭ, представляет собой совокупность пакетов от множества транспортных соединений, приведенный выше метод расчета размера буфера предлагается применять для отдельных транспортных соединений, разрешенных для прохождения через МЭ. Разработанный метод, основанный на сделанных допущениях, позволяет определить диапазоны значений производительности и размера буферов, при которых МЭ функционирует в режиме скрытной фильтрации.

На рис. 6 приняты следующие обозначения: λ_i – интенсивность нагрузки *i*-го TCP соединения по отношению к пропускной способности физического канала, m_i – производительность обработки *i*-го TCP соединения в МЭ, q_i – размер буфера в пакетах, выделенный для *i*-го соединения.

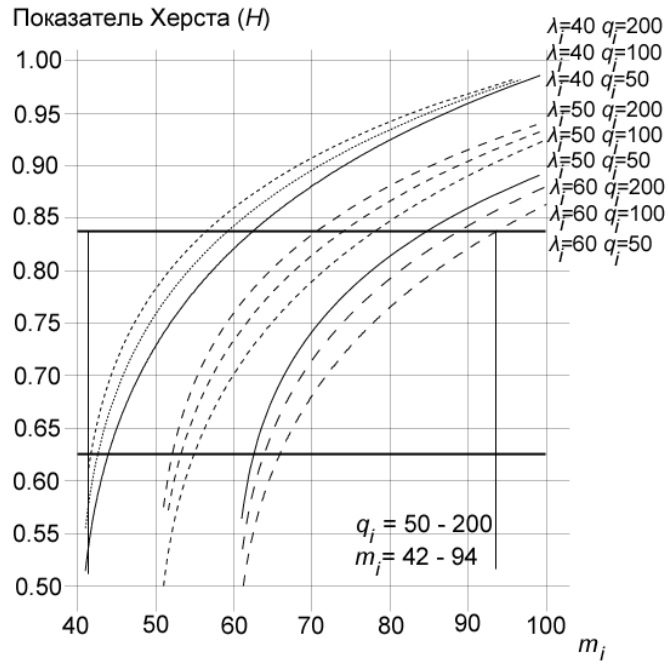

Рис. 6. Зависимость показателя Херста от параметров настройки МЭ

Путем построения зависимостей показателя Херста *H* при различных λ_i, q_i и m_i определены диапазоны значений m и q для *i*-го разрешенного TCP соединения. В частности, для случая с сетевыми интерфейсами МЭ 100 Мбит/сек, режим скрытной фильтрации будет обеспечиваться при q_i = 50-200 пакетов и m_i = 4200-9400 пакетов/сек, что соответствует производительности 6,3-14,1 Мбит/с.

В четвертой главе представлена архитектура и программный комплекс анализа регистрируемой информации МЭ в скрытном режиме. Для идентификации состояния сети используется МЭ в режиме сетевого анализатора. В этом режиме МЭ пропускает и регистрирует все поступающие на его интерфейсы пакеты.

Программный комплекс анализа регистрируемой информации МЭ предназначен для преобразования, хранения, отображения и анализа информации о событиях,

происходящих в процессе работы МЭ, потоковых сессиях и пакетах, поступающих на его фильтрующие интерфейсы. Программный комплекс включает в свой состав две подсистемы: 1) подсистема конвертации и хранения, реализованная в виде сервиса, осуществляющего преобразование бинарных файлов регистрации МЭ и распределение записей о пакетах, сессиях и событиях по таблицам (TCP, UDP, ICMP, IP, MAC, ARP, IPX, СЕССИИ, СОБЫТИЯ) базы данных (БД). Структура БД соответствует рекурсивной вложенности стека протоколов TCP/IP (рис. 7), 2) подсистема визуализации, реализованная в виде графического интерфейса для работы с БД, в котором можно настраивать параметры, производить запросы для анализа и сохранять полученные результаты.

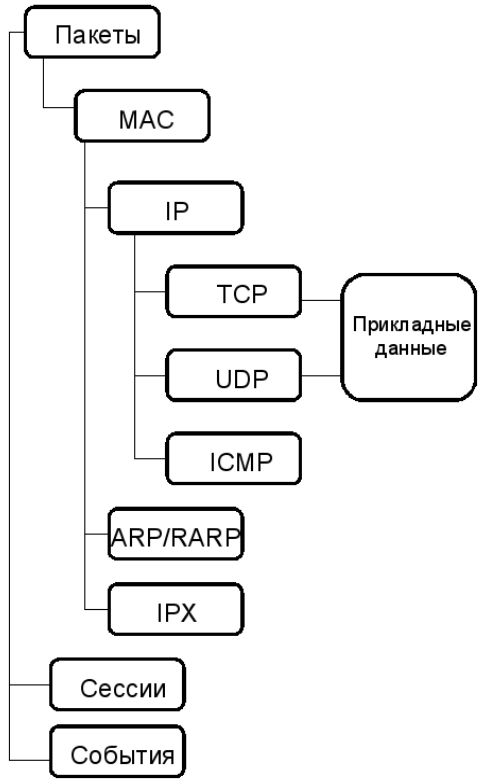

Рис. 7. Структура базы данных

Для организации хранения регистрируемых данных предложен специальный механизм, который позволяет циклически обновлять БД и ограничивать ее объем по количеству хранимых записей или по размеру занимаемого дискового пространства.

Совместное использование МЭ с программным комплексом идентификации и анализа регистрируемой информации позволяет: оценивать характеристики трафика и осуществлять параметрическую настройку МЭ для обеспечения скрытной фильтрации; описывать состояние сетевых потоков с различным уровнем детализации, т.е. агрегировать регистрируемые данные по различным полям заголовков пакетов на 2-7 уровнях модели OSI, а также анализировать их отдельные флаги или поля; обнаруживать паразитный, вирусный и закольцованный трафик, наличие которого увеличивает нагрузку на сетевое оборудование; выявлять в сети вредоносное и несанкционированное программное

обеспечение; перехватывать не зашифрованные прикладные данные; локализовать неисправности или ошибки конфигурации сетевого оборудования.

Основные результаты и выводы

В работе получены следующие основные результаты:

1. Предложен метод описания процессов на уровне виртуальных транспортных соединений с учетом фрактальных свойств потока пакетов.
2. Разработана модель TCP соединения, которая позволяет рассчитывать статистические характеристики временных задержек передачи данных и определить причины возникновения фрактальных свойств сетевых процессов.
3. Разработан метод параметрической настройки МЭ, осуществляющих фильтрацию трафика в скрытном режиме, с учетом фрактальных характеристик трафика.
4. Разработана архитектура и реализованы основные компоненты программного комплекса идентификации и анализа регистрируемой информации для обеспечения скрытной фильтрации трафика сетевыми средствами защиты, в частности МЭ.

Публикации по теме диссертационной работы

1. Vladimir Zaborovsky, Alexsander Gorodetsky, Andrey Lapin. Network Complexity: Cross-Layer Models and Characteristics //The Third Advanced International Conference on Telecommunications. AICT 2007. May, 2007 – Mauritius.
2. Vladimir Zaborovsky, Andrey Lapin, Vladimir Mulukha. Network Traffic Invariant Characteristics: Dynamics and Statistics aspects // The Third International Conference on Wireless and Mobile Communications. ICWMC 2007. March, 2007 - Guadeloupe, French Caribbean.
3. Городецкий А.Я., Заборовский В.С., Лапин А.А. Моделирование самоподобных процессов в компьютерных сетях // Научно-технические ведомости – СПб.: Изд-во СПбГПУ, 2006. № 5. -С.103-107.

4. Лапин А.А. Проблема измерения в компьютерных сетях: исследование и особенности // XXXV Неделя науки СПбГПУ Всероссийская межвузовская научно-техническая конференция студентов и аспирантов, СПб, 2005. -С.137-139.
5. Лапин А.А. Применение и анализ псевдослучайных последовательностей при моделировании процессов в компьютерных сетях // XXXIV Неделя науки СПбГПУ Всероссийская межвузовская научно-техническая конференция студентов и аспирантов, СПб, 2005. -С.178-180.
6. Лапин А.А. Моделирование процессов управления и оценка обработки пакетного трафика в узле сети при использовании «стеллс» - устройств // VI Всероссийская научно-практическая конференция «Теоретические и прикладные вопросы современных информационных технологий», Улан-Удэ, 2005. - С.69-74.
7. Лапин А.А. Методические аспекты использования средств моделирования при исследовании процессов в компьютерных сетях // V Всероссийская научно-практическая конференция «Теоретические и прикладные вопросы современных информационных технологий», Улан-Удэ, 2004. -С.197-202.