

Ю.Л. Леохин, Р.С. Зубков

ПРИМЕНЕНИЕ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ ДЛЯ ПРОГНОЗИРОВАНИЯ СОСТОЯНИЙ КОМПЬЮТЕРНЫХ СЕТЕЙ

В статье предложен метод прогнозирования состояний компьютерной сети, основанный на биометрических алгоритмах, дана оценка методов для решения задачи прогнозирования состояния компьютерной сети, рассмотрены примеры фазовых снимков, полученные в различных условиях функционирования компьютерной сети.

Ключевые слова: компьютерная сеть состояние, прогнозирование, биометрические технологии, фазовая траектория

Yu.L. Leokhin, R.S. Zubkov

APPLICATION OF BIOMETRIC TECHNOLOGIES FOR FORECASTING OF CONDITIONS OF COMPUTER NETWORKS

In article the method of forecasting of conditions of the computer network, based on biometric algorithms is offered, the assessment of methods for the solution of a problem of forecasting of a condition of a computer network is given, the examples of phase pictures received in various operating conditions of a computer network are considered.

Keywords: computer network condition, forecasting, biometric technologies, phase trajectory

Внедрение информационных технологий в деятельность предприятия является одним из главных условий повышения его конкурентоспособности в условиях рынка. Основой информационной инфраструктуры современного предприятия являются компьютерные сети, обеспечивающие транспорт для переноса информации между различными приложениями информационных систем.

Высокая интенсивность и разнообразие потоков данных, создаваемых сотнями и тысячами сотрудников современного предприятия, необходимость производить поиск данных в базах большой размерности, сложное взаимодействие распределенных приложений, невысокая скорость глобальных линий связи между отделениями корпорации, замедление скорости взаимодействия в шлюзах, согласующих неоднородные компоненты различных подсетей и т.д. – это факторы, влияющие на загрузку компьютерной сети, а, следовательно, на способность сети решать основную задачу – передавать данные между приложениями с заданной скоростью обмена.

Компьютерная сеть представляет собой сложный технический объект, требующий эффективного управления. Как показывает мировой опыт, на создание и внедрение эффективных систем управления тратится до 20% от стоимости оборудования компьютерных сетей, позволяющих поддерживать на заданном уровне сетевые ресурсы, необходимые для предоставления качественных услуг. При этом необходимо учитывать, что в современных мультисервисных корпоративных сетях используется сложное, многофункциональное коммуникационное оборудование, обеспечивающее поддержку специальных механизмов контро-

ля и управления качеством – QoS, развитых инструментов реализации корпоративной политики информационной безопасности.

Выделяют шесть функциональных групп задач системы управления, определенных стандартами ISO/ITU-T [1, 2, 3, 4, 5].

1-я группа: управление конфигурацией сети и именованнием – эти задачи заключаются в конфигурировании параметров сетевых узлов: коммутаторов, маршрутизаторов, сетевых адаптеров и сетевых интерфейсов, а также программного обеспечения.

2-я группа: обработка ошибок – эта группа задач включает выявление, определение и устранение последствий сбоев и отказов сети.

3-я группа: анализ производительности и надежности – задачи этой группы связаны с оценкой таких параметров, как время реакции системы, пропускная способность реального или виртуального канала связи, интенсивность трафика в отдельных сегментах и каналах сети, вероятность искажения данных при их передаче через сеть, а также коэффициент готовности сети. Функции анализа производительности и надежности сети нужны как для оперативного управления сетью, так и для планирования развития сети.

4-я группа: управление безопасностью – задачи этой группы включают в себя контроль доступа к данным при их хранении и передаче через сеть. Базовыми элементами управления безопасностью являются процедуры аутентификации пользователей, назначение и проверка прав доступа к ресурсам сети, управление полномочиями и т.д.

5-я группа: учет работы сети – задачи этой группы заключаются в регистрации времени использова-

ния различных ресурсов сети – устройств, каналов и транспортных служб.

6-я группа: идентификация и прогнозирования состояния сети. Современная корпоративная сеть – это сложная техническая система, состояние которой описывается многомерными векторами. Администраторам сложно работать с такими многомерными данными. Поэтому необходимо в составе систем управления корпоративными сетями использовать подсистемы идентификации состояний корпоративной сети. Качественный прогноз позволит администраторам вовремя подготовить сеть для предотвращения перегрузок, ошибок и других нештатных ситуаций.

Среди этих групп важной является шестая группа задач – идентификация и прогнозирование. Решение этих задач позволит администратору вовремя подготовить сеть до наступления критического события.

Таким образом, разработка методов, позволяющих генерировать качественный прогноз наступления критических событий в сети, является актуальной задачей.

В статье предлагается метод прогнозирования состояний компьютерной сети, основанный на биометрических алгоритмах.

В настоящее время биометрические алгоритмы уже используются в различных областях человеческой деятельности, например:

- в электронных системах идентификации человека по отпечаткам пальцев (дактилоскопия);
- для выявления заболеваний пациентов по отпечаткам ладоней (дерматоглифика);
- в поисковых системах (google, yandex и т.д.) для определения процента уникальности изображения;
- в системах аутентификации и т.д.

Предлагаемый метод прогнозирования основан на распознавании фазовых траекторий (ФТ) состояний компьютерной сети (КС) адаптированным биометрическим алгоритмом. Распознавание фазовых траекторий происходит в три этапа:

1. Регистрация. Для прогнозирования события предлагается на основе статистики, предшествующей ранее наблюдавшемуся событию, регистрировать отпечатки фазовых траекторий параметров состояния корпоративной сети. Полученные отпечатки сохраняются в базе данных эталонов.
2. Верификация. Проводится сравнение эталонных фазовых траекторий с наблюдаемыми фазовыми траекториями.
3. Идентификация. В случае совпадения фазовых траекторий, идентифицируется событие или состояние компьютерной сети.

Для верификации фазовых траекторий предлагается использовать биометрический алгоритм «Сравнение

по контрольным точкам» [7, 10, 11]. Для его адаптации под решение задачи прогнозирования состояний компьютерной сети необходимо было решить следующие задачи:

- выполнить классификацию элементов (в биометрии используется термин “узор”), составляющих фазовую траекторию;
- определить новые сравниваемые элементы, при помощи которых возможно идентифицировать фазовую траекторию (состояние, в котором находится компьютерная сеть);
- разработать ряд сравниваемых критериев;
- разработать способ кодирования и сравнения фрагментов фазовой траектории.

Компьютерная сеть является сложной технической системой. Существует большое количество методов [6, 8, 9] решений задачи прогнозирования, но не все они способны сформировать качественный прогноз состояния сложной технической системы. Для оценки эффективности известных методов прогнозирования [6, 8, 9] использовались следующие критерии:

1. Способность обработки данных в реальном времени;
2. Способность обработки данных, представленных в разных шкалах;
3. Способность спрогнозировать ранее не наблюдавшееся событие;
4. Способность строго формализовать и алгоритмизировать методы решения задачи;
5. Способность решать слабо формализованную задачу;
6. Способность решать задачу в условиях недостатка данных;
7. Способность формирования многопараметрического прогноза;
8. Способность к аппаратной реализации;
9. Способность к преодолению трудностей, связанных с реализацией метода.

Шкала оценки имеет следующие значения:

- “-” – не эффективно;
- “0” – эффективно не во всех ситуациях;
- “+” – эффективно;
- “+” и “-” = “0”.

Метод **временной экстраполяции** исследует исторические данные. Прогнозирование параметров состояния в виде временной экстраполяции характеристик использует в качестве аргумента один параметр – время. Кроме того, метод временной экстраполяции включает в себя эвристические элементы, которые используются в разработке математической модели и анализе результатов прогнозирования. Отсюда и появляется некоторая степень субъективности, влияющая на конечный результат.

Таблица 1. Оценка методов для решения задачи прогнозирования состояния компьютерной сети

Требования, предъявляемые к методу прогнозирования состояния сложного технического объекта	Метод временной экстраполяции	Метод пространственной экстраполяции	Моделирование	Эвристические методы	Регрессионные методы	Логические методы	Метод сравнения фазовых снимков
Способность обработки данных в реальном времени	-	-	+	-	0	-	+
Способность обработки данных, представленных в разных шкалах	-	+	+	+	-	0	+
Способность спрогнозировать ранее не наблюдавшееся событие	-	+	0	+	-	+	-
Способность строго формализовать и алгоритмизировать методы решения задачи	+	0	0	-	+	+	+
Способность решить слабо формализованную задачу	-	-	0	+	+	+	-
Способность решить задачу в условиях недостатка данных	-	+	-	+	-	0	+
Способность генерации многопараметрического прогноза	-	+	+	-	0	-	+
Способность к аппаратной реализации	+	+	0	-	0	-	+
Способность преодоления трудностей, связанных с реализацией метода	-	0	-	-	0	-	0
Итоговая оценка	(-) X5	(+) X3	(+) X1	(-) X1	(-) X1	(-) X1	(+) X4

Пространственная экстраполяция связана с прогнозированием в пространстве характеристик. Суть метода пространственной экстраполяции состоит в распространении вывода, полученного в результате анализа одной части процесса, на другую часть или на процесс в целом. Данный метод работает при одном условии – закон изменения состояния в прошлом должен сохраниться в будущем. Поэтому внесение каких-либо изменений в систему повлечет за собой корректировку множества законов изменения состояний компьютерной сети, что является весьма трудоемкой задачей. А те законы изменения состояний, которые были получены до момента изменения системы, станут неработоспособными.

К достоинству метода пространственной экстраполяции можно также отнести отсутствие необходимости разработки громоздких прогнозных моделей по результатам наблюдений.

Если **моделировать** процессы функционирования компьютерной сети, то первоочередной задачей будет детальное описание исследуемой системы при помощи математического и физического моделирования. Это представляется крайне сложным в силу гетерогенности и “непостоянства” исследуемой системы, что влечет за собой большие по объёму вычисления. Кроме того, метод моделирования процессов будет не эффективен в ситуациях, требующих быстрой реакции на изменение состояния системы.

Для реализации **эвристических** методов в многопараметрической системе необходимо использование

знаний нескольких экспертов, что также создаст трудности в быстрой реакции на изменение состояния компьютерной сети. Исследование большого количества экспертиз займет много времени.

Для решения задачи методом **нейронных сетей** нет необходимости в исследовании процессов состояния компьютерной сети. Необходимым условием является набор параметров, необходимых для обучения нейронной сети. В нашем случае набором входных параметров является ряд функций, которые зависят от множества непредсказуемых факторов. Необходимо отметить, что решение поставленной задачи практической реализацией программной модели данного метода выглядит крайне затруднительным.

Использование **логических** методов также не принесет желаемого результата, поскольку задача исследуемой области не подразумевает решения, основанного на тех или иных логических действиях.

Регрессионные методы также требуют громоздких вычислительных действий, так как требуют детального исследования зависимостей между переменными, влияющими на состояние компьютерной сети.

Наибольшая итоговая оценка была присвоена разрабатываемому методу **сравнения фазовых снимков** по следующим причинам:

1. (+) Разработанный метод позволяет получать как долгосрочные, так и краткосрочные прогнозы.
2. (+) Метод проводит сравнение динамических показателей системы.

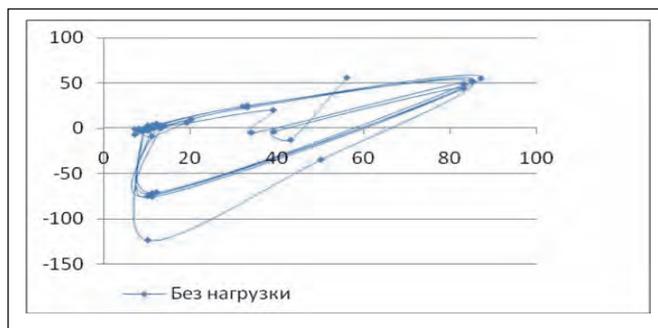


Рис. 1

3. (-) Данный метод работает при одном условии - динамические изменения состояния в прошлом должны сохраниться в будущем.
4. (+) Метод формализуется и поддается алгоритмизации.
5. (-) Прогноз формируется на основании статистических данных уже наблюдавшегося события. Задача прогнозирования формируется системой управления компьютерной сетью (СУКС) на основании событий, которые уже наблюдались в КС.
6. (+) В случае недостатка статистических данных той или иной функции, возможно замещение этой функции другой, например, о том, что узел перегружен, будет свидетельствовать как функция коэффициента перегрузки порта, так и функция изменения скорости передачи.
7. (+) В случае если в сегменте сети сформируются симптомы динамических состояний для возникновения нескольких событий одновременно, то система управления сформирует прогноз для каждого события в отдельности и независимо от того, связаны события друг с другом или нет.
8. (+) Планируется аппаратная реализация данного метода в составе функций системы управления компьютерной сетью.
9. Планируется реализовать бета-версию системы управления компьютерной сетью при помощи стандартного языка программирования и БД.

Рассмотрим примеры фазовых снимков, полученные в различных условиях функционирования компьютерной сети.

При этом под **фазовым состоянием** параметра компьютерной сети будем понимать координату ($f_{\text{среднее}}(t), \Delta f(t)$) на плоскости, соответствующей точке данного параметра в конкретный момент времени.

Здесь: $f_{\text{среднее}}(t) = (f(t_1) + f(t_2))/2$; $\Delta f(t) = f(t_2) - f(t_1)$; $f(t_1)$ – значение параметра МІВ в начальный момент времени; $f(t_2)$ – значение параметра МІВ в конечный момент времени; $f_{\text{среднее}}(t)$ – среднее значение двух параметров за время $t_2 - t_1$; $\Delta f(t)$ – приращение значения функции $f(t)$.

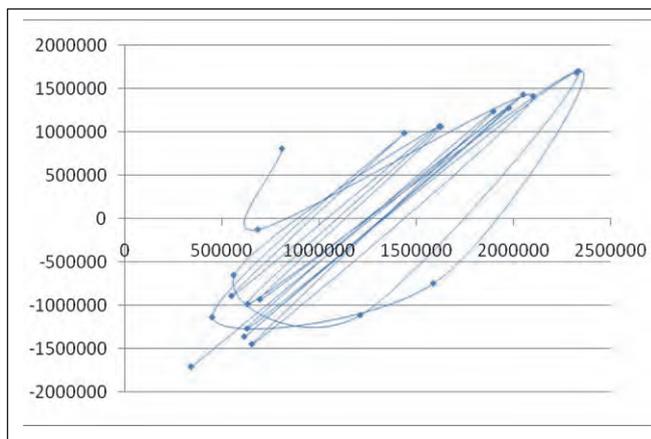


Рис. 2

Под фазовой траекторией (ФТ) будем понимать ряд фазовых состояний параметра или параметров компьютерной сети на одной плоскости за определенный временной интервал.

С помощью разработанной системы управления компьютерной сетью был получен ряд фазовых траекторий, присущих конкретным условиям функционирования компьютерной сети.

Нормальные условия – состояние равновесия, без нагрузки (рис. 1).

Ось абсцисс – параметр скорости входящего трафика. Ось ординат – скорость изменения наблюдаемого параметра.

В нормальных условиях компьютерная сеть функционирует без нагрузки. По сети передается малый объем трафика. В основном это служебный трафик.

Работа под нагрузкой (рис. 2)

Ось абсцисс – параметр скорости входящего трафика. Ось ординат – скорость изменения наблюдаемого параметра.

Компьютерная сеть функционирует под нагрузкой, происходит перемещение файла через наблюдаемый порт.

Работа под нагрузкой – наблюдение в одинаковых условиях нескольких потоков (рис. 3).

Из снимка видно, что одинаковым условиям соответствуют идентичные динамические состояния системы. Диапазоны значений, направленность, ориентация и другие критерии очень похожи для одинаковых условий функционирования компьютерной сети.

Перегрузка

Будем увеличивать нагрузку на порт сетевого устройства до переполнения буфера устройства и затем её понижать.

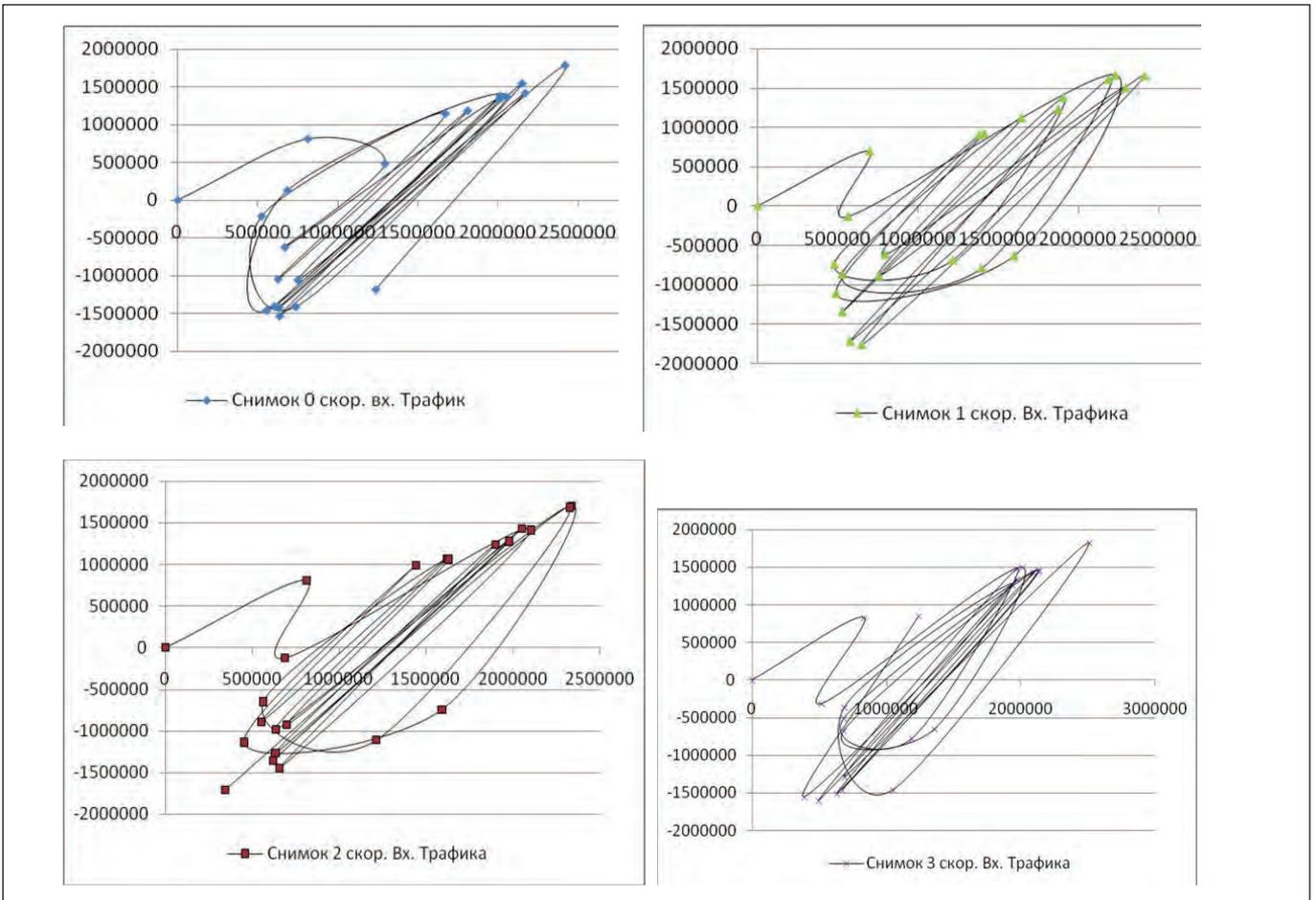


Рис. 3

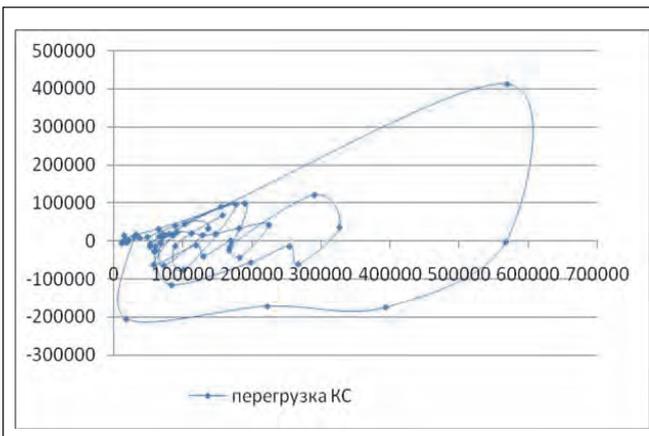


Рис. 4

Ось абсцисс – параметр скорости исходящего трафика. Ось ординат – скорость изменения наблюдаемого параметра.

На снимке видно, что производительность сегмента корпоративной сети колебалась от 50000 до 200000 октетов в секунду (рабочий режим). Затем скачок скорости до 330000 и 600000 октетов в секунду. Была достигнута “точка насыщения”, после чего резкое снижение в ноль.

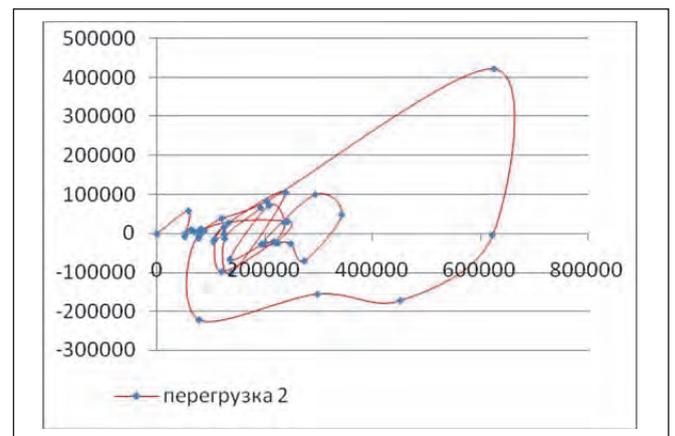


Рис. 5. Перегрузка порта в условиях предыдущего теста до состояния потери кадров

Перегрузка порта в условиях предыдущего теста до состояния потери кадров

Снимок соответствует перегрузке и потере кадров. На снимке видно, как после момента перегрузки передача практически останавливается. Очевидно, это связано с тем, что происходит отправление накопленных

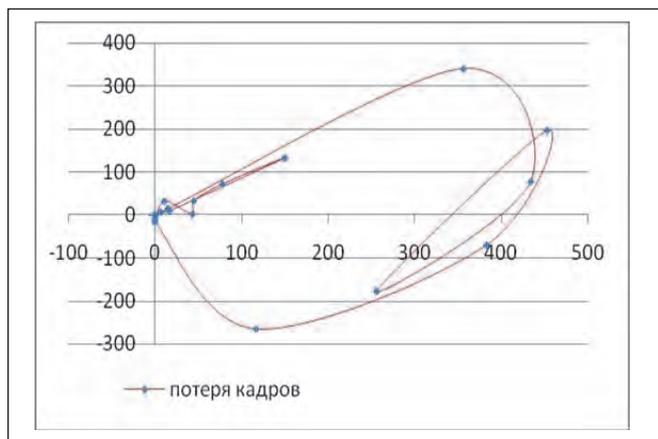


Рис. 6. Фазовый снимок соответствующей потери кадров

кадров и запрос на повтор потерянных. После этих мероприятий очередь кадров опять насыщается (малый виток на рисунке “перегрузка 2”), что опять влечет за собой потери, и уменьшается с понижением нагрузки.

Таким образом, при помощи фазовых траекторий можно идентифицировать состояние компьютерной сети и спрогнозировать появление критического события. Результаты анализа методов прогнозирования сложных технических объектов, к которым относится компьютерная сеть, показывают, что для прогнозирования состояний компьютерной сети наибольшую итоговую оценку получил предлагаемый метод верификации фазовых снимков.

Метод можно также применять не только для прогнозирования состояний компьютерной сети, но и в следующих областях:

- прогнозирование экономических процессов;
- прогнозирование землетрясений и извержений вулканов;
- прогнозирование погоды;
- прогнозирование дорожных пробок;
- другие области применения, в которых можно выделить факторы, влияющие на систему.

ЛИТЕРАТУРА

1. Иванов И.А., Леохин Ю.Л. Интеллектуальное управление компьютерными сетями //

Автоматизация и современные технологии. 2006. № 12. С. 26-31.

2. Леохин Ю.Л. Архитектура современных систем управления корпоративными сетями // Качество. Инновации. Образование. 2009. № 2. С. 54-63.

3. Мельников Д.А. Информационные процессы в компьютерных сетях. – М.: Кудиц-Образ, 1999. 256 с.

4. Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы. 3-е изд. – СПб: Издательство «Питер», 2008. 958с.

5. Пятибратов А.П., Гудыно Л.П. Вычислительные системы, сети и телекоммуникации. – М.: Финансы и статистика, 2001. 512с.

6. Назаров А.В, Лоскутов А.И. Нейросетевые алгоритмы прогнозирования и оптимизации систем. Наука и техника. – СПб, 2003. С. 384.

7. Пьявченко А.О., Вакуленко Е.А., Качанова Е.С. Распределенная система идентификации и контроля доступа // Известия ЮФУ. Технические науки №11. – Таганрог: Издательство ТТИ ЮФУ, 2008.

8. Сидельников Ю.В. Системный анализ технологии экспертного прогнозирования. – М.: Изд-во МАИ, 2007. С. 453.

9. Фатхутдинов Р.А. Управленческие решения. – М.: Инфра-М, 2002. С. 314.

10. Anil Jain, Ruud Bolle, Sharath Pankanti. Biometrics: Personal Identification in Networked Society. – USA, Massachusetts, Kluwer Academic Publishers, 2002. С. 419.

11. Lawrence O’Gorman, Michael J. Sammon, Michael Seul. Practical Algorithms for Image Analysis: Description, Examples, Programs and Projects. – USA, New York, Cambridge University Press, 2008. С. 355.

Леохин Юрий Львович,
д-р техн. наук, профессор,
нач. научно-исследовательской части МГИЭМ
leo@miem.edu.ru

Зубков Роман Сергеевич,
аспирант МГИЭМ.