УДК 004.7.032.8

НЕЧЁТКИЕ МОДЕЛИ И ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ АНАЛИЗА ХАРАКТЕРИСТИК ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Р.В. МАКАРУК
В.Н. ГИЛЯРОВ

«Санкт-Петербургский государственный технологический институт (технический университет)»

e-mail:

giljarow@mail.ru

Повышение качества и безопасности корпоративных компьютерных сетей, на сегодняшний день, является задачей актуальной. Прежде всего это связно с повсеместным использованием таких сетей на предприятиях различного масштаба и направленности.

Для решения задачи повышения качества функционирования сетей необходимо произвести оценку основных её характеристик производительность, надёжность и безопасность. Данная задача является сложной по своей сути. В работе для её решения предложено использовать методы нечёткой логики. Тем самым решая задачу формализации таких субъективных показателей, как опыт и знание эксперта, которые крайне важны в процессе оценки.

Ключевые слова: нечёткие модели, локальные вычислительные сети, производительность, надёжность, безопасность, анализ характеристик сети.

Без использования локальных вычислительных сетей (ЛВС) и многомашинных вычислительных систем (ВС) не мыслимо эффективное функционирование современных предприятий. Связно это с тем, что для решения задач планирования и управления производством необходимо, иметь среду передачи данных характеризующуюся возможностью без потерь и перерывов в обслуживании, передавать с заданной скоростью защищённую от несанкционированного доступа и подмены информацию [4].

Локальные вычислительные сети предприятий представляют собой многосегментные структуры, в которые входит большое количество рабочих станций, серверов (общие файловые хранилища, базы данных, управление политиками учётных записей, печать, серверы терминального доступа и т. д.) и сетевого оборудования (коммутаторы, маршрутизаторы, точки доступа беспроводной связи и т. д.). Таким образом перед администраторами ЛВС встаёт ряд сложных задач по обеспечению качества работы сети.

Важно, чтобы ЛВС не просто работала, но работала качественно. Понятие качества обслуживания включает в себя такие характеристики, как надёжность, производительность и безопасность. Каждая из перечисленных характеристик оценивается разными показателями:

производительность: скорость передачи информации и задержка передачи пакетов;

надёжность: доля потери пакетов, доступность, отказоустойчивость;

безопасность: наличие взаимосвязанных мер (использование специальных технических и/или программных средств, организационных мероприятий, нормативно-правовых актов и т. д.).

Математический аппарат теории нечётких множеств, на сегодняшний день, всё чаще применяют для решения различных прикладных задач. Это привело к появлению моделей и систем с нечёткой логикой, направленных на решение задач оценки характеристик ЛВС и ВС. Связано это с тем, что процессы протекающие в ЛВС и ВС характеризуются неопределённостью, нестабильностью и т. п. Все эти факторы являются существенным препятствием для создания моделей на основе классических математических теорий и методов. Оценивая производительность, надёжность и безопасность ЛВС и ВС необходимо учитывать не только объективные параметры, но и такие параметры как суждение, знание и опыт эксперта [3].

Для оценки производительности необходимо собрать статистические данные работы ЛВС. Здесь применяются активные измерения, основанные на генерации сервером специальных пакетов, либо отправляемых на порт программы-монитора установленной на клиенте, либо эхо-запрос к клиенту (если нет возможности использования программы-монитора). В первом случае измеряется интервал времени между моментом отправки первого бита пакета и получением последнего бита этого пакета клиентом. При использовании второго метода измеряется интервал времени разделённый пополам между отправкой клиенту эхо-запроса и получением сервером эхо-ответа. Таким образом рассчитывается односторонняя задержка пакетов (One-Way Delay Metric, OWD), входящая в состав стандартов IPPM (IP Performance Metrics – метрика производительности IP-сетей) и описанная в RFC 2679 [1]. Последовательность измерений выполняется достаточно длин-

ном промежутке времени, а пакеты отправляются в случайные моменты времени, подчиняющиеся распределению Пуассона. В качестве оценки односторонней задержки используется медиана выборки.

Далее оценивается время реакции сети, представляющую собой интегральную характеристику производительности сети с точки пользователя. Время реакции сети определяется как интервал времени между отправкой эхо-запроса и получением эхо-ответа [4].

Затем инициируется передача данных между сервером и клиентом (программой-монитором) для измерения средней скорости работы ЛВС. Средняя скорость (Sustained Information Rate, SIR) определяется на промежутке времени равным 10 секундам и вычисляется как частное от деления объёма переданных данных на продолжительность передачи.

Для оценки качества ЛВС и ВС по производительности используется нечёткая модель, представленная на рисунке 1. Оценка производится по пятибалльной шкале: «низкая», «ниже среднего», «средняя», «выше среднего», «высокая». На рисунке 1 элементы в виде прямоугольника — нечёткие лингвистические переменные; элементы в виде круга — нечёткие операционные модули, основанные на правилах. Нечёткий модуль, основанный на правилах, представляет собой базу продукционных правил, которые связывают между собой входные и выходные нечёткие лингвистические переменные (НЛП). Используемые продукционные правила можно представить в следующей обобщенной форме:

$$\text{ЕСЛИ } x_1 = A_1^j \perp x_2 = A_2^j \perp \ldots x_n = A_n^j \text{, ТО } y_1 = B_1^k \text{ И } y_2 = B_2^k \text{ И } y_m = B_m^k, \quad (1)$$

где x_i — i-я входная лингвистическая переменная (ЛП); A_i^j — j-ий терм i-ой входной переменной (возможно с функцией-модификатором > (больше), < (меньше) или not (не)); y_l — l-я выходная ЛП; B_l^k — k-ый терм l-ой выходной переменной (возможно с функцией-модификатором not (не)); $\perp$ — лингвистическая связка «И», «ИЛИ».

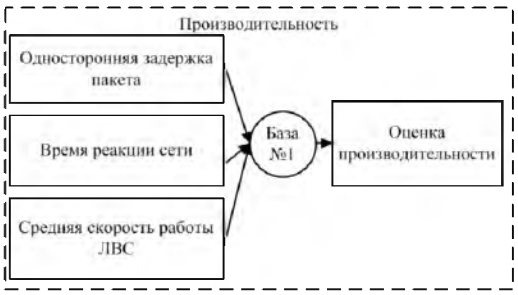

Рис. 1. Модель оценки производительности

Лингвистические связки «И» и «ИЛИ» реализуются с помощью γ-функции:

$$\alpha = \left(\prod \alpha_i\right)^{(1-\gamma)} \left(1 - \prod (1 - \alpha_i)\right)^{\gamma} \quad (2)$$

где α — оценка возможности реализации лингвистического факта (высказывания), связанного с одним из термов *i*-ой ЛП.

При $\gamma \approx 0$ в (2), реализуется лингвистическая связка «И», иначе при $\gamma \approx 1$ — «ИЛИ». Применение γ-функции позволяет достаточно тонко отслеживать особенности формулировок эксперта.

После формирования качественной оценки по производительности, программный комплекс переходит на следующий этап – оценка надёжности. Для определения доли потерянных пакетов серверная часть инициирует посылку большого количества эхо-запросов к клиенту. Каждый эхо-запрос отправляется не дожидаясь эхо-ответа на предыдущий запрос. Такая передача продолжается на протяжении одной минуты. Результатом данной операции будет отношение количества потерянных пакетов к общему количеству переданных пакетов.

Доступность (доля времени, в течении которого система или служба находится в работоспособном состоянии [4]) является долговременной характеристикой, поэтому измеряется на достаточно большом промежутке времени (день, неделя, месяц, год). В случае, когда программный комплекс только внедрён в эксплуатацию на предприятии доступность рассчитывается системным администратором ЛВС по имеющимся у него данным.

Данная характеристика особенно важна для серверного сегмента сети, где обрабатываются данные и производится контроль учётных записей пользователей.

Для сложных систем, которыми являются ЛВС предприятия, под отказоустойчивостью понимается способность ЛВС скрывать от пользователя отказ отдельных её элементов. Например, Интернет-шлюз подключен к двум каналам связи, один из которых является резервным. При выходе из строя основного канала шлюз должен переключится на резервный с, по возможности, сохранением всех установленных сессий. Чтобы сформировать оценку по данной характеристике пользователю системы необходимо ответить на ряд вопросов, касающихся резервирования критически важных узлов ЛВС.

Таким образом, надёжность ЛВС оценивается по значениям характеристик доли потери пакетов, доступности и отказоустойчивости в соответствующей нечёткой модели представленной на рис. 2. Оценка выставляется по пятибалльной шкале описанной выше.

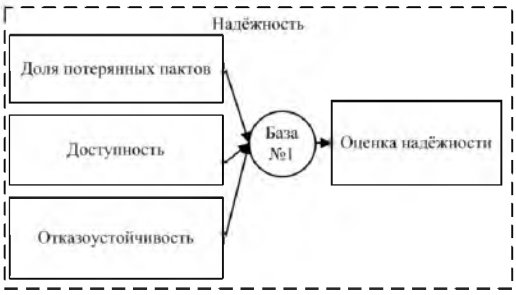

Рис. 2. Модель оценки производительности

Производительность и надёжность ЛВС измеряются в соответствии со стандартами IPPM. В этих стандартах описывается каждая характеристика как случайная величина, правила получения выборок, приводятся рекомендуемые статистические оценки, которыми следует пользоваться при обработке полученной выборки значений.

Безопасность является одной из важнейшей характеристики ЛВС и трудоёмкой в оценке. Связано с это с тем, что действия злоумышленников носят комплексный характер, поэтому необходима оценка многих показателей влияющих на безопасность, а также необходим системный характер защиты.

Оценка уровня безопасности ЛВС предусматривает две стадии: получение характеристик сети и получение ответов пользователя системы на анкету. В анкету входят, например, такие вопросы: «Имеется возможность воспользоваться постороннему человеку компьютером, установленным в офисе?», «На компьютерах, обрабатывающих секретные данные, имеется выход в сеть Интернет?», «Используется в вычислительной сети технологии Honeypot?» и т. д. На основании полученных данных производится оценка текущего уровня безопасности вычислительной сети [3]. Общая последовательность действий оценки представлена на рис. 3.

На первом этапе пользователь системы производит выбор метода получения характеристик сети автоматизированное сканирование или ручной ввод. При выборе автоматизированного метода получения характеристик сервером инициируется запуск модуля сканирования сети, по работе которого формируется протокол. Далее протокол сканирования или введённые вручную данные анализируются для формирования параметров V_i необходимых для оценки уровня безопасности ЛВС по данным сканирования Fs_i. На втором этапе пользователь системы отвечает на вопросы анкеты. Ответы формируют параметры A_i, необходимые для формирования оценки уровня безопасности по данным опроса Fa_i. Последний этап заключается в формировании оценки уровня безопасности вычислительной сети F_i на основе полученных оценок Fs_i и Fa_i.

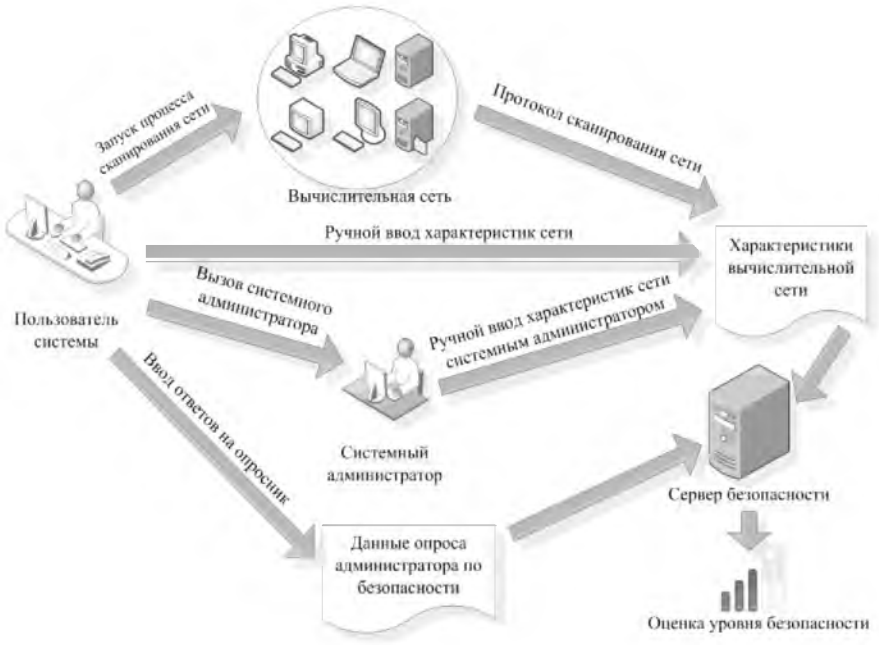

Рис. 3. Общая последовательность действий оценки уровня безопасности ЛВС

Для решения задачи оценки уровня безопасности ЛВС на основе серии стандартов ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 27001 и интервьюирования экспертов разработана модель, представленная на рисунке 4 [2].

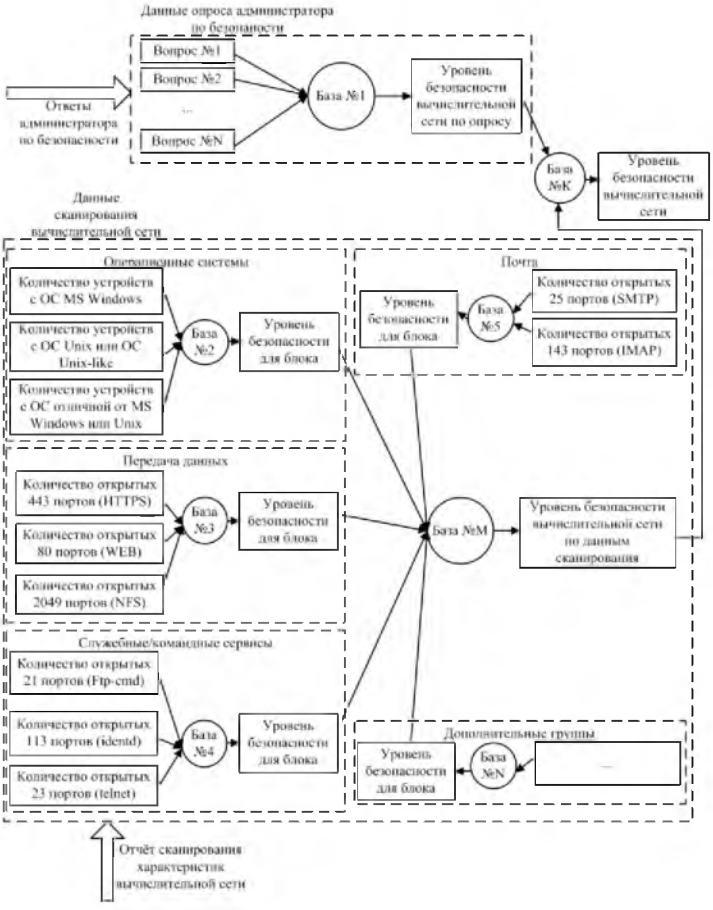

Рис. 4. Модель оценки безопасности

Программный комплекс анализа характеристик вычислительной сети состоит из нескольких подсистем [3]. Общая структурная схема программного комплекса представлена на рисунке 5.

Интерфейс администратора базы данных. Данный интерфейс позволяет следить за актуальностью базы данных программного обеспечения для построения комплекса повышения безопасности.

Рис. 5. Общая структура схема программного комплекса

Интерфейс инженера знаний. Интерфейс для дополнения и изменения базы знаний. Инженер знаний работает с экспертами, вместе они формируют базу знаний, с помощью которой производится оценка производительности, надёжности и безопасности ЛВС.

Модуль оценки производительности, надёжности и безопасности ЛВС. В этом модуле на основе собранных данных о ЛВС оцениваются основные характеристики ЛВС, а также формируется общая оценки ЛВС.

Модуль поиска необходимого программного обеспечения для защиты ЛВС. На основе оценки безопасности ЛВС, модуль производит поиск в базе данных программного обеспечения (ПО) для построения защиты.

Модуль поиска рекомендаций. Данный модуль формирует рекомендации по повышению оценок характеристик ЛВС.

Отличие данного программного комплекса от аналогичных продуктов состоит в том, что качественная оценка характеристик производительности, надёжности и безопасности ЛВС и ВС основывается на методах нечёткой логики; серверная часть работает только под управлением ОС Unix, что является гарантией надёжности и безопасности; программы-мониторы функционируют под следующими операционными системами: Linux (минимальная версия ядра 2.6.16), FreeBSD (минимальная версия 7.0), Microsoft Windows (минимальная версия XP); программный комплекс работает с пользователем от стадии проектирования безопасности до стадии работы компонентов обеспечения безопасности и мониторинга их работы.

На данный момент программный комплекс прошёл апробацию в ЛВС кафедры систем автоматизированного проектирования и управления СПбГТИ(ТУ), которая ежедневно используется сотрудниками кафедры, аспирантами и большим количеством студентов. На программный комплекс получено свидетельство о государственной регистрации программ для ЭВМ №2013617294 от 08 августа 2013 года.

Список литературы

1. RFC 2679 [Электронный ресурс] – Режим досутпа : http://www.ietf.org/rfc/rfc2679.txt, свободный – Загл. с экрана. – Яз. Англ.
2. Макарук, Р.В. Оценка текущего уровня безопасности вычислительной сети с использованием мягких вычислений / Р.В. Макарук, Д.А. Тратканов // ММТТ-25 : сб. тр. XXV междунар. науч. конф., г. Волгоград, 29 мая – 31 мая 2012 г.: в 10 т. – Саратов, 2012. – Т. 4. С. 15-18.
3. Макарук, Р.В. Поддержка при выборе компонент информационной защиты локальных вычислительных сетей / Р.В. Макарук, В.Н. Гиляров, О.Г. Новикова // Известия Санкт-Петербургского государственного технологического института (технического университета). – 2012. – № 16(42). С. 52–56.
4. Марченков А.Е., Сафонов В.Л., Трубицин С.Н. Вероятностная организация систем адаптивного управления мультисервисной системой // «Научные ведомости БелГУ» № 7 (126) выпуск 22/1, раздел информационно-коммуникационные технологии, Белгород, 2012 г. С. 174 – 181.
5. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы. Издание 4-ое. / В.Г. Олифер, Н.А. Олифер. – СПб. : Питер, 2010. 943 с.

FUZZY MODELS AND SOFTWARE PACKAGE FOR ANALYSIS CHARACTERISTICS OF COMPUTER NETWORK

R.V. MAKARUK
V.N. GILYAROV

State Institute of Technology
Saint-Petersburg Russia
Saint-Petersburg

e-mail:
giljarow@mail.ru

Improved quality and safety of corporate computer networks, today is the actual task . First of all it is connected with the widespread use of such networks in enterprises of different size and orientation.

To solve the problem of increasing the quality of the networks needs to assess its basic characteristics of performance, reliability and security. This task is complex in nature. In this paper to solve it is proposed to use fuzzy logic techniques. Thereby solving the problem of formalization of subjective indicators such as experience and knowledge of the expert, which is extremely important in the evaluation process.

Key words: fuzzy model, local area networks, performance, reliability, security, network performance analysis.