На правах рукописи

Мусатов Владислав Константинович

РАЗРАБОТКА МЕТОДА ОЦЕНКИ ПОКАЗАТЕЛЕЙ ПРОИЗВОДИТЕЛЬНОСТИ МЕЖСЕТЕВЫХ ЭКРАНОВ ПРИ ФУНКЦИОНИРОВАНИИ В УСЛОВИЯХ ПРИОРИТИЗАЦИИ ТРАФИКА

Специальность 05.12.13 - Системы, сети и устройства телекоммуникаций

Автореферат

диссертации на соискание ученой степени

кандидата технических наук

Москва – 2018

Работа выполнена в ордена Трудового Красного Знамени федеральном государственном бюджетном образовательном учреждении высшего образования «Московский технический университет связи и информатики» (МТУСИ).

Научный руководитель: **Пшеничников Анатолий Павлович**
кандидат технических наук, профессор.

Официальные оппоненты: **Гайдамака Юлия Васильевна**
доктор физико-математических наук, доцент кафедры прикладной информатики и теории вероятностей Федерального государственного автономного образовательного учреждения высшего образования «Российский университет дружбы народов».

Леваков Андрей Кимович
кандидат технических наук, технический директор Макрорегионального филиала «Центр» Публичного акционерного общества «Ростелеком»

Ведущая организация: Федеральное государственное унитарное предприятие «Центральный научно-исследовательский институт связи»

Защита состоится «28» июня 2018 г. в 13:00 на заседании диссертационного совета по защите докторских и кандидатских диссертаций Д 219.001.04 при ордена Трудового Красного Знамени федеральном государственном бюджетном образовательном учреждении высшего образования «Московский технический университет связи и информатики» по адресу: 111024, Москва, ул. Авиамоторная, д. 8а, МТУСИ, аудитория А-448 (малый зал заседаний учёного совета).
С диссертацией можно ознакомиться в библиотеке МТУСИ и на сайте: http://srd-mtuci.ru/images/Dis-Musatov/dis-Musatov.pdf.

Автореферат разослан «__» _____ 2018 г.

Ученый секретарь
диссертационного совета
к.т.н., доцент Максим Валерьевич Терешонок

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследований. Рост числа мобильных клиентских устройств, желание пользователей постоянно быть на связи, расширение номенклатуры онлайн-сервисов, распространение социальных сетей и видеоконференцсвязи способствуют дальнейшему развитию технологии широкополосного доступа и повышению требований к качеству передачи данных.

Согласно прогнозам ежегодного исследования Cisco Visual Networking Index, с 2016 г. по 2021 г. ожидается рост числа персональных сетевых устройств на человека с 2,3 до 3,5; доля людей, подключенных к глобальной сети, увеличится с 44% до 58% от общего населения планеты, а средняя скорость доступа мобильных устройств вырастет с 6,8 до 20 Мбит/с.

В ответ на подобные вызовы международное сообщество в лице Международного союза электросвязи (МСЭ) в 2015 г. сформировало оперативную исследовательскую группу IMT-2020, которая способствует развитию технологии сетей 5G и концепции Будущих сетей (англ. Future Networks). Эта группа в своём отчёте и рекомендации ITU-R M.2083-0 определила требования к разрабатываемой технологии сетей 5G, например, задержку передачи данных «из конца в конец» («end-to-end») в рамках одного сегмента сети необходимо снизить с 10-ти до 1 мс. Это, в свою очередь, требует повышения производительности сетевого оборудования.

Крайне актуальной задачей является обеспечение информационной безопасности. Один из ее подразделов – сетевая безопасность, является важной задачей, решаемой при создании и эксплуатации информационных систем и сетей связи. В концепции сетевой безопасности базовым и наиболее распространённым элементом является межсетевой экран (англ. Firewall).

Межсетевым экраном называется программное или программно-техническое средство, реализующее функции контроля и фильтрации информационных потоков не криптографическими методами в соответствии с заданными правилами.

Если рассматривать межсетевой экран как узел сети передачи данных, то легко обнаружить, что в большинстве случаев он вызывает бóльшую задержку

обслуживания пакетов, чем обычное сетевое оборудование (маршрутизаторы, коммутаторы). Это связано с наличием широкого спектра функций обеспечения безопасности, на выполнение которых межсетевому экрану требуется время. Подобные устройства могут стать «узкими местами» в Будущих сетях и сетях 5G.

Часть сетевого трафика является критичным к задержкам и/или другим показателям качества обслуживания (англ. Quality of Service, QoS). Например, к трафику, критичному к отдельным показателям качества обслуживания, относят сигнальный трафик, трафик видеоконференцсвязи реального времени, медицинский трафик и др.

В оборудовании современных сетей связи предусмотрены различные механизмы QoS. Один из механизмов предусматривает формирование приоритетов обслуживания одних классов трафика над другими и называется механизмом управления перегрузками (англ. congestion management), который в диссертации именуется механизмом приоритизации обслуживания.

Вследствие того, что в стандартах Будущих сетей предъявляются жёсткие требования к задержкам передачи пакетов в рамках сегмента сети, механизмы приоритизации обслуживания трафика будут применяться не только внутри операторской сети связи, но и в локальных вычислительных сетях (ЛВС). Отдельные типы современных межсетевых экранов, используемых на границе ЛВС с операторской сетью, не поддерживают механизмы приоритизации обслуживания. Из-за особенностей обслуживания пакетов в межсетевых экранах применение приоритизации обслуживания в ряде случаев актуальней во входной очереди, а не в выходной, что не распространено в современных межсетевых экранах корпоративного сегмента.

Работа посвящена разработке метода оценки показателей производительности межсетевых экранов корпоративного сегмента, функционирующих в условии приоритизации обслуживания критичного к задержкам трафик во входных очередях.

Всё вышесказанное обуславливает актуальность данного направления исследований.

Степень разработанности темы. Вопросам моделирования функционирования сетевого оборудования и фильтрации трафика в предметной области посвящены работы зарубежных и отечественных авторов: Acharya S., Al-Shaer E., Gusev M., Kaur H., Liu A. X., Salah K., Барабанова В. Ф., Богораза А. Г., а в теоретической области работы: Гайдамака Ю. В., Коломойцева В. С., Левакова А. К., Назарова А. Н., Самуйлова К. Е., Шабурова А. С., Шелухина О. И. и других.

Наиболее близкими к теме диссертации являются работы Gusev M., Liu A. X., Salah K. В этих работах анализируются процессы обслуживания пакетов в различных межсетевых экранах и формируются соответствующие математические модели, однако, в них не рассматривается приоритизация обслуживания пакетов во входных очередях межсетевых экранов.

Объектом исследования является межсетевой экран, функционирующий в условиях приоритизации обслуживания трафика. Объект исследования представлен на рис. 1.

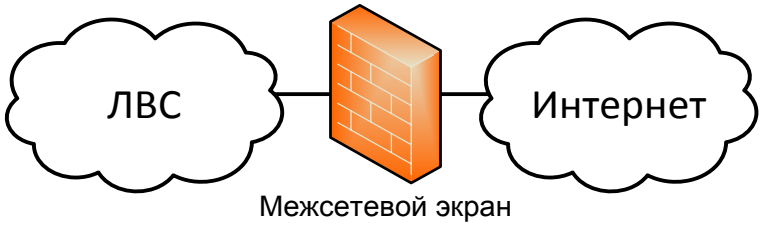

Рис.1 – объект исследования.

Рассматривается пограничный межсетевой экран между защищаемой ЛВС и сетью Интернет. Между ЛВС и сетью Интернет передаётся приоритетный и неприоритетный трафик.

Предметом исследования являются показатели производительности межсетевого экрана, функционирующего в условиях приоритизации обслуживания трафика.

Цель исследования. Целью диссертационной работы является разработка метода оценки показателей производительности межсетевых экранов, функционирующих в условиях приоритизации обслуживания чувствительного к задержкам трафика и исследование влияния приоритизации трафика на входных интерфейсах межсетевых экранов на их производительность.

Для достижения цели в диссертационной работе решены следующие задачи:

1. Анализ принципов реализации механизмов QoS в межсетевых экранах. Сформулирована постановка задачи для разработки модели функционирования межсетевого экрана в условиях приоритизации обслуживания трафика на его входе.

2. Разработка математической и имитационной моделей функционирования межсетевого экрана в условиях приоритизации обслуживания трафика на его входе.

3. Сравнительный анализ результатов математического и имитационного моделирования при снятии в имитационной модели ряда допущений, принятых в математической модели.

4. Исследование влияния числа проверок по базе правил фильтрации и объема пакетной очереди на показатели качества обслуживания пакетов межсетевым экраном. Сравнительный анализ показателей производительности межсетевого экрана, полученных с включенными и выключенными механизмами приоритизации обслуживания трафика на его входе.

Научная новизна результатов диссертационной работы заключается в следующем:

1. Разработан метод оценки показателей производительности межсетевого экрана, включающий в себя математическую и имитационную модели, который в отличие от существующих методов позволяет учитывать обслуживание на входах межсетевых экранов двух классов трафика – приоритетного и неприоритетного.

2. Для решения системы уравнений равновесия трёхмерной марковской модели функционирования межсетевого экрана разработана процедура перевода трехмерной матрицы переходных вероятностей в двумерную матрицу, позволяющая применить эффективный вычислительный метод расчёта стационарных вероятностей, основанный на применении блочных треугольных разложений.

3. Выявлены зависимости показателей качества обслуживания трафика межсетевыми экранами, функционирующими в условиях приоритизации обслуживания критичного к задержкам трафика, от длины очереди, длительности обслуживания и правил фильтрации при функционировании в режимах без перегрузки и с перегрузкой. Учёт данных зависимостей при эксплуатации

межсетевых экранов позволяет снизить задержки проходящего сквозь них трафика и избежать дополнительных перегрузок.

Теоретическая и практическая значимость работы. Разработан метод оценки показателей производительности межсетевых экранов при их функционировании в условиях приоритизации обслуживания чувствительного к задержкам трафика в их входных очередях. В основу метода положены математическая и имитационная модели. Разработанный метод позволяет рассчитать показатели производительности межсетевого экрана в различных условиях его функционирования.

Разработанный метод оценки показателей производительности межсетевых экранов позволяет производителям оборудования оценить необходимость использования механизмов приоритизации обслуживания трафика в ряде существующих межсетевых экранов корпоративного сегмента.

Рекомендации по управлению объёмом входной очереди межсетевых экранов и механизмами приоритизации обслуживания трафика позволяют эксплуатационному персоналу повысить показатели качества обслуживания трафика, проходящего сквозь межсетевой экран.

Имитационная модель с интуитивным и понятным графическим интерфейсом и инструкцией пользователя позволяет быстро получить искомые показатели производительности межсетевых экранов. Исходные коды имитационной модели на языке C# можно получить при обращении по email: vladmus89@gmail.com.

Методология и методы исследования. Для решения поставленных в диссертационной работе задач использованы методы теории массового обслуживания, теории марковских случайных процессов, теории сетей связи, а также методы имитационного моделирования и программирования на высокоуровневом языке общего назначения C#.

Основные положения, выносимые на защиту:

1. В существующих межсетевых экранах корпоративного класса, как правило, не предусмотрена возможность использования механизмов приоритизации обслуживания трафика во входных очередях. При переполнении входных очередей межсетевых экранов для обеспечения заданного уровня обслуживания критичного к

задержкам трафика необходимо применение механизмов приоритизации обслуживания во входных очередях.

2. Функционирование межсетевого экрана в условиях приоритизации трафика может быть представлено в виде однолинейной системы массового обслуживания типа $\vec{M}/M/1/L/f_1^{22}$ с ограниченным накопителем пакетов, комбинированными потерями и смешанными приоритетами обслуживания.

3. При функционировании межсетевого экрана с приоритизацией обслуживания трафика в режиме перегрузки при времени обслуживания, распределённом по экспоненциальному закону, среднее время нахождения неприоритетных пакетов в очереди становится меньше, чем при постоянном времени обслуживания, что обуславливается повышенной вероятностью частичного освобождения очереди.

4. При функционировании межсетевого экрана с приоритизацией обслуживания трафика в режиме без перегрузки увеличение максимального объёма очереди приводит к сглаживанию флуктуаций входящего трафика, что снижает потери. Однако при этом в режиме продолжительной перегрузки увеличение максимального объёма очереди приводит к повышению времени нахождения пакетов в ней, но не обеспечивает снижение потерь пакетов.

5. Механизм приоритизации обслуживания пакетов во входной очереди межсетевого экрана позволяет снизить потери пакетов приоритетного потока и в несколько раз снизить их задержку в очереди. Так, в условиях 30% перегрузки при доле входящего потока приоритетных пакетов в 15% от общего потока, включение механизмов приоритизации обслуживания снижает:

- потери приоритетного потока с 23% до нулевого уровня при повышении потерь неприоритетного потока на 4 %;
- среднее время нахождение приоритетного пакета в очереди в 21 раз (с 105 до 5 мкс) при увеличении этой величины для неприоритетных пакетов на 19%.

Апробация работы. Основные результаты работы докладывались и обсуждались на следующих 9 конференциях:

- Международный форум информатизации (МФИ-2011, МФИ-2012, МФИ-2013). Москва, 2011, 2012, 2013;

– Международная научно-техническая конференция «Фундаментальные проблемы радиоэлектронного приборостроения» (INTERMATIC – 2012). Москва, 2012;
– 7-ая, 8-ая, 9-ая, 10-ая Отраслевая научная конференция «Технологии информационного общества». Москва, 2013, 2014, 2015, 2016;
– Международная конференция «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» (RES-2013). Москва, 2013.

Личный вклад. Результаты диссертационной работы получены автором самостоятельно, математические процедуры и программные средства разработаны при его непосредственном участии.

Публикации. По материалам диссертационной работы опубликовано 12 печатных работ, из них 4 – в рецензируемых журналах, рекомендованных ВАК Минобрнауки России.

Результаты исследования соответствуют паспорту научной специальности 05.12.13 – «Системы, сети и устройства телекоммуникаций» по пунктам:

– 3: разработка эффективных путей развития и совершенствования архитектуры сетей и систем телекоммуникаций и входящих в них устройств;

– 10: исследование и разработка новых методов защиты информации и обеспечения информационной безопасности в сетях, системах и устройствах телекоммуникаций;

– 14: разработка методов исследования, моделирования и проектирования сетей, систем и устройств телекоммуникаций.

Структура и объем работы. Диссертация состоит из введения, 5 разделов, заключения, списка сокращений и обозначений, списка литературы, списка иллюстративного материала и 7 приложений. Основные результаты изложены на 148 страницах, в том числе на 44 рисунках и в 11 таблицах. Дополнительные сведения изложены на 76 страницах в приложениях. В библиографию включено 143 источников на русском и английском языках

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, определены цели и задачи исследований, сформулирована теоретическая и практическая значимость работы, представлены научные результаты и основные положения, выносимые на защиту.

Первый раздел «Анализ методов повышения производительности межсетевых экранов».

В разделе приведен анализ стандартов и рекомендаций международных и отечественных организаций по стандартизации и регулированию применения межсетевых экранов.

Проведен краткий анализ современных методов повышения производительности межсетевых экранов, приведены примеры ряда методов. Рассмотрены материалы по мобильным сетям 5G и Будущим сетям. В стандартах выявлены требования по снижению задержек передачи данных в рамках одного сегмента сети из «конца в конец» с 10 до 1 мс.

Выполнен краткий анализ применения механизмов QoS в современных сетях передачи данных. При анализе поддержки механизмов QoS в межсетевых экранах выявлена низкая степень их поддержки в межсетевых экранах корпоративного сегмента.

Второй раздел «Анализ принципов обработки пакетов в межсетевых экранах».

В разделе проведён анализ процесса обслуживания пакетов в межсетевых экранах в части функционирования очередей и выделения объёмов памяти, работы механизмов QoS и фильтрации трафика. Представлены и описаны процессы обслуживания пакетов для продуктовых линеек межсетевых экранов корпоративного сегмента (Enterprise): Cisco ASA, Juniper SRX, Huawei USG6000, а также NetFiler/IPTables.

Обосновано решение о разработке модели на основе межсетевого экрана типа NetFilter/IPTables. Рассматриваемая модель функционирования межсетевого экрана

в условиях приоритизации обслуживания трафика на его входе представлена на рис. 2.

Содержательная постановка задачи включает ряд допущений для упрощения модели. На вход модели поступает два потока пакетов с интенсивностями поступления приоритетного потока – λ_1 и неприоритетного потока – λ_2. Постановка в очередь осуществляется с абсолютным приоритетом. Если очередь заполнена полностью, а на интерфейс пришел приоритетный пакет, то он вытеснит неприоритетный пакет и займет его место в очереди. Полный объем модели равен L+1 пакетов – один пакет находится на обслуживании, остальные пакеты находиться в очереди, вмещающей L пакетов. Постановка на обслуживание осуществляется с относительным приоритетом. Это связано тем, что обслуживание пакета не может быть остановлено или отменено с приходом приоритетного пакета. Общее количество этапов обслуживания К. Ядро обработки пакетов имеет среднее время обслуживания $1/\mu^*$. Оставшиеся К-1 этапов представляют правила фильтрации со временем $1/\mu$ для каждого.

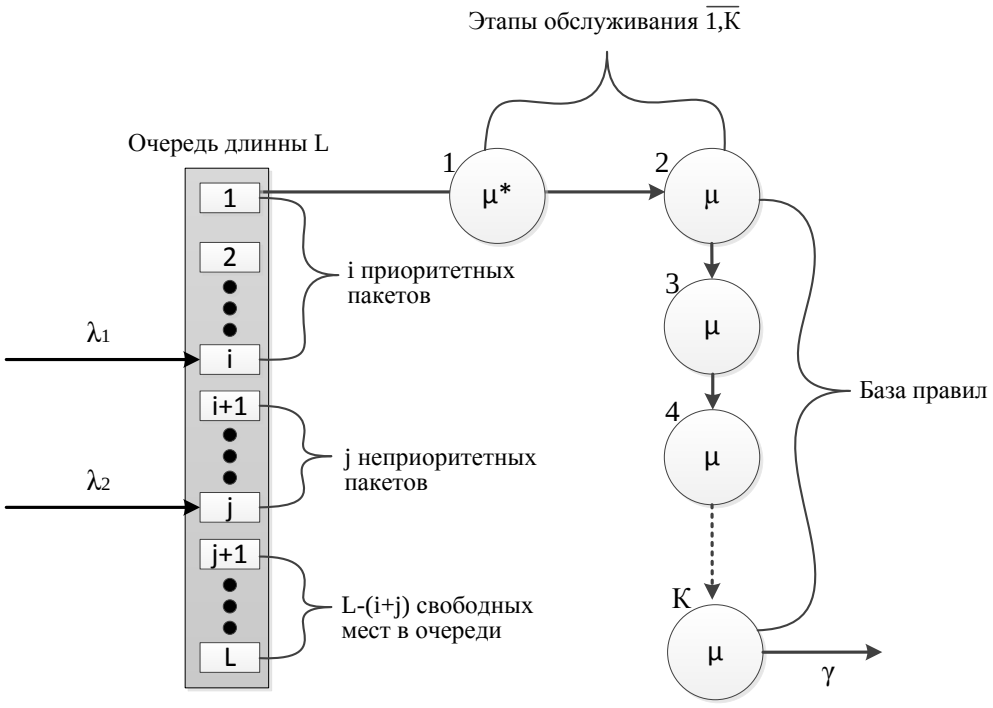

Рис.2 –Модель функционирования межсетевого экрана.

Третий раздел «Разработка математической модели функционирования межсетевого экрана в условиях приоритизации обслуживания трафика».

В разделе произведена адаптация содержательной постановки задачи для ее реализации с использованием математического аппарата марковских процессов с непрерывным временем. Сформулированы допущения к модели, накладываемые выбранным математическим аппаратом. Межсетевой экран представлен в виде системы массового обслуживания (СМО). Математическая модель представляет однолинейную СМО с ограниченным накопителем пакетов (заявок), комбинированными потерями и смешанными приоритетами обслуживания (абсолютным приоритетом постановки в очередь и относительным приоритетом постановки на обслуживание). На вход модели поступает простейший поток вызовов. В соответствии с модифицированной классификацией Дж. Кенделла СМО обозначается как: $\overrightarrow{\mathrm{M}} / \mathrm{M} / 1 / \mathrm{L} / \mathrm{f}_1^{22}$, где L – доступный объем очереди, а f – описывает наличие/отсутствие приоритетов их тип.

Поведение межсетевого экрана описывается процессом $\{X(t), t \geq 0\}$, являющимся марковским случайным процессом с непрерывным временем и дискретным множеством состояний:

$$S = \left\{ (0,0,0);\ (i,j,k),\ 0 \leq i \leq L,\ 0 \leq j \leq L,\ i + j \leq L,\ k = \overline{1,\mathrm{K}} \right\},$$

где i – количество приоритетных пакетов в очереди; j – количество неприоритетных пакетов в очереди; k – состояния межсетевого экрана или номер этапа обслуживания, на которой в рассматриваемый момент находится обслуживаемый пакет. $k = 0$ только если межсетевой экран пуст и не обслуживает пакеты ($k = 0$, при $i = j = 0$). В этом случае вероятность нахождения СМО в состоянии i, j, k будет выражена как:

$$p_{i,j,k},\ 0 \leq i \leq L,\ 0 \leq j \leq L,\ 0 \leq i + j \leq L,\ k = \overline{1,\mathrm{K}}.$$

Сформирована диаграмма состояний и переходов, для которой разработана система из 22 групп уравнений и уравнения нормировки, составляющих систему уравнений равновесия. Решение системы уравнений равновесия в аналитическом виде получить не удалось. Диаграмма состояний и переходов, описывающая

поведение межсетевого экрана, представляет трехмерную структуру с треугольным основанием, формируемую по тем же правилам, что и вероятности состояний СМО. Для упрощения проведения операций над трехмерными данными было решено хранить их в двумерном массиве, для чего была разработана процедура формирования матрицы. Выявлено, что при использовании процедура формирования матрицы определенного вида, матрица результатов принимает блочный трехдиагональный вид:

$$Q=\begin{pmatrix} B_0 & A_1 & 0 & \cdots & 0 & 0 & 0 \\ C_0 & B_1 & A_2 & \cdots & 0 & 0 & 0 \\ 0 & C_1 & B_2 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & B_{L-1} & A_L & 0 \\ 0 & 0 & 0 & \cdots & C_{L-1} & B_L & A_{L+1} \\ 0 & 0 & 0 & \cdots & 0 & C_L & B_{L+1} \end{pmatrix}.$$

Размеры блоков подчиняются следующим правилам:

$$B_0 - 1\times 2;\ B_1 - K\times K;\ B_i, i=\overline{2,L} - (i\cdot K)\times(i\cdot K);\ B_{L+1} - (L+1)\cdot K\times(L+1)\cdot K$$

$$C_0 - K\times 1;\ \tilde{C}_0 - K\times K;\ C_1=\begin{pmatrix}\tilde{C}_0\\ \tilde{C}_0\end{pmatrix};\ C_2=\begin{pmatrix}C_1 & 0\\ 0 & \tilde{C}_0\end{pmatrix}=\begin{pmatrix}\tilde{C}_0 & 0\\ \tilde{C}_0 & 0\\ 0 & \tilde{C}_0\end{pmatrix};\ C_3=\begin{pmatrix}C_1 & 0 & 0\\ 0 & \tilde{C}_0 & 0\\ 0 & 0 & \tilde{C}_0\end{pmatrix}$$

$$A_1 - 1\times K;\ \Lambda_1,\Lambda_2 - K\times K;\ A_2=\begin{pmatrix}\Lambda_2 & \Lambda_1\end{pmatrix};\ A_3=\begin{pmatrix}\Lambda_2 & \Lambda_1 & 0\\ 0 & \Lambda_2 & \Lambda_1\end{pmatrix}\ \text{и т.д.}$$

Блочный вид матрицы переходных вероятностей позволил применить эффективный вычислительный метод расчёта стационарных вероятностей, основанный на применении блочных треугольных разложений.

Для расчета конечных показателей производительности использованы следующие аналитические выражения:

$p_1^{loss}=\dfrac{\lambda_1}{\lambda_1+\lambda_2}\sum_{i=0}^{L-1}\sum_{k=1}^{K}p_{i,L-i,k}$ – вероятность вытеснения неприоритетного пакета из заполненной очереди при приходе приоритетного пакета;

$p_2^{loss} = \frac{\lambda_2}{\lambda_1 + \lambda_2} \sum_{i=0}^{L} \sum_{k=1}^{K} p_{i,L-i,k}$ – вероятность сброса неприоритетного пакета из-за переполнения очереди;

$p_{prior}^{loss} = \frac{\lambda_1}{\lambda_1 + \lambda_2} \sum_{k=1}^{K} p_{L,0,k}$ – вероятность сброса приоритетного пакета из-за переполнения очереди другими приоритетными пакетами;

$Q_{prior} = \sum_{i=0}^{L} \sum_{j=0}^{L-i} \sum_{k=1}^{K} ip_{i,j,k}$ – среднее число приоритетных пакетов в очереди;

$Q_{unprior} = \sum_{i=0}^{L} \sum_{j=0}^{L-i} \sum_{k=1}^{K} jp_{i,j,k}$ – среднее число неприоритетных пакетов в очереди.

Математическое моделирование функционирования межсетевого экрана, выполнено с помощью программы Wolfram Mathematica 10. Причиной выбора этой среды моделирования является ее преимущества над аналогами в символьных вычислениях. Выполнена оценка полученных результатов.

Четвёртый раздел «Разработка имитационной модели функционирования межсетевого экрана в условиях приоритизации обслуживания трафика».

Разработка имитационной модели произведена для расширения функциональных возможностей разрабатываемого метода. В разделе сформулирована постановка задачи на разработку имитационной модели. Обоснован выбор дискретно-событийного моделирования в качестве подхода к реализации модели. Для реализации модели выбран высокоуровневый язык общего назначения C#.

Представлены блок-схемы алгоритма имитационной модели. Описаны:

- события, возникающие в процессе моделирования;
- операции, проводимые над пакетами;
- процедуры воплощения алгоритма в коде;
- внутренние и внешние переменные, способы их расчета и размерность;
- сторонние библиотеки, использованные при разработке имитационной модели;
- реализация генераторов случайных чисел;

– способов сбора статистики и её агрегации.

Представлены результаты имитационного моделирования в сравнении с результатами, полученными с использованием математической модели. Результаты сравнения представлены в графическом виде. Различие интенсивностей суммарной обслуженной нагрузки находится в пределах 1-2%, а различие среднего заполнения очереди пакетами в пределах 3-11% от общего объема очереди.

Пятый раздел «Оценка функционирования межсетевого экрана в условиях приоритизации обслуживания трафика при изменении его характеристик обслуживания».

Получена оценка показателей производительности межсетевого экрана при условиях, что время обслуживания является постоянной величиной или случайной величиной, распределенной по экспоненциальному закону. Результаты имитационного моделирования показали, что соотношения задержек пакетов обоих приоритетов в очереди, обоснованные в теории массового обслуживания, соблюдаются при функционировании межсетевого экрана в режиме без перегрузок.

Получена оценка влияния допустимого размера очереди и количества правил фильтрации, которые необходимо пройти пакету на обслуживании, на показатели производительности межсетевого экрана.

Выполнен сравнительный анализ показателей производительности межсетевого экрана при включенном и выключенном механизме приоритизации обслуживания.

По результатам имитационного моделирования сформулированы рекомендации по управлению объёмом входной очереди межсетевых экранов и механизмами приоритизации обслуживания трафика позволяют эксплуатационному персоналу повысить показатели качества обслуживания трафика, проходящего сквозь межсетевой экран.

В заключении приведены основные результаты работы.

ЗАКЛЮЧЕНИЕ

1. Разработан метод оценки показателей производительности межсетевых экранов корпоративного сегмента при функционировании в условиях

приоритизации обслуживания чувствительного к задержкам трафика на их входах. В основу метода положены математическая и имитационная модели.

2. Для обеспечения требований к показателям качества обслуживания трафика рекомендуется учитывать приведённые далее зависимости.

При функционировании межсетевых экранов в режиме без перегрузки:

- увеличение объёма очереди приводит к сглаживанию флуктуаций входящего трафика как при включенной, так и выключенной приоритизации обслуживания;
- активация приоритизации обслуживания при отсутствии перегрузок не даёт значительного снижения потерь пакетов приоритетного трафика, особенно при увеличении объёма очереди, однако, обеспечивает значительное снижение задержки в очереди для приоритетных пакетов в диапазоне 50-100% загрузки межсетевого экрана.

При функционировании межсетевого экрана в режиме перегрузки:

- увеличение объёма очереди приводит только к увеличению задержек обслуженных пакетов, но не обеспечивает снижения потерь, как и при случае с функционированием в режиме без перегрузок;
- применение приоритизации обслуживания во входной очереди межсетевого экрана позволяет эффективно поддерживать значения потерь и задержки приоритетных пакетов, что особенно актуально для протоколов сигнализации и управления, не имеющих приоритизации обслуживания по умолчанию.

Использование алгоритмов с «жёсткой» приоритизацией, таких как PRIOR (Linux), LLQ (Cisco) и др. способствует «выдавливанию» пакетов с низким приоритетом из очереди пакетами с высоким приоритетом. При использовании подобных алгоритмов необходимо обоснованно выбирать типы трафика, которые будут иметь высший приоритет, так как рост интенсивности этих типов трафика может привести к отказу обслуживания неприоритетных типов трафика;

Периодическое перестроение базы (списка) правил фильтрации с целью снижения порядкового номера наиболее часто срабатывающего правила позволяет снизить среднюю задержку обслуживания пакетов.

3. Результаты диссертации использованы в ЗАО «Научно-производственное предприятие «Безопасные информационные технологии», а также в учебном процессе на кафедре Сетей связи и систем коммутации МТУСИ, что подтверждено соответствующими актами.

ПУБЛИКАЦИИ ПО МАТЕРИАЛАМ ДИССЕРТАЦИИ

Публикации в изданиях, рекомендованных ВАК:

1. Мусатов, В.К. Анализ тенденций развития рекомендаций МСЭ-Т по информационной безопасности [Текст] / В.К. Мусатов // T-Comm: Телекоммуникации и транспорт. – 2013. – №7. – С. 93-96.

2. Мусатов, В.К. Обоснование эффективности применения автокоррекции баз правил фильтрации в средствах межсетевого экранирования [Текст] / В.К. Мусатов // T-Comm: Телекоммуникации и транспорт. – 2014. – №8. – С. 68-72.

3. Мусатов, В.К. Математическое моделирование средств межсетевого экранирования в условиях приоритизации трафика [Текст] / В.К. Мусатов, А.А. Щербанская // T-Comm: Телекоммуникации и транспорт. – 2015. – Том 9, №8. – 2015.– С.47-57.

4. Мусатов, В.К. Имитационное моделирование средств межсетевого экранирования в условиях приоритизации трафика [Текст] / В.К. Мусатов, А.П. Пшеничников, А.А. Щербанская // T-Comm: Телекоммуникации и транспорт. – 2016. – Том 10, №12. – С. 10-17.

Публикации в других изданиях:

5. Мусатов, В.К. Анализ информационной безопасности в сетях связи [Текст] / В.К. Мусатов, С.А. Васильев // Международный форум информатизации (МФИ-2011). Телекоммуникационные и вычислительные системы: труды конференции – М.: ООО «Информпресс-94», 2011. – С. 37-38.

6. Мусатов, В.К. Моделирование производительности средств межсетевого экранирования [Текст] / В.К. Мусатов // Международный форум информатизации

(МФИ-2012). Телекоммуникационные и вычислительные системы: труды конференции – М.: ООО «Информпресс-94», 2012. – С. 42-43.

7. Мусатов, В.К. Анализ стандартов и рекомендаций по обеспечению информационной безопасности сетей передачи данных [Текст] / В.К. Мусатов // Международной научно-технической конференций «INTERMATIC – 2012» Фундаментальные проблемы радиоэлектронного приборостроения: матер. конф. часть 6. – М.: Энергоатомиздат, 2012. – С. 93-98.

8. Мусатов, В.К. Исследование вопросов фильтрации DDoS атак в контексте облачных вычислений [Текст] / В.К. Мусатов // Международная конференция «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» RES-2013: доклады. – М.: ООО «Информпресс-94», 2013. – С. 209-212.

9. Мусатов, В.К. Анализ механизмов фильтрации в межсетевых экранах [Текст] / В.К. Мусатов // Международный форум информатизации (МФИ-2013). Телекоммуникационные и вычислительные системы: труды конференции. – М.: ООО «Информпресс-94», 2013. – С. 35-36.

10. Мусатов, В.К. Анализ возможности применения динамических списков фильтрации в средствах межсетевого экранирования [Текст] / В.К. Мусатов // Международной научно-технической конференций «INTERMATIC – 2012» Фундаментальные проблемы радиоэлектронного приборостроения: матер. конф. часть 4 – М.: Энергоатомиздат, 2013. – С. 190-195.

11. Мусатов, В.К. Моделирование влияния приоритизации трафика на входном интерфейсе межсетевого экрана на его показатели производительности [Текст] / В.К. Мусатов, А.П. Пшеничников. // 12-ая международной научно-технической конференции «Перспективные технологии в средствах передачи информации»: матер. конф. том II – Владимир: Изд-во ВлГУ, 2017. – С.84-86.

12. Мусатов, В.К. Влияние применения приоритизации обслуживания пакетов на входе межсетевого экрана на показатели производительности [Текст] / В.К. Мусатов // Международный форум информатизации (МФИ-2017). Телекоммуникационные и вычислительные системы: труды конференции – М.: Горячая линия - Телеком, 2017. – С. 51-55.

Подписано в печать __.__.2018 г.

У сл. п. л.– 1.0

Заказ №_____.

Тираж: 100 экз.