

СПбГУТ  
**68-я**

РЕГИОНАЛЬНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ СТУДЕНТОВ, АСПИРАНТОВ  
И МОЛОДЫХ УЧЕНЫХ

22 – 23  
апреля  
2014



Студенческая весна  
С.-Петербург 2014

**СБОРНИК НАУЧНЫХ СТАТЕЙ**

УДК 378:621.395.34:004:654.9:001.891.31

ББК 74.58

С 23

68-я региональная научно-техническая конференция студентов,  
С 23 аспирантов и молодых ученых «Студенческая весна – 2014» : сб.  
научных статей [Электронный ресурс] / Под ред. С. М. Доценко;  
сост. А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков. – СПб. :  
СПбГУТ, 2014. – 463 с.

В научных статьях участников конференции исследуются со-  
стояние и перспективы развития мирового и отечественного уров-  
ня ИТ и телекоммуникаций.

Предназначено студентам, аспирантам и специалистам отрасли  
связи.

УДК 378:621.395.34:004:654.9:001.891.31

ББК 74.58

Издание подготовлено  
редакцией электронного журнала  
«Информационные технологии и коммуникации»  
[www.itt.sut.ru](http://www.itt.sut.ru)

© Авторы статей

© СПбГУТ

## **ОРГАНИЗАЦИОННЫЙ КОМИТЕТ ))))**

### *Сопредседатели*

Машков Г. М. – доктор технических наук, профессор,  
первый проректор – проректор по учебной работе СПбГУТ  
Доценко С. М. – доктор технических наук, профессор,  
проректор по научной работе СПбГУТ

### *Заместитель председателя*

Владыко А. Г. – кандидат технических наук,  
начальник управления организации научной работы  
и подготовки научных кадров

### *Ответственный секретарь*

Аникеевич Е. А. – кандидат технических наук,  
начальник отдела организации научно-исследовательской работы  
и интеллектуальной собственности

Иvasишин С. И. – кандидат технических наук  
начальник учебно-методического управления

Алексеенко И. А. – кандидат педагогических наук  
начальник управления маркетинга и рекламы

Шушпанов Д. В. – кандидат технических наук, доцент  
департамент фундаментальной подготовки

Пацкан М. Ю. – начальник управления эксплуатации  
инфокоммуникационных систем

Понамарёва Е. Ю. – начальник редакционно-издательского центра

## **ИНФОРМАЦИОННАЯ ПОДДЕРЖКА)))**



**WWW.ITT.SUT.RU**  
**ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ**  
**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**  
**И ТЕЛЕКОММУНИКАЦИИ**

**ЭЛЕКТРОННОЕ ПЕРИОДИЧЕСКОЕ ИЗДАНИЕ**

## С О Д Е Р Ж А Н И Е

Пленарное заседание . . . . .	5
Радиотехнологии связи . . . . .	14
Инфокоммуникационные сети и системы . . . . .	27
Информационные системы и технологии . . . . .	138
Теоретические основы радиоэлектроники . . . . .	225
Экономика и управление в связи . . . . .	231
Гуманитарные проблемы информационного пространства . . . . .	256
Сети связи специального назначения . . . . .	318
Аннотации . . . . .	417
Авторы статей . . . . .	443
Авторский указатель . . . . .	460

## ПЛЕНАРНОЕ ЗАСЕДАНИЕ

**УДК 004.89, УДК 004.75**

**Г. Г. Рогозинский (руководитель направления НОЦ СПбГУТ)**

### **РАСПРЕДЕЛЕННАЯ СИСТЕМА ГЕНЕРАЦИИ КОМПЬЮТЕРНОЙ МУЗЫКИ**

Компьютерная музыка – термин, вынесенный в заглавие доклада, связан с возникшими в середине 50-х годов прошлого столетия тенденциями в западной академической музыкальной среде после экспериментов ее представителей с вычислительной техникой. Это явление, в отличие от электронной музыки, под которой зачастую понимают традиционную поп-музыку, исполненную на синтезаторах, связано с вопросами использования компьютерной техники для создания новых тембральных пространств, реализации алгоритмических моделей для получения партитур музыкальных произведений и взаимодействием человек-машина в креативном процессе.

Первые эксперименты в области компьютерной музыки имели место в послевоенные годы. Профессоры университета Иллинойс Лежарен Хиллер (*Lejaren Hiller*) и Леонард Айзексон (*Leonard Isaacson*) в 1957 году получили первую в истории музыкальную композицию, написанную компьютером и названную *Illiad Suite* в честь этого компьютера. Для генерации партитуры струнного квартета использовались цепи Маркова с вероятностями перехода между состояниями, выявленными в результате предшествующего написанию композиции [1].

В том же году Макс Мэтьюз (*Max Mathews*), работая в компании Bell Labs, создал первую программу для генерации звука с помощью компьютера под названием **MUSIC**, которая в скором времени заинтересовала других ученых и композиторов и мотивировала их для дальнейшей работы с компьютерами в области создания новых тембров [2].

Спустя три десятилетия, когда компьютерная техника прошла значительный путь в своей эволюции, композитор и специалист в области компьютерного искусства Барри Верко (*Barry Vercoe*) в 1986 году на основе версии программы Макса Мэтьюза **MUSIC 11** разрабатывает язык музыкального программирования **Csound**, сыгравший важную роль в дальнейшем развитии компьютерной музыки [3].

Параллельно с совершенствованием технических средств для генерации компьютерной музыки и их освоением академическими композиторами

происходило развитие методов искусственного интеллекта, которые, в свою очередь, по мере их совершенствования, проникали в различные сферы деятельности человека, в том числе и в область компьютерной музыки, позволяя использовать язык алгоритмов и правил для формализации структур целых музыкальных произведений или их отдельных параметров.

На границе двух веков важными в области развития компьютерных музыкальных технологий стали процессы, связанные с переходом человечества к информационному обществу. Глобальная сеть Интернет, став крупнейшим инфокоммуникационным пространством, определила появление так называемых распределенных форм искусства, когда процесс создания того или иного произведения разделяется между участниками творческого процесса, которые могут находиться в разных частях света. Совершенствование технических средств обуславливает дальнейшее развитие подобных видов искусства. Так, один из видов телекоммуникационного искусства 80-х годов XX века фактически представлял собой передачу по факсу фрагментов изображений между медиахудожниками, при этом каждый участник процесса имел возможность модифицировать их тем или иным доступным ему способом [4], а работающий в настоящее время на десятках тысяч персональных компьютеров и мобильных устройств скринсейвер Electric Sheep генерирует абстрактную графику в соответствии с полученными ранее с других компьютеров сети генами [5].

В настоящее время, находясь у порога общества знаний и Интернета вещей, мы обладаем огромным потенциалом вычислительных средств, для которого является открытым вопрос возможных применений. При этом здесь по-прежнему прослеживается традиционное восхождение от решения сугубо утилитарных задач к проблемам эстетики и философии. В литературе часто приводятся данные о том, что шестая версия IP-протокола позволит распределить примерно 1500 адресов на квадратный ангстрем поверхности нашей планеты (или миллиарды IPv6 адресов на квадратный метр), что само по себе говорит об огромном потенциале нового сетевого пространства.

Самоорганизующаяся сеть устройств, находящихся во взаимодействии друг с другом, преобразующих и передающих различную информацию, поступающую на их датчики – вот актуальная концепция для новейших форм компьютерного искусства.

Такие формы искусства смогут развиваться теоретически неограниченно во времени. Тенденции к мобильности и портируемости приложений смогут подготовить ситуацию, когда практически на любом устройстве сети будет возможна в той или иной форме реализация алгоритмов генерации распределенного искусства. Большое количество устройств, работающих совместно над созданием произведения искусства, позволит обеспечить вариативность решений. Постоянно совершенствуемые алгоритмы обеспечат

трансформацию потоков информации из различных баз данных в структурные элементы генеративного искусства.

На протяжении практически двух лет исследовательской группой, возглавляемой автором доклада, ведутся работы по моделированию рассматриваемой системы генерации компьютерной музыки.

В качестве звукового ядра используется система Csound, являющаяся мультиплатформенным языком музыкального программирования с открытым кодом. Последняя версия Csound 6 работает во всех основных операционных системах и на мобильных устройствах с ОС Android и iOS. Кроме того, возможен запуск Csound на платформах Raspberry PI и BeagleBone [6].

Большой потенциал в области методов синтеза звука и алгоритмов обработки сигналов совместно с высокой портируемостью приложения определяет эффективность применения Csound для рассматриваемых задач.

Csound написан на языке С и имеет интерфейсы программирования приложений (*API*) практически ко всем основным языкам программирования, включая Python и Java. Последний позволяет осуществлять эффективную разработку Web-приложений, то есть реализовывать задачи прикладного уровня для разрабатываемой системы генерации компьютерной музыки.

Совместно с ядром генерации звукового контента работает ядро искусственного интеллекта, которое несет важную задачу управления данными, поступающими с датчиков и передаваемыми от других устройств внутри сети. Помимо преобразования информации, в ядре искусственного интеллекта должен выполняться анализ и извлечение знаний в соответствии с разработанной онтологией.

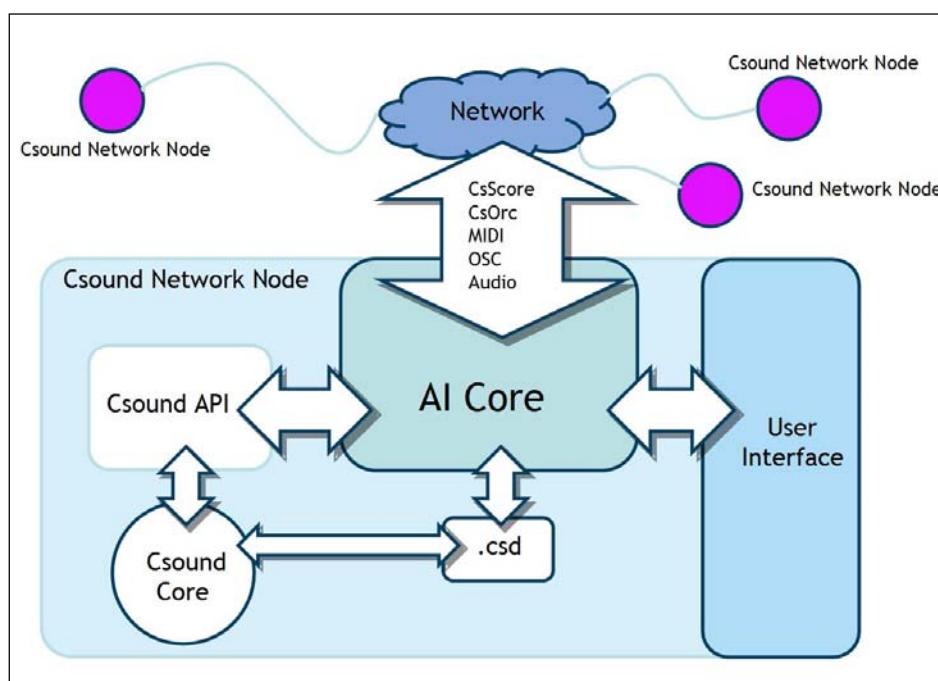


Рисунок. Структурная схема одного узла системы генерации компьютерной музыки

На рисунке представлена структурная схема одного из узлов моделируемой системы. Звуковое ядро Csound Core через интерфейс программирования приложений Csound API взаимодействует с ядром искусственного интеллекта AI Core. Пользователь имеет возможность оказывать влияние на работу локального узла через интерфейс пользователя User Interface.

Передача данных происходит в различных форматах. Для описания структуры алгоритма генерации звука используются собственные форматы системы Csound – Csound Document (*.csd*), Csound Score (*.sco*) и Csound Orchestra (*.orc*). Кроме того, возможна передача фрагментов звуковых данных в формате wav и специализированных сигналов управления в форматах MIDI (*Musical Instrument Digital Interface*) и OSC (*Open Sound Control*).

С самого начала в систему закладывается принцип динамического обновления. Модульный принцип построение инструментов в Csound обуславливает такой подход. Каждый инструмент представляет собой сеть примитивов (опкодов), которые обмениваются различными данными – звуком или сигналами управления. Фрагменты кода на языке Csound для синтеза и обработки звука могут модифицироваться со временем, алгоритмы, определяющие композиционные модели системы также могут изменяться, тем самым обеспечивается изменение музыкального контента, производимого системой в процессе работы.

С точки зрения анализа самого аудиоконтента, производимого кластером узлов системы, непрерывность процесса генерации музыкального материала накладывает некоторые ограничения на его содержание. С позиции упрощения композиционной модели непрерывно генерируемый аудиоконтент должен базироваться на ритмической, динамической, тембральной и пространственной музыкальных составляющих в гораздо большей степени, чем на мелодической и гармонической, во избежание проблем, связанных с мелодико-гармоническими аспектами музыкального контента. Это характерно для некоторых современных музыкальных жанров, таких как эмбиентная и этническая музыка, различные стили drum'n'bass и их производные, где мелодии, как правило, отводится менее значимая роль, чем ритму или гармонии. С другой стороны, современные авангардные композиционные техники, такие как спектральная музыка, интегральный сериализм и минимализм так же интересны с точки зрения выявления правил для генерации музыкального материала, так как часто основываются на реализации предкомпозиционных моделей и могут до определенной степени быть подвергнуты формализации.

#### Список используемых источников

1. **Experimental Music: Composition With an Electronic Computer/** L. Hiller and L. Isaacson. – Westport, Conn: Greenwood Press., 1979.
2. **Electronic and Computer Music /** P. Manning. – Oxford University Press, 2004.

3. **Ways Ahead: Proceedings of the First International Csound Conference /** ed. J. Heintz, A. Hofmann, I. McCurdy. – Cambridge Scholars Publishing, 2013.
4. **Telecollaborative Art Projects of Electronic Cafe International Founders.** – URL: <http://www.e cafe.com/museum/history/ksoverview2.html> (Дата обращения 23.05.2014).
5. **The Electric Sheep Screen-Saver: A case Study in Aesthetic Evolution /** S. Draves. – Spotworks, San Francisco CA, USA .
6. **Csound Journal.** – URL: [http://www.csounds.com/journal/issue18/beagle\\_pi.html](http://www.csounds.com/journal/issue18/beagle_pi.html) (Дата обращения 23.05.2014).

**УДК 535.317.23**

**А. В. Бахолдин (доцент кафедры ПиКО НИУ ИТМО)**  
**В. С. Шевкунов (студент магистратуры НИУ ИТМО)**

**ТЕОРЕТИЧЕСКОЕ И ПРАКТИЧЕСКОЕ МОДЕЛИРОВАНИЕ  
РАБОТЫ ОСВЕТИТЕЛЬНЫХ СИСТЕМ  
С ИК-ИСТОЧНИКОМ ИЗЛУЧЕНИЯ**

Осветительные системы, в основе которых лежит инфракрасный источник излучения имеют широкое применения в наблюдательных приборах, если нужно скрыть факт наблюдения, а также в приборах, передающих на расстояние путём освещения датчика закодированный сигнал.

С развитием сферы развлекательных услуг, всё большую популярность получает обновленная версия давно традиционного «пейнтбола». Инновация состоит в том, что вместо шариков с краской используется энергетический поток диода, излучение которого не попадает в видимую область. Закодированный в импульсах светодиода сигнал, пройдя через оптическую систему «оружия» стреляющего регистрируется приёмниками оптического излучения на одежде «мишени», после чего включается звуковая индикация, тем самым сообщая о попадании. Обновленная версия игры заняла свою коммерческую нишу в странах Запада и стала только появляться в городах России и СНГ [1].

С недавнего времени появилась необходимость разработки отечественной системы для дальнейшего внедрения в производство для коммерческого использования и проведения молодёжных спортивных соревнований.

Ввиду опыта наиболее комфортной игры, было сформулировано техническое задание, согласно которому диаметр пятна на дистанции 100 м должен составлять 1 м. Длина оптической системы не более 400 мм максимальный диаметр линз – 40 мм (табличные ограничены внутренним пространством корпуса). Длина волны излучения  $940 \text{ нм} \pm 50 \text{ нм}$ .

Был произведен обзор полимерных материалов, параметры которых представлены в таблице 1, для изготовления оптических компонентов, из

технических и экономических соображений был выбран материал полиметилметакрилат [2].

ТАБЛИЦА 1. Обзор материалов

Материал	CR-39	Трайвекс	Поликарбонат	Полиуретаны	Полиметилметакрилат	Стекло K8
Показатель преломления	1,49–1,50	1,53	1,59	1,64–1,74	1,49	1,52
Плотность, г/см <sup>3</sup>	1,31	1,11	1,2	1,3–1,5	1,16	2,51
Число Аббе	54–60	43–45	28–30	32–42	57	64

Излучение происходит в импульсном режиме, что позволяет развить большой ток без ущерба для светодиода, получая при этом значительную силу света для «пристрелки» с больших расстояний, поэтому был произведёт отбор источников излучения с учётом только следующих параметров:

- половинный угол рассеивания;
- размер источника;
- энергетические параметры;

Были выбраны светодиоды немецкой марки OSRAM. Данная марка была выбрана преимущественно из-за того, что производитель выкладывает в открытый доступ на официальном сайте файлы-модели, созданные по измерениям реального светодиода, где содержатся данные о ходе его лучей, которые можно использовать в расчётах в программах автоматизированного проектирования оптических систем.

Для трёх выбранных светодиодов (параметры приведены в таблице 2) был проведён габаритный расчёт [3]. Для того, чтобы уложиться в заданные габариты системы, так же максимально уменьшить длину системы решено использовать систему типа «телеобъектив». Для дальнейшего компьютерного моделирования и корректировки результатов была выбрана среда разработки оптических систем Zemax.

ТАБЛИЦА 2. Технические параметры инфракрасных источников излучения

Наименование ИК-источника	Половинный угол рассеивания, $\phi^\circ$	Диаметр, $2y$ , мм	Максимальный ток при импульсном питании, мА	Поток при максимально возможном токе, мВт	Поток при максимально возможном токе, мВт
Osram SFH4045	$\pm 9$	1,7	700	280	900
Osram SFH4248	$\pm 15$	2,6	1000	650	750
Osram SFH4545	$\pm 5$	5	1000	550	2600

На основе имеющихся данных о размере светящегося источника был произведён габаритный расчёт, высчитаны фокусные расстояния систем:

$$f' = \frac{y'}{\operatorname{tg}\omega}, \quad (1)$$

$$\operatorname{tg}\omega = \frac{D_{\Pi}}{2L}, \quad (2)$$

где  $\omega$  – угловой размер пятна,  $2y'$  – размер светящегося тела светодиода (представлены в таблице 2),  $D_{\Pi}$  – диаметр пятна рассеивания,  $L$  – расстояние от источника до пятна [4].

После расчёта фокусных расстояний получено, что две из трёх систем выходят за габариты 400 мм, поэтому было решено использовать двухкомпонентную оптическую систему, общий вариант, которой представлен на рисунке 1.

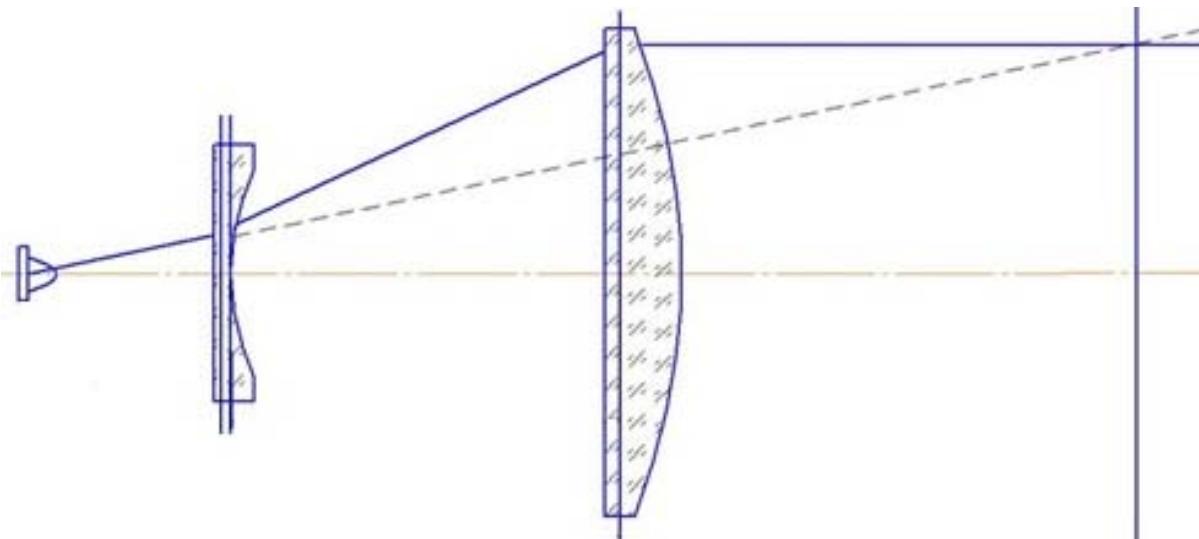


Рис. 1. Двухкомпонентная оптическая система

Для трёх моделей светодиодов были смоделированы системы, произведена оптимизация для достижения наименьших габаритов. Таблица 3 отражает конструктивные параметры полученных систем. Пятна рассеяния потока от системы показывают распределение облученности для каждой системы и представлены на рисунке 2 (а, б, в).

ТАБЛИЦА 3. Конструктивные параметры полученных систем

	Радиус, мм	Толщина, мм	Марка	Световые диаметры, мм
SFH4545 (а)	$\infty$	4,0	ПММА	8,5
	35,13	150,0	–	8,65
	$\infty$	4,0	ПММА	34,5
	-93,57	–	–	3,0
SFH4248 (б)	$\infty$	4,0	ПММА	8,2
	52,816	153,2	–	8,5
	$\infty$	4,0	ПММА	34,5
	-92,61	–	–	35
SFH4045 (в)	$\infty$	4,0	ПММА	8,2
	23,96	113,8	–	8,5
	$\infty$	4,0	ПММА	34,5
	-65,58	–	–	35,0

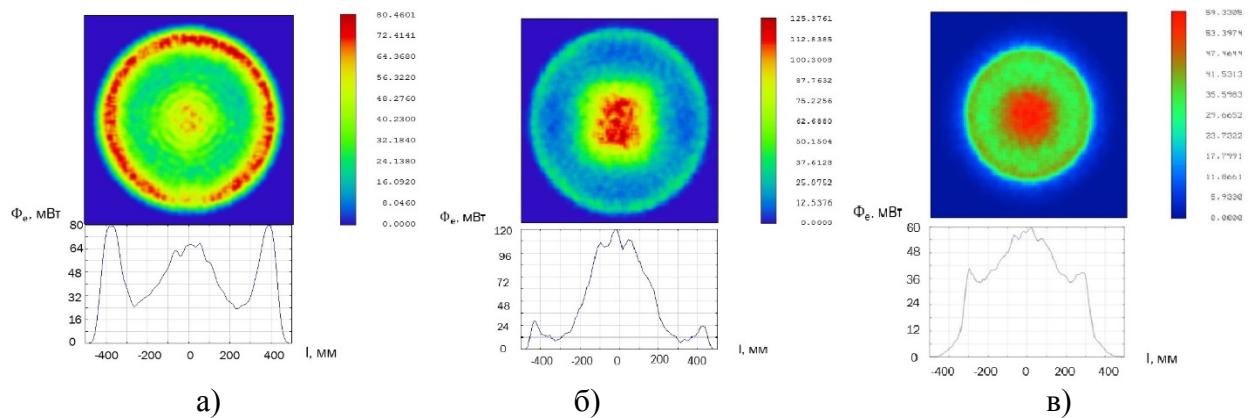


Рис. 2. Распределение облученности на площадке 1x1 метр для трёх разных систем:  
 а) система с ИК-диодом SFH4545, б) система с ИК-диодом SFH4248,  
 в) система с источником SFH4045

Анализируя каждую из полученных систем, можно назвать её более или менее удачной. Рассмотрев пятно, полученное от системы с ИК-диодом SFH4545 (рис. 2 а), нельзя не заметить наличие яркого кольца на периферии светового пятна. Вероятней всего, при увеличении фоновой засветки могут возникнуть ситуации, когда срабатывание приемника будет не в центре пятна, а на периферии – эффект «сбитого прицела». При использовании системы с ИК-диодом SFH4248 (рис. 2 б), пятно имеет более плавное распределение облученности в пятне, что более благоприятно при работе с увеличенной фоновой засветкой. Распределение облученности на приёмнике от системы с источником SFH4045 (рис. 2 в) можно было бы использовать для будущего усовершенствования самой игры, а именно: при тонкой настройке приёмника, периферийная область, попадая на него, распознавалась бы никак «попадание», а как «просвистевшая мимо пуля», что технически позволяет звуковая визуализация игры.

Допуски на точность изготовления всех линз и точность их установки в схему обеспечивают технологичность системы и не требуют специальной юстировки или повышенной точности изготовления. На рисунке 3 представлен внешний вид макета одной из систем.



Рис. 3. Внешний вид макета системы

1. **Преимущества** лазертага [Электронный ресурс]. – Режим доступа: <http://russianlasertag.ru/nashi-preimushhestva/> свободный. Загл. с экрана. Яз. рус.
2. **Полимерные** материалы [Электронный ресурс]. – Режим доступа: <http://www.optikomania.ru/plastic.php>, свободный. Загл. с экрана. Яз. рус.
3. **Сайт** производителя ИК-диодов OSRAM [Электронный ресурс]. – Режим доступа [http://www.osram.ru/osram\\_ru/](http://www.osram.ru/osram_ru/) свободный. Загл. с экрана. Яз. Рус.
4. **Прикладная** оптика. Часть 1 / Г. И. Цуканова. – СПб. : СПбГУ ИТМО, 2008 – 34 с.

Для большей точности экспериментов, система устанавливалась на штатив, диаметр пятна проверялся с помощью инфракрасной камеры. Измерения дальности действия системы проводились с использованием приёмника, используемого в игре на одежде игроков. Сигнал был получен на расстоянии 50 м, 75 м и 100 м.

#### Список используемых источников

1. **Преимущества** лазертага [Электронный ресурс]. – Режим доступа: <http://russianlasertag.ru/nashi-preimushhestva/> свободный. Загл. с экрана. Яз. рус.

2. **Полимерные** материалы [Электронный ресурс]. – Режим доступа: <http://www.optikomania.ru/plastic.php>, свободный. Загл. с экрана. Яз. рус.

3. **Сайт** производителя ИК-диодов OSRAM [Электронный ресурс]. – Режим доступа [http://www.osram.ru/osram\\_ru/](http://www.osram.ru/osram_ru/) свободный. Загл. с экрана. Яз. Рус.

4. **Прикладная** оптика. Часть 1 / Г. И. Цуканова. – СПб. : СПбГУ ИТМО, 2008 – 34 с.

# РАДИОТЕХНОЛОГИИ СВЯЗИ

УДК 004.7

**Д. К. Артур (аспирант кафедры РПдУ и СПС СПбГУТ)**

## USING THE CONCEPT OF QoS AND QoE IN EVALUATING THE IEEE 802.16 STANDARD

QoS is defined as the ability of the network to provide a service at an assured service level. QoS encompasses all functions, mechanisms and procedures in the cellular network and terminal that ensures the provision of the negotiated service quality between the subscriber station and the core network (CN) [1, 2].

One of the notable features of IEEE 802.16 wireless MAN is that it is designed to support a variety of services with QoS requirements, while providing high-bandwidth network accessibility and seamless roaming support for high-mobility users. Compared to conventional packet-switched networks (e.g., the original Internet), which were designed to provide best-effort service and do not provide full reliability in support of QoS-demand services, IEEE 802.16 wireless MAN aims at providing better service (better than best effort) to various classes of network traffic, which is called QoS.

But one main challenges for the IEEE 802.16 standard is to simultaneously provide QoS for various service flows that have very different QoS characteristics due to the fact that these service flows have different QoS requirements. To cope with these issues, the QoS in wireless networks is usually managed at the Medium Access Control (MAC) layer. In the MAC layer of IEEE 802.16 wireless MANs, four types of scheduling service flows are defined. These service flows and their usage rules are presented in table.

TABLE. Scheduling services and usage rules

Scheduling type	PiggyBack Request	Bandwidth stealing	Polling
UGS	Not allowed	Not allowed	PM bit is used to request a unicast poll for bandwidth needs of non-UGS connections
rtPS	Allowed	Allowed	Scheduling only allows unicast polling
nrtPS	Allowed	Allowed	Scheduling may restrict a service flow to unicast polling via the transmission/request policy; otherwise all forms of polling are allowed
BE	Allowed	Allowed	All forms of polling allowed

The IEEE 802.16 MAC is defined as connection oriented to support QoS for the above scheduling services. Every service, including an inherently connectionless service (packet service like IPv4, IPv6), is mapped to a connection. Each downlink connection has a packet queue at the BS. The BS downlink scheduler selects the next transmitted packets from those queues for the transmission to SSs in the next frame. The packet selection from the queue is based on the QoS demands of each connection and the current status of queues. On the other hand, each uplink connection has a packet queue at the SSs. The SSs uplink scheduler selects the next transmitted packets from those queues for the uplink transmission to BS based on the QoS requirements, the current status of the queues, as well as the grants from the BS.

Two types of bandwidth request are defined. One is incremental, and the other is aggregate. Incremental requests indicate that the connection still needs the quantity of bandwidth requested besides its current perception of the bandwidth need. On the contrary, the aggregate bandwidth request states the total quantity of bandwidth needed by the connection. The QoS for IEEE 802.16 wireless MAN applications cannot be achieved in a straightforward manner, as illustrated above and should be addressed from many other aspects. The design factors for QoS management addressed in this paper include admission control, packet scheduling, and buffer management.

The connection admission control is used to limit the number of connections/flows admitted into the network so that each individual connection/flow can get its desired QoS. It consists of key actions taken by the network during the connection setup phase to decide whether an incoming connection can be accepted into the network. The decision is made based on whether the QoS requirement of the incoming connection violates the QoS of existing connections. Therefore, before a decision is made, the network has to evaluate the QoS attributes of both the incoming connection and the existing connections. A connection can be accepted only if sufficient resources (bandwidth) are available to establish the connection with its required QoS, while the promised QoS (minimum transmission rate, maximum delay) of existing connections in the network must not be significantly affected by the new connection. The received QoS may be better than the promised QoS when network resources are sufficient. Connection admission control has to predict the fraction of the network resources that will be consumed by the traffic generated by each service. And the strategy and policy of connection admission control shall vary according to the type of services – UGS, rtPS, nrtPS, or BE – and also depend on the stochastic nature of the traffic of services.

The determination of transmission sequence is accomplished by a process of packet scheduling. Packet scheduling is a part of traffic control in the networks and is referred to as the decision process used to choose which packet should be sent out first. In the connection-oriented network, connection admission control is deemed to resource reservation at the connection level; packet scheduling, on the other hand implements fair resource allocation in the packet level. The general

packet scheduling algorithms include first in, first out (FIFO), round-robin, fair queuing, weighted fair queuing, etc. In FIFO, packets are forwarded in the same order in which they arrive at the transmitter. Round-robin and fair queuing are used for best-effort scheduling, and weighted fair queuing can be used as the QoS provision scheduling strategy.

Furthermore, buffer management achieves the QoS control by stipulating the buffer size and determining which packet to be dropped if the buffer is overflowed. Like network bandwidth, buffers are another network resource whose consumption should be controlled. The buffer management regulates the occupancy of a finite buffer queue. The buffer management makes the decision to admit or drop an incoming packet into the queue according to the state information, such as the content of the buffer queue, the flow to which the packet belongs, the number of packets in the flow current in the buffer queue.

All these parameters are configured by the network operators to give a certain QoS but QoE on the other hand is how a user perceives the usability of a service when in use – how satisfied one is with a service in terms of, for example, usability, accessibility, retainability and integrity of the service. Flawless transmission of packets does not make for happy users. So, the inference that QoE is improved because QoS mechanisms are used to reduce jitter or average packet delivery delay may not be accurate in all circumstances. What is important is good user experience or QoE, and the goal of QoS should be to deliver a high QoE.

QoS is often treated as a bottom-up process, i.e. taking into account QoS parameters of only the core network with little consideration for what happens on an end-to-end basis. A top-down approach should rather be used. This will be focused on the end-user perspective and provide the service performance levels necessary for a high QoE for the user. In practice, this means focusing on the customer – that is, the person who pays the bill – understand end-user expectations for QoS performance (QoE), and use these to drive requirements for specific QoS mechanisms (functions) for individual network domains such as SS, access, core, backbone and external packet data networks, and corresponding interfaces. The conceptual models of end-to-end QoE and QoS adopted in this paper is illustrated in Figure.

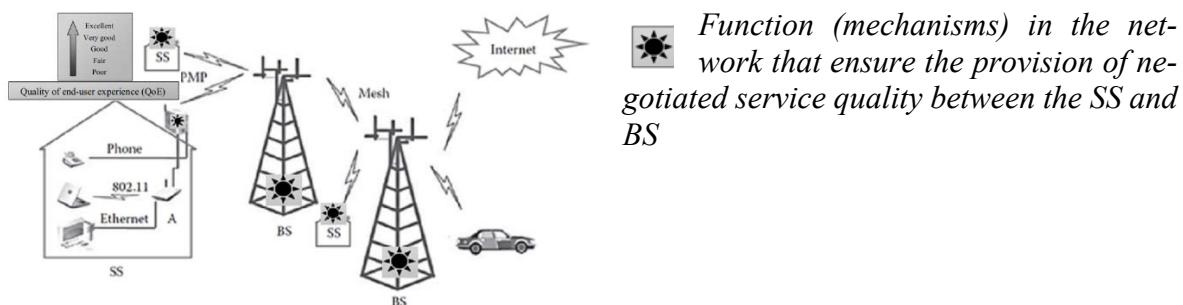


Figure. QoE is expressed in ‘feelings’ rather than metrics. QoS relates to all mechanisms, functions and procedures in the network and terminal that implement the quality attributes (bearer service) negotiated between the SS and BS

**Список используемых источников**

1. **QoS and QoE Management in UMTS Cellular Systems** Edited by David Soldani / Man Li and Renaud Cuny. – John Wiley & Sons, Ltd, 2006. – PP. 1–7.
2. **Wireless Quality of service** Edited by Maode Ma / Mieso K. Denko, Yan Zhang. – 2009 by Taylor & Francis Group, LLC. – PP. 115–145.

*Статья представлена научным руководителем канд. техн. наук, доцентом В. Е. Коротиным*

**УДК 004.7**

**А. С. Лежепёков (студент группы РМ-12 СПбГУТ)**

## **ПРОЕКТИРОВАНИЕ ВЫСОКОНАГРУЖЕННОЙ БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ СЕТИ WI-FI**

Wi-Fi («*Wireless-Fidelity*») – стандарт на оборудование Wireless LAN. Разработан консорциумом Wi-Fi Alliance в 1991 году, «Wi-Fi» – торговая марка «Wi-Fi Alliance» для беспроводных сетей на базе стандарта IEEE 802.11 [1].

Для создания Wi-Fi сети необходимо не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (*Ad-hoc*), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую», но проектирование такой сети в этом докладе рассматриваться не будет.

Главная проблема в организации рассматриваемой сети заключается в удовлетворении требований абонентов, отсутствии избыточности технического оборудования и обеспечения полного покрытия местности.

На сегодняшний день самый популярный подход к решению проблемы – приблизительная закупка технического оснащения и попытка реализации без какого-либо радиоисследования местности на наличие интерференции, что является в корне неверным решением.

Рассмотрим преимущества и недостатки нескольких актуальных на сегодняшний день способов проектирования сети:

- определение количества абонентов на точку доступа с последующим расчётом количества необходимого оборудования,
- размещение точек доступа с помощью специализированного ПО с обеспечением уровня сигнала не ниже заданного порога (например, – 65 дБм),
- способ, разработанный Andrew von Nagy, основанный на расчёте «эфирного времени» каждого пользователя.

Рассматривая первый способ расчёта «20 абонентов на точку доступа» для аудитории, рассчитанной на 150 человек, и, учитывая максимальный одновременный доступ, получаем 8 точек доступа (рис. 1). Такой способ не отнимает много времени и средств на проектирование, но абсолютно не учитывает потребности пользователей: тип радиомодуля, скорость работы в сети и прочие немаловажные параметры.

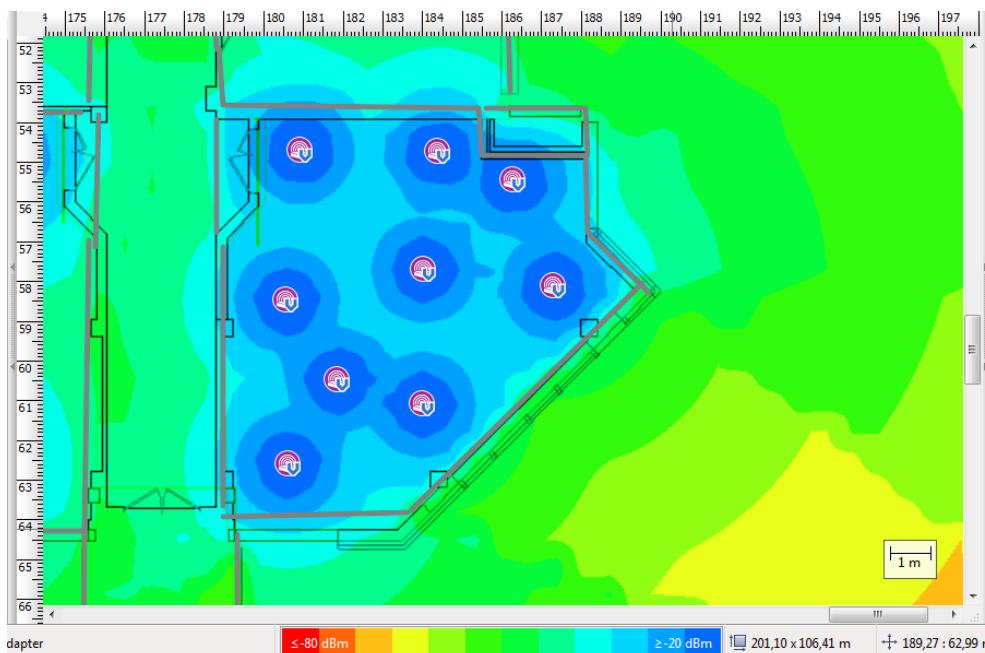


Рис. 1. Реализация первого способа проектирования в ПО TamoGraph Site Survey

Обращаясь ко второму («энергетическому») способу, мы расставляем в ПО TamoGraph Site Survey точки доступа так, чтобы обеспечить уровень сигнала на всей зоне покрытия не менее заданного (например,  $-65$  дБм) и получаем 3 точки доступа (рис. 2). Затратив небольшие усилия, мы снизили количество точек доступа на 5 – ощутимая экономия средств, но не выигрыш в ресурсах, которые мы предоставляем всё тем же 150 людям, находящимся в аудитории.

Решением проблем первого и второго способа является следующий метод проектирования – способ, созданный одним из ведущих Wi-Fi-экспертов в мире – Andrew von Nagy. Этот способ учитывает «эфирное время», поддерживаемые скорости и типы адаптеров каждого пользователя сети.

За основу взят третий этаж и, исходя из статистических данных с учётом пригодности этой сети в перспективе нескольких лет вперёд, тогда на 100 % пользователей приходится:

- 60 % смартфонов;
- 25 % планшетов;
- 15 % переносных ПК.

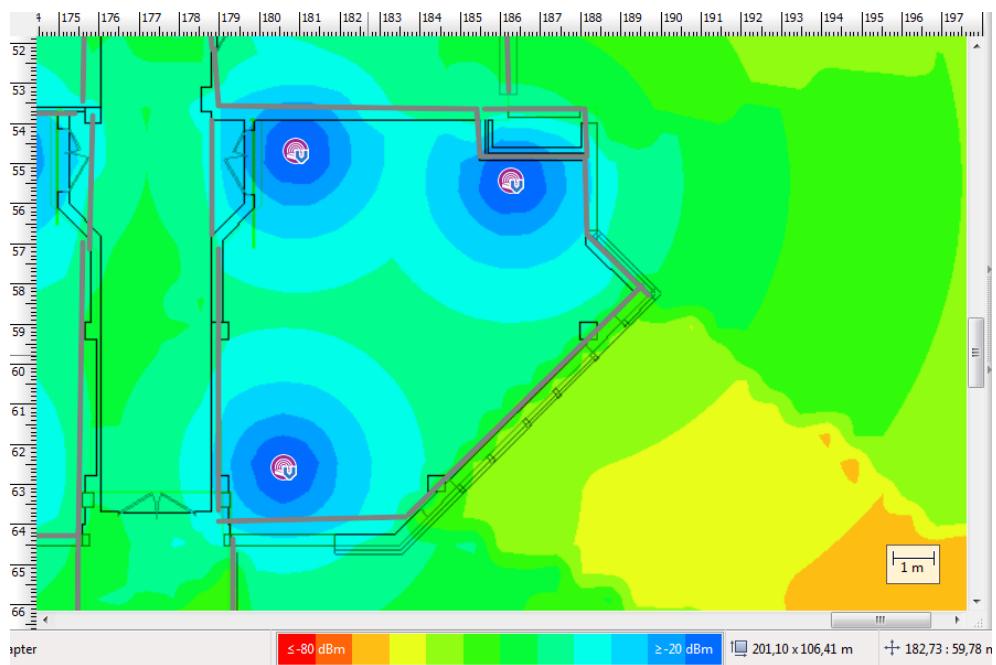


Рис. 2. Реализация «энергетического» способа проектирования в ПО TamoGraph Site Survey

Используя таблицу характеристик этих устройств, рассчитаем «эфирное время» с учётом, что примерно 80 % пользователей обновляет социальные сети, почту, используя этим порядка 1 Mbps, а остальные 20 % выполняют сторонние операции с файлами, используя этим около 5 Mbps. Далее берём во внимание, что приблизительно 70 % устройств использует радиомодуль 2,4 ГГц, а оставшиеся 30 % – 5 ГГц и составим таблицу (рис. 3) с расчётами для каждой аудитории.

	A	B	C	D
1	Номер аудитории	Количество человек	Нагрузка 2.4 ГГц, %	Нагрузка 5 ГГц, %
15	414	50	232	51
16	415	45	212	47
17	416	15	82	28
18	417	15	82	28
19	418	18	90	31
20	419	18	90	31
21	420	19	95	31
22	421	19	95	31
23	422	19	95	31
24	423	8	49	23
25	424	6	39	23
26	425	2	26	20
27	426	5	39	20
28	427	8	49	23
29	428	8	49	23
30	429	1	20	20
31	430	3	26	20
32	431	3	26	20
33	432	10	59	25
34	433	0	0	0
35	434	11	59	25
36	435	14	76	28

Рис. 3. Таблица MS Excel с результатами вычисления «эфирного времени»

В целях экономии времени, мною был реализован алгоритм вычисления максимальной нагрузки средствами языка программирования PHP и разметкой HTML. Тогда для искомой аудитории, вместимостью 150 человек, мы получаем следующий результат (рис. 4).

## Расчёт сектора

Количество человек:

Device Category	Airtime in 20 Mhz	Airtime in 40 Mhz
Laptops	32.7777777777778%	20.833333333333%
Smart Phones	165.44117647059%	0%
Tablets	91.176470588235%	76.470588235294%

**Sum # AP:** 4 (310%) on 20 mHz + 2 (118%) on 40 mHz

**Concurrent clients:** 150

Рис. 4. Результат расчёта количества точек доступа для 150 пользователей, учитывая исходные данные

Итоговая максимальная нагрузка с учётом запаса мощности и учтённых требований к сети ожидается 310 % (4 точки доступа) на диапазоне 2,4 ГГц и 118 % (2 точки доступа) на 5 ГГц, что соответствует 6 точкам доступа в сумме. Далее мы выбираем способ установки: либо комбинируем 4 точки доступа на 2,4 ГГц и две на 5 ГГц, либо 5 точек доступа с одновременной поддержкой 2,5/5 ГГц – принципиальной разницы нет.

Расчёчная часть окончена. Переходим к симуляции с помощью вспомогательного ПО, например, TamoGraph Site Survey. Создаем проект, обрисовываем план этажа (рис. 5) в соответствии с теми типами материалов, из которых он сделан, для того, чтобы учитывать интерференционные свойства при расставлении точек доступа. Устанавливаем роутеры (рис. 6) в соответствии с расчётной частью, конфигурируем сеть.

В результате мы имеем приближенную к реальной часть модели сети с широким спектром доступных визуализаций, о которых вы можете узнать непосредственно у представителя программного обеспечения.

Подводя итог, хотел бы отметить способ, представленный Andrew von Nagy, как наиболее эффективный на сегодняшний день, так как он учитывает и приближает теоретический расчёт максимально близко к тому, что ожидает нас на практике.

## Список используемых источников

1. Aerohive High-Density Wi-Fi Design Guide [Электронный ресурс] / A. Nagy // Aerohive Design & Configuration Guide High-Density Wi-Fi – Режим доступа:

[http://www.aerohive.com/330000/docs/help/english/documentation/Aerohive\\_High-Density\\_Wi-Fi-Design-Config-Guide\\_330073-02.pdf](http://www.aerohive.com/330000/docs/help/english/documentation/Aerohive_High-Density_Wi-Fi-Design-Config-Guide_330073-02.pdf) (Дата обращения 26.08.2014).

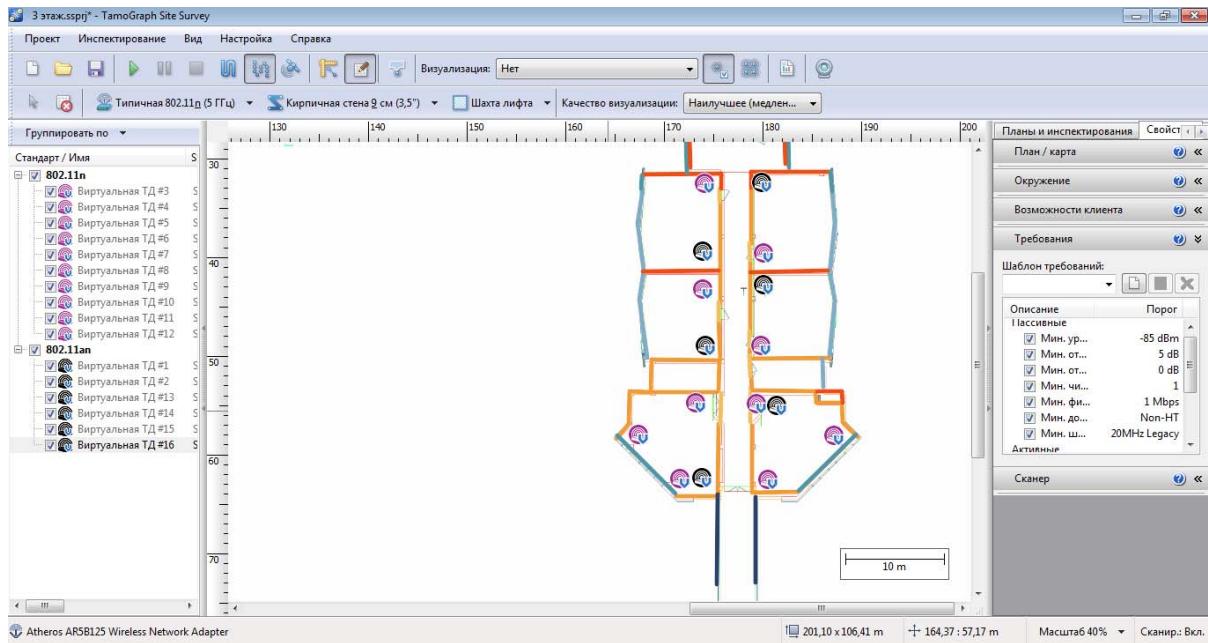


Рис. 5. Обрисовывание части плана третьего этажа в TamoGraph Site Survey

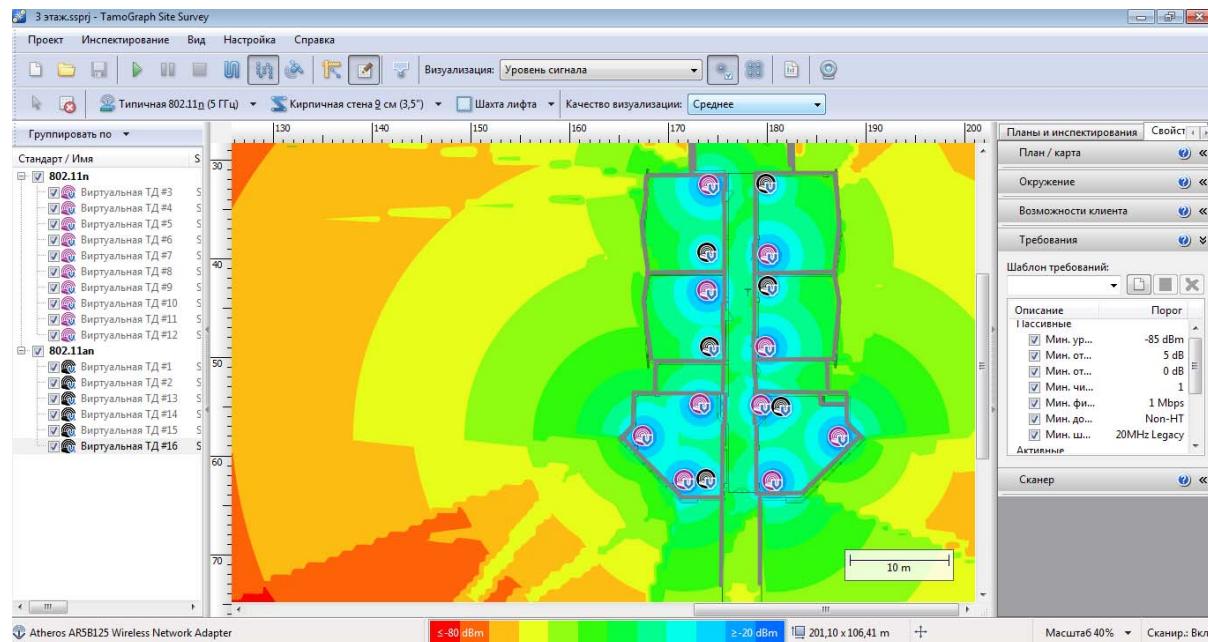


Рис. 6. Визуализация в TamoGraph Site Survey

Статья представлена научным руководителем,  
старшим преподавателем В. А. Лаврухиным.

**УДК 159.9.072.43**

**Д. А. Парицкая (студентка группы Р-05 СПбГУТ)**

## **ИСПОЛЬЗОВАНИЕ ФОНОВОЙ МУЗЫКИ В СИСТЕМЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

За последние несколько лет в сфере высшего образования осваивались различные технологии для повышения качества образования и преподавания. Хорошо известна польза фоновой музыки в начальной школе и дошкольном образовании, но это обстоятельство пока еще игнорируется в системе высшего образования. Цель данного исследования – показать достоинства использования фоновой музыки в высшем образовании и обозначить те направления в будущей работе, которые могли бы привести к окончательным доказательствам этого предположения.

### *Введение*

Довольно обычная ситуация: лектор монотонно читает возле доски, и веки некоторых студентов тяжелеют. Другие быстро отвлекаются, теряя суть темы.

Может быть, все-таки существует способ заставить мозг студентов работать эффективнее при том, что сами молодые люди этого осознавать не будут? Такой подход мог бы способствовать созданию комфортной среды обучения и содействовать более глубокому изучению предмета.

Вопрос в том, оказывает ли определенным образом подобранная фоновая музыка (или шум) какой-либо эффект (положительный или, наоборот, негативный) на процесс обучение в вузах. В данном исследовании сделана попытка проанализировать результаты исследований, выполненных в этой области, и сформулировать выводы о потенциальной пользе использования фоновой музыке в системе высшего образования.

Исследования содержат информацию о различных видах музыки, которую предположительно можно использовать в качестве фоновой, о том, как та или иная музыка влияет на наш мозг, а также о том, какими соображениями следует руководствоваться, чтобы выбрать наиболее подходящую музыку. А также сопровождается обзором исследований, проведенных в разных возрастных группах, для выявления характера фоновой музыки, наиболее подходящей для этих групп. При этом особое внимание уделено оценке ее позитивного влияния на студентов вузов. Даётся описание связи музыкальных способностей человека и эффективности фоновой музыки.

## Обзор видов фоновой музыки

Фоновая музыка – это музыка, звучащая «вторым планом», без установки на осознанное восприятие.

Возможно, из-за недостатка знаний фоновая музыка почти не применяется в вузах. Можно ли расширить эти знания и применять их для сферы обучения, как это делается на коммерческом рынке? В этом разделе мы попытаемся ответить на данный вопрос, проведя анализ воздействия музыки на мозг, и определив, как это воздействие может принести пользу процессу обучения и познания.

## Теория когнитивного обучения

Мозг фокусируется на меняющихся раздражителях (переходный процесс), игнорируя более стабильные, постоянные. Такую функцию фильтрации можно назвать «схемой адаптации». Знание о существовании этой функции адаптации приводит к созданию когнитивной теории обучения, которая поясняет, что человеческий мозг не способен обработать множество параллельных потоков информации. Очевидно, что отвлекающие факторы должны быть сведены к минимуму. Именно поэтому идея использования фоновой музыки в образовании для некоторых экспертов кажется недопустимой [1].

К счастью, исследования на этом чрезмерно обобщенном заключении не закончились. При последующих исследованиях обнаружилось, что обработка речи, фонового шума и музыки производится в разных частях головного мозга.

Если рассматривать процесс обучения, то фоновая музыка будет напрямую влиять на способность к восприятию и усвоению информации: либо положительно или отрицательно. В процессе учебного занятия (лекции) внимание студента время от времени может рассеиваться и способность к восприятию и запоминанию информации может снижаться, что приводит,



Рис. 1. Эффективность обучения как функция уровня внешнего возбуждения

соответственно, к снижению эффективности обучения. В таких ситуациях фоновая музыка способна действовать как положительный внешний раздражитель, повышая мотивацию к обучению. Но использовать этот раздражитель необходимо очень аккуратно, так как возможен и эффект перевозбуждения, который является помехой обучению и снижает работоспособность (рис. 1) [1, 2].

### Типы личности

Чтобы найти «золотую середину» при использовании фоновой музыки в качестве внешнего стимулятора для повышения качества обучения, необходимо рассмотреть различные типажи личности.

Исследования показывают, что экстравертам и интровертам требуется различное воздействие для достижения эффективного обучения [3]. Экстраверты способны вытерпеть гораздо большие уровни шумов, чем интроверты. Интровертам требуется меньшее внешнее воздействие. Идея в том, чтобы использовать музыку такого уровня, чтобы она положительно воздействовала на экстравертов и, в то же время, не отвлекала интровертов.

### Идеальные характеристики музыки

Исследования показали, что жанр не является определяющим признаком при выборе фоновой музыки. Влияние музыки больше определяется её темпом, тональностью, тембром, динамикой, мелодией и гармонией.

Наиболее эффективной оказывается музыка с темпом в интервале 60–120 BPM (*BPM – beats per minute*), а диапазон 70–110 BPM некоторыми исследователями определяется как идеальный. Кроме того, темп 60 BPM соответствует идеальной ЧСС (частоте сердечных сокращений) [4].

Много дискуссий было сосредоточено на определении идеального уровня воспроизведения фоновой музыки. В одной из рекомендаций говорится, что идеальный уровень фоновой музыки составляет 35 дБ, что, как правило, чуть выше естественного уровня фонового шума. Экспериментально установлено, что этот уровень обеспечивает максимальную внимательность и позволяет улучшить успеваемость. Для выбора фоновой музыки её жанр не так важен, но все же музыка должна быть инструментальной, чтобы при ее обработке избежать попадания информации в речевой центр мозга, который необходим для обработки речи лектора.

### Возрастной подход

Этот раздел призван собрать информацию о том, что в настоящее время известно о влиянии фоновой музыки на разные возрастные группы. Цель – дать рекомендации для применения музыки в области высшего образования.

Значительное количество исследований было сосредоточено на влиянии фоновой музыки на младших школьников (5–13 лет).

Выбор фоновой музыки для маленьких детей довольно широкий, так как дети меньше ассоциируют музыку с происходящими событиями [5]. Поэтому они имеют гораздо больше шансов извлечь из музыки необходимые эмоции, способствующие здоровому обучению.

Исследований, сфокусированных на влиянии фоновой музыке на взрослых, еще меньше. Существует достаточно большое количество литературы

по использованию музыкотерапии для взрослых, страдающих от соматических и психических заболеваний, но не охватывает влияние музыки в образовательной сфере. Также существуют работы, направленные на изучение негативных эффектах шумов на рабочем месте (фоновые разговоры, телефонные звонки и прочее).

Есть огромное количество информации о том, как влияет фоновая музыка на пожилых людей в контексте понимания и запоминания информации. Хотя этот возрастной диапазон выходит за рамки студенческого возраста, можно провести параллели между пожилыми и молодыми людьми с целью восполнения недостающей информации.

### *Связь с музыкальными навыками и способностями*

Влияет ли музыкальное образование и музыкальные способности на эффект воздействия фоновой музыки в сфере высшего образования? Исследований на эту тему нет. Но есть достаточное количество литературы о влиянии музыкального образования на дальнейшее обучение и успеваемость. Эти данные могут быть очень полезны для дальнейших исследований.

### *Выходы*

В виду того, что исследования рассматриваемой проблемы еще далеки от завершения, вопрос о том, имеет ли фоновая музыка позитивное влияние на умственные способности студентов вузов, следует считать пока открытым. Но в любом случае при выборе фоновой музыки необходимо учитывать те результаты, которые уже получены:

- 1) Узкий динамический диапазон.
- 2) Темп 60–80 ударов в минуту.
- 3) Уровень воспроизведения порядка 35–40 дБ (примерно на 6 дБ выше уровня шума).
- 4) Для студентов лучше использовать малознакомую музыку.
- 5) Музыку необходимо регулярно менять, чтобы избежать снижения положительного эффекта со временем.
- 6) Корректировки на основе обратной связи со стороны студентов (особенно в начальный период внедрения).
- 7) Музыка должна приносить пользу всем студентам, независимо от музыкального образования и навыков, хотя связь эта имеется.

Даже с учетом недостатка некоторых данных ясно, что фоновая музыка приносит пользу почти всем, а тем более студентам с музыкальным образованием. Исследования показывают, что улучшается восприятие информации, её запоминание, развивается критическое мышление.

Это, безусловно, является преимуществом для образовательной среды, и поэтому фоновая музыка должна быть опробована на уровне высшего образования.

### Список используемых источников

1. **Background** music and the learning environment: Borrowing from other disciplines / M. Griffin. – MSc dissertation, School of Education, University of Adelaide, Australia. June 2006.
2. **What** implications might research arousal have for educators? / E. Alpay. – Imperial College of Science, London (internal report), 2002.
3. **The** influence of musical distraction of varying complexity on the cognitive performance of extroverts and introverts / A. Furnham, K. Allass // European Journal of Personality. – 1999. – Vol. 13, No. 1. – PP. 27–38.
4. **An** exploratory investigation of responses elicited by music varying in tempo, tonality, and texture / J. J. Kellaris, R. J. Kent // Journal of Consumer Psychology, vol. 2, no. 4, p.381, 1993.
5. **Personality** and music preferences: The influence of personality traits on preferences regarding musical elements / M. Kopacz // Journal of Music Therapy. – 2005. – Vol. 42, No. 3. – P. 216.

*Статья представлена научным руководителем, доцентом В. А. Никаминым.*

## ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

**УДК 50.41.00, 50.37.23**

**А. Д. Алексеев (студент группы МБИ-22м СПбГУТ)**

### **ПРОТИВОДЕЙСТВИЕ АТАКАМ МЕТОДОМ ПЕРЕПОЛНЕНИЯ БУФЕРА**

Переполнение буфера (англ. *buffer overflow*) – название самой распространенной уязвимости в области безопасности программного обеспечения.

На сегодняшний день около 40 % всех известных уязвимостей в программном обеспечении приходится на переполнение буфера, а стало быть, обусловленные ими угрозы и связанные с этим проблемы безопасности являются наиболее актуальными [1, 2, 5].

Переполнение буфера может вызывать аварийное завершение или зависание программы, ведущее к отказу обслуживания. Наибольшую опасность представляют такие виды переполнений, как переполнение в стековом кадре, которые позволяют злоумышленнику загрузить и выполнить произвольный машинный код от имени уязвимой программы и с правами учетной записи пользователя, от которой она выполняется. В случае, если уязвимость присутствует в программе, выполняемой от имени администратора, злоумышленник может получить полный контроль над операционной системой [2].

*Буфер* – это область в оперативной памяти определенного размера, выделяемая под каждую переменную, объявленную в программе в соответствии с ее типом. Принципиально важной особенностью является то, что если записать в такой буфер количество данных заведомо большее, чем его размер, то не поместившийся остаток данных затрет и заменит следом стоящие данные в памяти. Этот процесс и называется переполнением.

Множество буферов со значениями переменных, в свою очередь, формируют *стек* – структуру последовательно идущих друг за другом данных, организованных по принципу LIFO (с англ. *last in – first out*) «последним вошел – первым вышел». Наиболее удачным примером из жизни, иллюстрирующим работу стека является пистолетный магазин, в котором

заправка патронов осуществляется сверху, а первой выстреливает последняя заряженная пуля.

Когда речь идет о языках высокого уровня, таких как С и С++, напрямую работающих с оперативной памятью, стек формируется соответственно для каждой функции программы и содержит в себе, помимо буферов со значениями переменных, *указатели на данные* в других областях памяти, *указатели на другие функции*, а также *адрес возврата* – тот адрес, по которому будет передано управление после отработки конкретной функции [3].

В архитектурах Intel x86 и им подобных в случае переполнения буфера, любые вышеперечисленные составляющие стека могут быть беспрепятственно перезаписаны. Кроме того, важной особенностью этих архитектур является то, что данные в стеке являются исполняемыми и могут быть выполнены как код. Все эти условия в совокупности дают злоумышленнику массу возможностей атаковать систему.

В этом случае целей для атаки может быть несколько:

- чтение и/или изменение секретных переменных, в частности паролей, ключей и других важных сведений, находящихся в общей памяти, а также значений, влияющих на ход выполнения программы, таких как переменные циклов;
- передача управления произвольному внедренному злоумышленнику за счет переполнения коду путем подмены адреса возврата из функции;
- передача управления «секретной» функции, используемой в самой программе, либо функции, имеющейся в подключенной динамической библиотеке, путем замены адреса возврата, либо указателя.

В результате злоумышленник может нарушить ход выполнения программы, получить секретные данные: пароли и ключи, а также, что самое опасное – выполнив произвольный код с правами уязвимой программы или воспользовавшись системной функцией, повысить свои привилегии в операционной системе (ОС) вплоть до административных.

Все методы защиты от переполнения буфера можно разделить на две большие группы:

1. Методы, применяемые на этапе разработки программного обеспечения (ПО), направленные в основном на минимизацию уязвимостей в коде.
2. Методы, реализуемые в процессе работы ПО в операционной системе, допускающие наличие уязвимостей, но сводящие к минимуму возможность направленных на них атак.

Первая группа методов направлена в основном на поиск уязвимостей в исходных кодах программы с целью ее последующей доработки.

Для этого, в настоящее время применяются следующие подходы:

- сквозная инспекция исходных текстов;

- аудит исходных текстов программного обеспечения;
- динамическое тестирование нагрузкой («фаззинг»).

*Сквозная инспекция исходных текстов* проводится экспертом-аудитором. В ходе инспекции, аудитор строит ментальную модель работы программы и старается определить, какие внешние воздействия могут нарушить ход ее работы. При этом аудитор мысленно упрощает систему, что позволяет ему сконцентрировать внимание на структуре и поведении ПО в контексте обработки внешних данных. Данный подход является наиболее тщательным, но при этом крайне медленным. Кроме того, при сквозной инспекции до сих пор применяется в основном ручная техника анализа, что, учитывая человеческий фактор, дополнительно снижает эффективность исследований и существенно увеличивает их трудоемкость.

*Аудит исходных текстов программного обеспечения* представляет собой процесс автоматического сканирования (при помощи специализированных программных средств) исходных текстов ПО с целью выявления определенных синтаксических конструкций, про которые априорно известно, что при определенных информационных воздействиях они потенциально опасны.

При анализе применяются специализированные сканеры безопасности исходного кода, представляющие собой инструментальные средства, ориентированные на выявление потенциально опасных синтаксических конструкций в исходных текстах ПО. Выявленные конструкции заносятся в отчет, который затем совместно с исходными текстами подвергается ручному анализу аудитором. Инструментальные средства для аудита можно условно разделить на несколько категорий: синтаксические, семантические и эвристические по типам обнаруживаемых конструкций.

У всех подобных средств существует два недостатка:

- 1) Любой сканер имеет большое число ложных срабатываний, т. е. реакций на код, который на самом деле не представляет опасности.
- 2) Сканеры могут обнаружить потенциально-опасные конструкции только по заранее заданным шаблонам.

*Динамическое тестирование нагрузкой* («фаззинг») основано на анализе поведения реально функционирующей системы при подаче на ее входы различных информационных воздействий. При помощи данного подхода были выявлены уязвимости в большом числе реально работающих систем. Однако сам процесс тестирования не имеет какого-либо системного характера, и выявление уязвимостей носит случайный характер. При помощи «фаззинга» можно успешно атаковать систему, однако предоставить какие-либо гарантии защищенности в случае отсутствия успешных атак невозможно, поэтому данный подход используется только в дополнение к сквозной инспекции или аудиту, например, для того, чтобы на практике проверить реализуемость теоретически построенного сценария атаки либо уточнить дополнительные условия для реализации угрозы [4].

Таким образом, каждый из рассмотренных подходов имеет свои существенные недостатки и ограничения. Поэтому при реальных исследованиях ПО применяют различные комбинации аудита, сквозной инспекции и тестирования, и методология анализа развивается в направлении поиска наиболее оптимального сочетания данных методов.

Ко второй группе методов относятся те, что применяются уже в процессе эксплуатации ПО и являются средствами безопасности ОС. Основными из них являются: предотвращение выполнения данных (DEP) и рандомизация адресного пространства (ASLR).

DEP (англ. *Data Execution Prevention*) – метод который позволяет помечать области памяти как «только для данных», тем самым запрещая их исполнение. Данный метод является эффективным при атаке, предполагающей внедрение произвольного кода, который, будучи помещенным в память за счет переполнения не сможет быть выполнен и не нанесет вреда программе и ОС. Однако данный метод бесполезен в случае других видов атак, без использования произвольного кода [2].

ASLR (*Address Space Layout Randomization*) – метод, позволяющий рандомизировать адресное пространство в оперативной памяти. Одним из условий успешной атаки является тот факт, что злоумышленнику необходимо знать, по какому адресу в памяти окажется внедренный им в результате переполнения код, для того чтобы сослаться на него, подменив адрес возврата из функции или указатель. Либо с этой же целью нужно знать адрес системной функции из самой программы или подключаемой библиотеки. В результате работы ASLR эти адреса меняются при каждом запуске программы, что значительно затрудняет (но не исключает полностью [5]) возможность осуществления атаки.

Недостатком как DEP, так и ASLR является их несовместимость со многими существующими программами, а также некоторыми компонентами ОС, т. е. их эффективность явно зависит от разработчиков ПО.

Подводя итоги можно сделать вывод о том, что не существует единого метода, полностью решающего проблему переполнения буфера. Существующие сегодня методы имеют недостатки, а о защищенности системы можно говорить только при их грамотном сочетании. В то же время эффективность этих методов напрямую зависит от разработчиков. Так как, в рамках одной ОС, обычно используется решения разных производителей, соблюдение всех аспектов защиты становится проблематичным. Таким образом, полностью решить проблему переполнений можно 2-мя путями: создать метод, который не зависит от разработчиков ПО или использовать для написания программ языки, не имеющие прямого доступа к памяти.

### Список используемых источников

1. **Атаки** на переполнение буфера [Электронный ресурс] / А. Колищак // Статьи: ANDR: Атаки на переполнение буфера – 1999. – Режим доступа: <http://securityvulns.ru/articles/bo.asp> (Дата обращения: 17.04.2014).
2. **Ошибки** переполнения буфера извне и изнутри как обобщенный опыт реальных атак / К. Касперски // Системный администратор. – 2005. – № 3. – С. 64–72.
3. **Переполнение** буфера [Электронный ресурс] / К. Третьяков // CodeNET.ru: Все для программиста – 2011. – Режим доступа: <http://www.codenet.ru/progr/asm/overflow.php> (Дата обращения: 20.04.2014).
4. **Подходы** к оценке защищенности программного обеспечения от негативных информационных воздействий / С. Е. Кузнецов // Information Security. Информационная безопасность. – 2011. – № 6. – С. 30–32.
5. **ASLR** Bypass Apocalypse in Recent Zero-Day Exploits [Электронный ресурс] / X. Chen. – 2013. – Режим доступа <http://www.fireeye.com/blog/technical/cyber-exploits/2013/10/aslr-bypass-apocalypse-in-lately-zero-day-exploits.html> (Дата обращения 01.05.2014).

*Статья представлена научным руководителем канд. техн. наук, профессором А. В. Красовым.*

**УДК 004.7-027.31.056.53**

**В. И. Андрианов (доцент кафедры ЗСС СПбГУТ)  
Л. А. Виткова (студентка группы МБИ-22м СПбГУТ)**

## **АКТУАЛЬНОСТЬ БИОСИСТЕМНЫХ ТЕХНОЛОГИЙ И ПЕРВИЧНЫЙ АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В БИОСИСТЕМАХ**

Необходимость в новых разработках и актуальность создания концептуально новых средств защиты информации обусловлена тенденциями современности, например, согласно исследованию Gartner, опубликованному в феврале 2013 года, за 2012 год рынок информационной безопасности вырос на почти на 8 % – до \$19,135 млрд по сравнению с 2011 годом [1].

Актуальность вопросов защиты информации объясняется еще и тем, что количество атак и жертв огромно, по данным отчета компании Symantec, жертвами киберпреступлений в 2013 стали 378 млн человек, что почти в 3 раза выше ежегодного показателя рождаемости, и только зарегистрированные и разглашенные потери составили 132 миллиарда долларов США [2].

Сегодня перед учёными всего мира стоит задача разработки новых систем защиты. Большинство современных атак комплексные, они направлены не на операционные системы, а на получение распределенных ресурсов, похищение данных, денежных средств, перегрузки сетей, серверов, источников питания.

Эксперты Gartner Security прогнозируют следующие тенденции развития рынка:

- переход средств компьютерной безопасности к высокоинтеллектуальным решениям, их синергия с другими средствами защиты (биометрическая аутентификация, облачные сервисы) с целью разносторонней защиты телекоммуникационных систем и информации пользователя;
- переход к защищенным платформам, в которых будет объединяться защищенная операционная система, облачные сервисы и аппаратные устройства с предварительными настройками для обнаружения атак.

Правительства многих стран принимают решительные меры, увеличивают бюджеты, формируют отделы по борьбе с киберпреступлениями, а также все больше делают акцент на разработку новейших технологий и аппаратно-программных средств поиска и обнаружения аномалий в телекоммуникационных сетях и в вычислительных процессах.

В 2011 г. на официальном сайте Белого дома США был опубликован документ «Международная стратегия по действиям в киберпространстве», в котором правительство США приравнивает киберпреступления к традиционным военным действиям, оставив за собой право реагировать на них соответствующе, вплоть до применения ядерного оружия [3].

В июле 2013 г. президентом Российской Федерации В. В. Путиным был подписан документ «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года».

По мнению авторов статьи, современные технологии защиты требуют создания адаптивных СЗИ и носят комплексный характер. Необходимо расширить методологию. Многие ученые сходятся во мнении, что следует обратить внимание на биосистемные технологии, в частности на механизмы естественного иммунитета.

Наблюдаются следующие тенденции эволюции средств защиты информации:

- создание ИТ-систем с элементами адаптивности и самоорганизации, в которых присутствовали бы и процессы зарождения, и процессы приспособления и возможности развития, обучения;
- применение биоаналогий, что находит свое отражение в следующих разделах:
  - 1) архитектура ИТ систем;
  - 2) иммунные механизмы защиты ресурсов и полей информации;

3) Эволюционные процессы наследования, развития, адаптации и отбора;

4) структурирование информации по информационным полям;

5) программирование ИТ механизмов посредством распределенных избыточных информационных полей.

Исследования данного вопроса и разработки ведутся уже более пятнадцати лет, пример [4].

Как и правительства, так и корпорации вкладывают средства в новые разработки, в которых использовалась бы встроенные механизмы адаптивной памяти, иммунитет, применялись бы принципы избыточности. В 2013 году сообщалось, что производитель IBM планирует открыть собственную лабораторию по кибер-безопасности в Тель-Авиве, в которой будут работать свыше 200 специалистов [5].

#### *Анализ основ организации защиты информации в биосистемах*

Анализ показывает, что «Биосфера – иерархическая информационная система с единым подходом к защите процессов хранения, преобразования и переноса информации».

Ученые отмечают двойственность биосферы. Это и биосистема и сложная информационная система. Предполагается, что все что нас окружает – это сигналы, которые переносятся химическими, биоэлектрическими способами между элементами биосферы, такими как: молекулы; хромосомы, клетки, ткани, органы.

Жизнеспособность видов связана с избыточным кодированием, распределенным хранением и передачей информации в виде генетического кода, который и можно рассматривать как распределенное информационное поле.

Чем сложнее система, тем избыточнее код и тем сложнее процесс воспроизведения потомства.

Зашиту в биосистемах обеспечивают механизмы наследственности и изменчивости. Передачу генетической информации обеспечивает ДНК. Сущность ДНК заключена в его двойственности – это:

1. Защищенный носитель информации.

2. Источник информации в виде генетического кода.

Наименьшей структурой является клетка, она осуществляет хранение и декодирование информационных сигналов. Клеточный принцип строения биосистемы обеспечивает защищенность структуры ДНК за счет избыточности, то есть одной клетки достаточно для клонирования целого организма.

Биосистемы и клетки это прежде всего информационные системы, в которых есть иерархия, методология хранения, кодирования и преобра-

зования информации, и благодаря этому реализован совершенный механизм защиты.

Естественная иммунная система призвана реализовать процессы глобального уровня, используя локальные взаимодействия. В ней используются механизмы обучения, памяти и ассоциативного поиска для решения задач распознавания и классификации информации.

Естественная иммунная система – сложная система, состоящая из ряда функциональных компонентов. Она применяет многоуровневую систему защиты против внешних антигенов, включая действие неспецифических, а именно вырожденных, и специфических, а именно приобретённых, механизмов защиты.

Основной ролью естественного иммунитета является распознавание клеток организма и их классификация на «свои» / «чужие». Чужие клетки подлежат дальнейшей классификации с целью стимуляции механизмов защиты соответствующего типа.

Базовый иммунитет есть у всех, в процессе эволюции естественная иммунная система учится различать внешние антигены и собственные клетки или молекулы организма.

Иммунная система способна эффективно обрабатывать значительные объемы данных. В частности, она выполняет большой объем сложных высокопараллельных распределенных вычислений, функционирует как «второй мозг», т. к. способна хранить информацию о предыдущих контактах с антигенами и отвечать на ранее не встречавшиеся антигены.

Для разработки средств защиты информации перспективны следующие свойства иммунной системы.

– *Распознавание.* Естественная иммунная система способна классифицировать молекулярные структуры: распознавание своего и чужого – одна из основных задач естественной иммунной системы.

– *Выделение особенностей.* Клетки иммунитета выделяют особенности антигенного окружения и маркируют антигены на своей поверхности для лимфоцитов.

– *Разнообразие.* Естественная иммунная система использует механизм генерации рецепторов лимфоцитов, гарантирующий взаимодействие лимфоцита с любым неизвестным антигеном.

– *Обучение.* Естественная иммунная система оценивает структуру антигена через его случайные контакты с клетками естественной иммунной системы. Обучение выражено в изменении концентрации лимфоцитов при первичном ответе за счет механизма размножения и супрессии клонов.

– *Память.* Часть лимфоцитов в процессе иммунного ответа становится клетками памяти, сохраняя информацию о контактах с антигеном.

– *Распределенный поиск.* Естественная иммунная система – распределенная система, клетки которой рециркулируют через кровь, лимфу, органы и ткани, где встречаются с антигенами.

– *Саморегуляция.* Иммунная защита обладает свойством саморегуляции – не существует центрального органа, управляющего функциями естественной иммунной системы.

– *Пороговый механизм.* Иммунный ответ и размножение иммунокомпетентных клеток происходят по преодолению некоторого порога концентрации.

– *Динамическая защита.* Клональное (от слова клон) размножение и соматическое (клетки, образующие тело) гипермуттирование продуцирует иммунокомпетентные клетки, что создает динамический баланс между изучающей и защитной функцией адаптивного иммунитета.

– *Вероятностное обнаружение.* Реакции при иммунном ответе – это т. н. стохастический процесс, а именно процесс состоит из случайных переменных, значения которых меняются во времени. То есть лимфоцит взаимодействует с множеством сходных антигенов.

В иммунном ответе на антиген важную роль играют такие характеристики иммунитета, как адаптируемость, специфичность, самотolerантность, дифференцировка.

Структура естественной иммунной системы может и должна рассматриваться примером в процессе разработки модели адаптивных систем защиты, иммунитет несет в себе тысячелетиями отработанную логику защиты от внешних атак, модель естественной защиты организмов может быть использована для защиты телекоммуникационных сетей.

Нам необходимо показать аппаратно-математическую реализуемость принципов естественной иммунной системы, что позволит «не изобретать велосипед», а привлечет к решению проблемы создания адаптивной системы информационной безопасности всю мощь естественного процесса по принципу «Все придумано до нас». Наша задача: «Не ждать милостей от природы», а приспособить ее иммунные KNOW-HOW для своих нужд.

### Список используемых источников

1. Gartner Says Worldwide Security Software Market Grew 7.9 Percent in 2012 [Электронный ресурс]. – URL: <http://www.gartner.com/newsroom/id/2500115> (Дата обращения: 20.05.2014)
2. 2013 Norton Report. Систем. требования: Adobe Acrobat Reader [Электронный ресурс]. – URL: <http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pptx> (Дата обращения: 20.05.2014)
3. International strategy for cyberspace. Систем. требования: Adobe Acrobat Reader. [Электронный ресурс]. – URL: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/International\\_Strategy\\_Cyberspace\\_Factsheet.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf) (Дата обращения: 20.05.2014)

4. Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты: пер. с англ. под ред. А. А. Романюхи. – М. : ФИЗМАТЛИТ, 2006. – 343 с.

5. IBM купила ИБ-разработчика Trusteer [Электронный ресурс]. – URL: <http://www.securitylab.ru/news/443459.php> (Дата обращения: 20.05.2014)

**УДК 658:656.25 (075.8)**

**Э. В. Бенета (студентка группы АС-807 ПГУПС)**

## **СРАВНЕНИЕ И ОЦЕНКА СУЩЕСТВУЮЩИХ КОНЦЕПЦИЙ ПОСТРОЕНИЯ СИСТЕМ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЬЯМИ**

Сегодня самым большим и динамично развивающимся сектором мировой экономики является рынок телекоммуникаций. Развитие телекоммуникаций происходит в направлении создания рынка телекоммуникационных услуг, внедрения новых телекоммуникационных и информационных технологий, их конвергенции. Телекоммуникационные сети по быстродействию и надежности являются одной из самых требовательных отраслей. На современном рынке телекоммуникаций можно встретить множество постоянно совершенствующихся систем управления телекоммуникациями с высоким уровнем конкуренции. Рассмотрим некоторые из них.

Часто встречающимся стандартом в области организации и управления информационными технологиями, обобщившим в себе лучший международный опыт, является Information Technology Infrastructure Library (ITIL) (табл. 1). В библиотеке ITIL разъясняется, что надо сделать для организации такого подхода. В ITIL описывается, как должна быть организована деятельность структур информационных технологий (ИТ). Каждая из книг библиотеки ITIL рассматривает вопросы отдельной части структурированной процессной основы. В них дается описание того, что необходимо для организации ИТ. Библиотека ITIL определяет цели и виды деятельности, входные и выходные параметры каждого из процессов в ИТ организации. Акцент делается на проверенном практикой подходе, который может быть реализован различными способами в зависимости от обстоятельств [1].

При использовании COBIT (*Control of Objectives for Information and related Technology*) (табл. 1) информационная система строится исходя из требований бизнеса и условий жесткой экономии ресурсов, а также эффективного использования этих ресурсов. Другими словами, стандарт COBIT описывает бизнес-ориентированный подход к созданию информа-

ционной среды: ИТ рассматриваются в виде инструмента бизнеса, а стандарт определяет принципы построения и организации работы ИТ департамента.

PRINCE2 (*Projects IN Controlled Environments 2*) представляет собой структурированный метод управления проектами, обеспечивающий стандартный подход к менеджменту проектов, доказанные и установленные ценные практики в руководстве проектом [2]. Методология PRINCE2 включает в себя подходы к менеджменту, контролю и организации проектов. PRINCE2 содержит в себе 4 основных элемента: Принципы, Процессы, Темы и Адаптация (табл. 1).

OSS/BSS системы (*Operations Support Systems/Business Support Systems* – системы поддержки операций/системы поддержки бизнеса) предназначены для комплексного управления телекоммуникационными ресурсами предприятия. В основу работы систем OSS/BSS положен процессный подход, в центре внимания которого – бизнес-процесс. Процессный подход позволяет проследить и оценить работу всех подразделений компании на всех уровнях – от ресурсов до конечного продукта, что дает оператору возможность увидеть в целом не только сеть, но и весь бизнес (табл. 1). Набор модулей OSS/BSS, наиболее часто используемых телекоммуникационными компаниями для автоматизации своей деятельности насчитывает 14 модулей. Только два из них относятся к BSS. В настоящий момент понятие OSS/BSS тесно связано с концепцией NGOSS (*New Generation Operations Support System*). NGOSS – подход к разработке, внедрению и использованию систем поддержки операционной деятельности OSS/BSS для телекоммуникационных компаний. NGOSS позволяет определить стандарты для бизнес-процессов операторов связи, форматы предоставления используемых в системах управления данных и интерфейсы взаимодействия со средой, в которую интегрируется решение.

TMN (*Telecommunication Management Network*) – специальный подход к управлению, ориентированный на интегрированное управление любыми по структуре, составу и технологиям телекоммуникационными сетями [3]. TMN является самостоятельной управляющей системой, связанной с управляемой телекоммуникационной сетью (объект управления) с помощью ряда интерфейсов, обеспечивающих получение информации о состоянии сети и передачи в нее выработанных TMN управляющих воздействий. Существует множество технологий, которые могут применяться к прикладным задачам управления на основе распределенных систем, например, CORBA (и другие нестандартные системы, ориентированные на брокерский запрос), DCE (распределенное компьютерное окружение (среда), разработанная *Open Group*), DCOM (предлагаемая Microsoft распределенная объектная технология), DTP (распределённая обработка транзакций *Distributed Transaction Processing*, которая включает множество продуктов и соответствующих стандартов) (табл. 1).

ТАБЛИЦА 1. Сравнение подходов

	<b>ITSM/ITIL</b>	<b>COBIT</b>	<b>PRINCE2</b>	<b>OSS/BSS</b>	<b>TMN</b>
<b>Содержание</b>	Сервисный процессный подход. ISO 9001: 2000 ISO 20000: 2005	Процессный подход. ISO 9000; подходы стандартов PRINCE2, ITIL и др.	Структурированный метод	Процессный подход	Комплексный подход к управлению сетями связи. Рек. МСЭ-Т М.3010, М.3020, М.3100
<b>Назначение, цели</b>	Планирование часто используемых процессов, ролей и видов деятельности, определение связей между ними	Контроль и аудит существующей системы управления ИТ, организация оперативного и стратегического управления ИТ, анализ расходов на ИТ проекты	Управление проектами: контроль в использовании ресурсов и управление рисками. Раньше в области только ИТ-проектов (1989), теперь – в любых проектах (1996)	Комплексное управление телекоммуникационными ресурсами предприятия. Решение бизнес-задач	Управление любыми по структуре, составу и технологиям телекоммуникационными сетями
<b>Создатели</b>	CCTA. С апреля 2001 г. OGC.	ISACA и ITGI	CCTA	TMF	МСЭ-Т, 1992 г.
<b>Критерии</b>	1. Обеспечение бизнеса информационными сервисами. 2. Service Level Agreement – утвержденный документ, по которому сервисы поставляются бизнесу. 3. Качество сервиса измеряется.	1. Ориентация на бизнес-требования. 2. Процессный подход к управлению ИТ. 3. Цели контроля к управлению ИТ-процессами. 4. Оценка эффективности ИТ.	Баланс между функциями по поддержанию текущей деятельности в компании и преобразованию бизнес-операций, вводимых для поддержания конкурентоспособности и получения максимальной отдачи для организации	1. Повышение качества и оперативности обслуживания. 2. Мониторинг и управление ресурсов. 3. Взаимодействие персонала удаленных подразделений. 4. Обнаружение и пресечение мошеннических действий.	Управление услугами сетей связи, эксплуатация и техническое обслуживание оборудования, оперативно-технический контроль и администрирование сетевыми устройствами
<b>Существующие версии</b>	1991 г. – ITILv1 Конец 90-х гг. – ITILv2* 2007 г. – ITILv3	1992 – первая версия 2000 – COBIT3.0 2003 – COBIT3.1Online 2005 – COBIT 4.0 2007 – COBIT4.1*	1989 – первая редакция (только для ИТ проектов) 1996 – расширен (в любых проектах)	Программа NGOSS (New Generation Operations Support System), разрабатываемая TMF.	Для управления объектами – архитектура «менеджер-агент» с протоколами CMIP/CMIS, SNMP. Прикладные задачи: CORBA, DCE, DCOM, DTP.

	<b>ITSM/ITIL</b>	<b>COBIT</b>	<b>PRINCE2</b>	<b>OSS/BSS</b>	<b>TMN</b>
<b>Особенности</b>	1. Продолжительное время перехода. 2. Недостаток понимания целей внедрения и процессов. 3. Вовлеченность руководства и приверженности сотрудников на всех уровнях. 4. Инвестиции в инструментальные средства.	1. Требует использования специфичных стандартов. 2. Руководство, а не готовое решение. 3. Требует кастомизации с учетом бизнес целей компании, рисков и организаций, проектов и инфраструктуры ИТ.	Обеспечивает общую терминологию для участников проекта. Предусматривает контроль в использовании ресурсов и управлении рисками.	Внедряются только на основе построенной модели процессов оператора связи, являются компонентой большой работы по организации деятельности компаний и выбору приоритетов.	Задача – поддержание ТКС в рабочем состоянии с помощью системы эксплуатации и технического обслуживания.
<b>Преимущества</b>	1. Ориентация работы ИТ на решение задач бизнеса. 2. Стандарты и правила для ИТ-персонала. 3. Внедрение подходов менеджмента качества в управления ИТ-сервисами. 4. Постоянно перерабатывается и обновляется.	1. Соответствие требованиям бизнеса. 2. Понятное для менеджмента видение деятельности ИТ. 3. Определение четкого владения ИТ-процессами и распределения ответственности. 4. Полнота.	Может быть применен к любому проекту, независимо от масштаба проекта, типа организации, географии и культуре.	Бизнес-процесс позволяет проследить и оценить работу всех подразделений компании на всех уровнях, что дает оператору возможность увидеть в целом не только сеть, но и весь бизнес.	1. Оптимизирует систему управления. 2. Обеспечивает механизмы защиты и целостности данных. 3. Минимизирует время локализации и устранения неисправностей в сети. 4. Расширяет спектр предоставляемых услуг связь пользователям.
<b>Структура основной версии подхода</b>	Семь элементов, взаимодействующих между собой. Поддержка услуг и Предоставление услуг – центральные.	Концептуальное ядро версии 4.1 состоит из 34 высокогенеральных процессов (которые покрывают порядка 200 целей контроля), сгруппированных в 4 домена (сферы деятельности)	PRINCE2 содержит в себе 4 основных элемента: Принципы (7 шт), Процессы (7 шт), Темы (7 шт) и Адаптация.	Набор из 14 модулей, используемых телекоммуникационными компаниями.	Центры (станции) управления являются основными программно-аппаратными средствами. Иерархическая структура из четырех уровней управления: элементы сети, сеть, услуги и административный уровень.

Для предприятия неизбежным этапом является выбор и внедрение той или иной системы управления. Когда текущие процессы уже не выполняются в полной мере, перед руководителями встают новые задачи, которые диктуют необходимость введения новых процессов. Здесь имеет большое значение правильный подход к выбору системы управления. Обобщение ведущих систем управления по основным сравнительным характеристикам представлено в виде таблицы. Такой анализ методов систем управления показал состав и структуру каждого подхода относительно остальных. Обобщение, сравнение и анализ формирует правильный выбор метода системы управления, вносит ясность в определение необходимости внедрения, позволяет организовать процесс управления с возможными интеграциями соседних систем управления.

#### **Список используемых источников**

1. ИТ Сервис-менеджмент. Введение / Ян Ван Бон; пер. с англ. – IT Expert, 2003. – 225 с.
2. ITIL на практике [Электронный ресурс] / С. Довгань // Открытые системы. – 2002. – № 12. – Режим доступа: [www.osp.ru/os/2002/12/033.htm](http://www.osp.ru/os/2002/12/033.htm).
3. Стандарты и технологии управления сетями связи / А. Ю. Гребешков. – М. : Эко-Трендз, 2003. – 288 с.:илл.

*Статья представлена научным руководителем д-ром техн. наук, профессором А. К. Канаевым.*

**УДК 621.395**

**В. Ю. Бондарев (студент группы СК-92 СПбГУТ)**  
**А. В. Лейкин (старший преподаватель кафедры ИКС СПбГУТ)**

#### **БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ MESH-СЕТЕЙ. ПРИНЦИП ДЕЙСТВИЯ АЛГОРИТМА CORIDS**

Последние 10–15 лет мы можем наблюдать неуклонную тенденцию в развитии технологий беспроводных сетей (БС) и увеличения их производительности. И это не удивительно, ведь не смотря на то, что на текущий момент эти сети могут уступать по пропускной способности проводным линиям связи, они все же обеспечивают достаточную ширину канала связи, а также его надежность для поддержки интерактивных мультимедийных приложений, обладая при этом большей мобильность, доступностью и простотой развёртывания. Использование оборудования с поддержкой раз-

личных протоколов беспроводных сетей стало повсеместным – мобильные телефоны, компьютеры, планшеты. Казалось бы, даже самые обычные и привычные для нас устройства становятся все более интеллектуальными: весы, холодильники, телевизоры и фотоаппараты с Wi-Fi, тахографы со спутниковым или GSM подключением, счётчики и различные датчики, не говоря уже о банкоматах и POS-терминалах, которые сами продают товары, выполняют транзакции, обновляют свое программное обеспечение – все это подключается к IP-сетям, Интернету, различным облачным сервисам и является реалиями современного времени. К сожалению, одно из основных преимуществ БС стало ее ахиллесовой пятой. Предоставляя общую среду передачи – радиоэфир – мы открываем широкую дверь для злоумышленников, поэтому так важно разрабатывать новые и усовершенствовать текущие алгоритмы обнаружения вторжений (*Intrusion Detection System*), о которых и пойдет речь в данной статье. Разговор идет об информационной безопасности одной из ключевых технологий, активно внедряемой в сетях следующего поколения (NGN), технологий беспроводных ячеистых сетей (*Wireless mesh networks*). В частности, будет рассмотрен принцип работы и достоинства нового алгоритма системы обнаружения вторжений (IDS) в этих сетях – *cluster-oriented reward-based intrusion detection system* (CORIDS) [1]. А также будут приведены результаты сравнительного анализа производительности с его предшественником, похожим по принципу действия, алгоритмом *misbehavior detection algorithm* (MDA), используя сетевой симулятор QualNet [2].

### *Кластерная архитектура для WMN*

Рассматриваемая сеть обладает гибридной архитектурой и иерархической моделью организации узлов (рис. 1). Она делится на кластеры, каждый из которых включает в себя стационарно расположенный головной узел кластера Cluster Head (ГУК), являющийся маршрутизатором, и некоторое количество мобильных, но ограниченных в ресурсах *mesh*-узлов, которые находятся на расстоянии не более одного перехода от ГУК. Кластеры могут между собой пересекаться, но располагаются на таком расстоянии, что ГУК в его составе может быть только один. Таким образом число кластеров в сети определяется количеством головных узлов. *Mesh*-узлы, входящие в кластер, взаимодействуют непосредственно с ним, так как находятся в непосредственном радиусе действия каналов радиосвязи, при этом в сети обычно используются стандарты группы IEEE 802.11. Также в ГУК хранится информация о членстве узлов в кластере, где она обновляется через постоянные интервалы времени [1]. Необходимо отметить, что исследуемый алгоритм выполняется только в ГУК – это позволяет минимально задействовать остальные узлы, что бесспорно является преимуществом, так как позволяет снизить их энергопотребление.

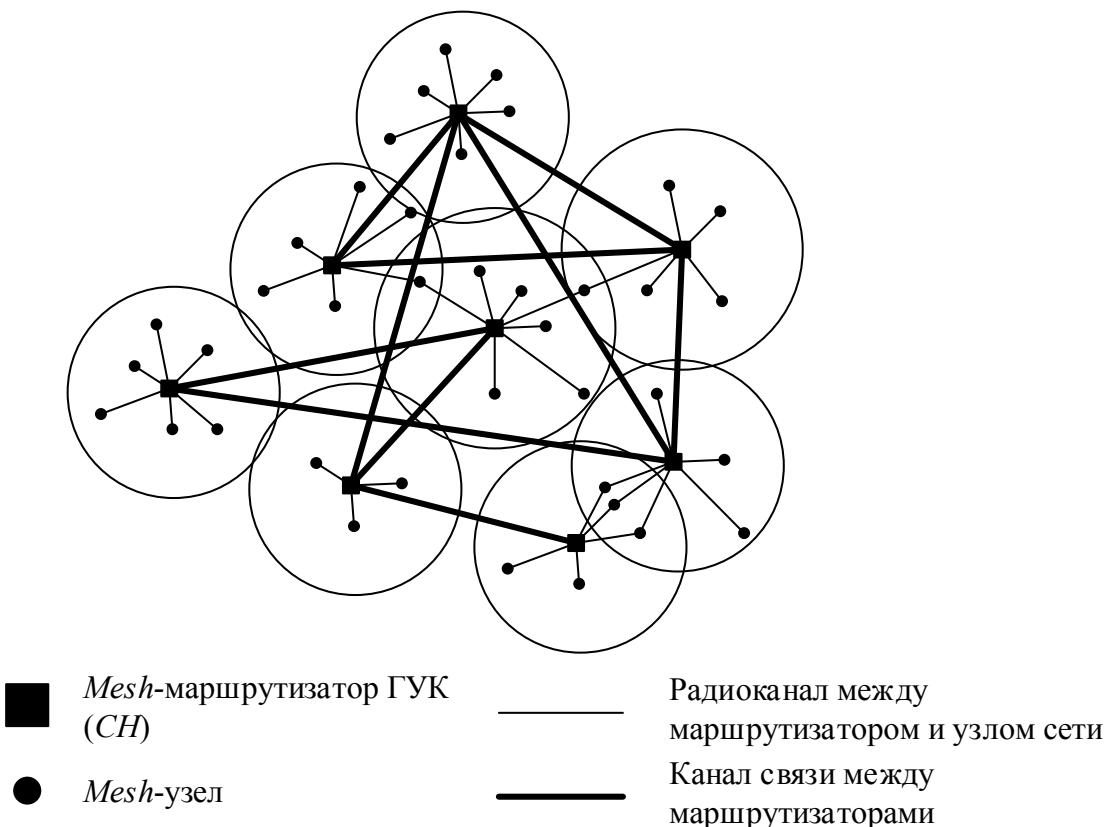


Рис. 1. Предлагаемая к анализу беспроводная ячеистая сеть (*wireless mesh network*) с кластерной топологией

Прежде чем перейти к рассмотрению самого алгоритма CORIDS приведем основные условия его работы в исследуемой сети:

- 1) Каждый ГУК следит за активностью узлов своего кластера.
- 2) Все узлы сети и ГУК имеют глобальный уникальный идентификатор.
- 3) Головные узлы кластера достаточно защищены или имеют достаточно ресурсов для реализации различных уровней безопасности.
- 4) Пороговые значения предварительно вычисляются и устанавливаются для всей сети. Они хранятся в ГУК и в зависимости от приоритета кластеров могут принимать разные значения, установленные в качестве пороговых.
- 5) Счетчики количества отправленных и полученных пакетов на стороне клиентов задаются операционной системой и не могут быть искажены злоумышленником.

### *Алгоритм CORIDS*

Обозначим параметры, используемые в процессе обнаружения вторжений алгоритмом CORIDS:

$TR_{val}$  – показатель доверия узла кластера, определённый его ГУК;

$TH_{tr}$  – пороговое значение показателя доверия; если показатель доверия узла сети упадёт ниже этого порога, то узел будет определён, как вредоносный;

$PAR_X$  – скорость получения пакетов для узла  $X$  поддерживаемая его ГУК;

$PDR_X$  – скорость отправки пакетов для узла  $X$  поддерживаемая его ГУК;

$TH_{PAR}$  – пороговое значение скорости получения пакетов;

$N_X$  – уникальный ID узла  $X$ ;

$PS$  – количество пакетов, отправленных ГУК;

$PR$  – количество пакетов, полученных из ГУК.

Работу алгоритма можно разделить на три фазы:

1) Обмен информацией между ГУК узлами и ее обновление.

2) Передача информации от узлов сети соответствующим головным узлам.

3) Сравнение всех полученных показателей с пороговыми значениями и последующее их обновление, а на основе вычисленных результатов изменение уровня доверия узла, и, при необходимости, объявление узла злонамеренным.

Рассмотрим каждую фазу алгоритма более подробно и обозначим формулы вычисления основных показателей, использующиеся при обнаружении вторжений.

#### *Алгоритм CORIDS. Фаза 1:*

1.1. Головные узлы кластеров хранят значения  $PAR$ ,  $PDR$ ,  $PR$  и  $PS$  каждого члена кластера вместе с соответствующими им ID.

1.2. После фиксированного отрезка времени, ГУК транслирует свою соответствующую информацию об узлах всем другим ГУК в сети.

1.3. Когда ГУК получает такой пакет обновления, он просматривает его и проверяет наличие информации о некотором узле, который также принадлежал его кластеру в некоторый момент времени. Проверка выполняется на основании полученного ID узла  $N_X$  и связанных с ним набором параметров.

1.4. Если любой ID  $N_X$  совпадает с ID какого-либо из узлов этого кластера, то ГУК обновляет информацию, связанную с ID этого узла.

1.5. Шаги 1.3 и 1.4 выполняются всеми головными узлами.

1.6. Переход к фазе 2.

#### *Алгоритм CORIDS. Фаза 2:*

2.1. Узлы каждого кластера отправляют значение количества пакетов, отправленных и полученных со стороны соответствующего этому кластеру ГУК.

2.2. Вместе с информацией из п. 2.1 узлы сети отправляют свой ID NX.

2.3. ГУК содержит таблицу о членах кластера в пределах своего собственного кластера;

2.4. Переход к фазе 3.

*Алгоритм CORIDS. Фаза 3:*

3.1. ГУК сравнивает значение PAR и PDR для члена кластера с соответствующими ему значениями PR и PS, а также их пороговые значения.

3.2. Классификация атак основывается на этих значениях.

3.3. Уровень доверия рассчитывается для всех узлов. Причем для узлов, имеющих нормальное поведение, он повышается, а для узлов с некорректным поведением понижается.

3.4. Показатели доверия для членов кластера обновляются, исходя из вновь вычисленных значений уровней доверия.

3.5. Обновлённые показатели доверия сравниваются с предопределённым пороговым значением показателя доверия. Если показатель доверия любого члена кластера опустился ниже порогового значения, то он будет определён как злонамеренный узел, если нет, то, как доверенный.

3.6. Остановка алгоритма.

Описанный алгоритм выполняется в ГУК регулярно, но в случайные интервалы времени. Суть действия алгоритма заключается в том, что информация об узлах (их показатель доверия) обновляется, исходя из текущей информации, получаемой путем сравнения определенных параметров. По результатам сравнения показатель доверия небезопасных узлов должен быть снижен, в то время как показатель безопасных узлов увеличен. Для расчёта параметров, используемых в оценке уровня доверия узлов, предлагаются следующие формулы:

1) Начальный показатель доверия, присваивающийся узлу при присоединении к сети

$$TR_{VAL} = \frac{(2^n - 1)}{2},$$

где  $n$  – число бит, выделенных для хранения показателя доверия.

2) Величина уровня доверия нормально работающего узла

$$Reward = R \times \frac{(PAR_X + PDR_X)}{2}.$$

3) Величина изменения уровня доверия для DoS-атак

$$Reward = -R \times (PAR_X - TH_{PAR}).$$

4) Величина изменения уровня доверия для Blackhole-атак

$$Reward = R \times (PR_X - PDR_X).$$

5) Переоценка показателя доверия узла

$$TR_{VAL_x}(t) = TR_{VAL_x}(t - 1) + Reward_x.$$

После обновления информации в ГУК выполняется сравнение вычисленного значения с пороговым и если  $TR_{VAL_x}(t) < TH_{Tr}$ , то узел объявляется злонамеренным. Более подробно с работой алгоритма и описанием формул можно ознакомится в данной работе [1].

### *Результаты моделирование и анализа производительности*

Разработчиками [1] было проведено имитационное моделирование и анализ производительности рассматриваемого алгоритма CORIDS с его предшественником MDA [3] с помощью сетевого симулятора QualNet [2]. Анализ алгоритмов был направлен в сторону исследования зависимости их эффективности и количества ложных срабатываний от изменения пороговых значений, мобильности и плотности узлов, а также от изменения процентного соотношения доверенных и злонамеренных узлов [1]. На приведенных рисунках (рис. 2, 3) представлены только итоговые результаты, показывающие преимущество алгоритма CORIDS над MDA при различных процентных соотношениях злонамеренных узлов.

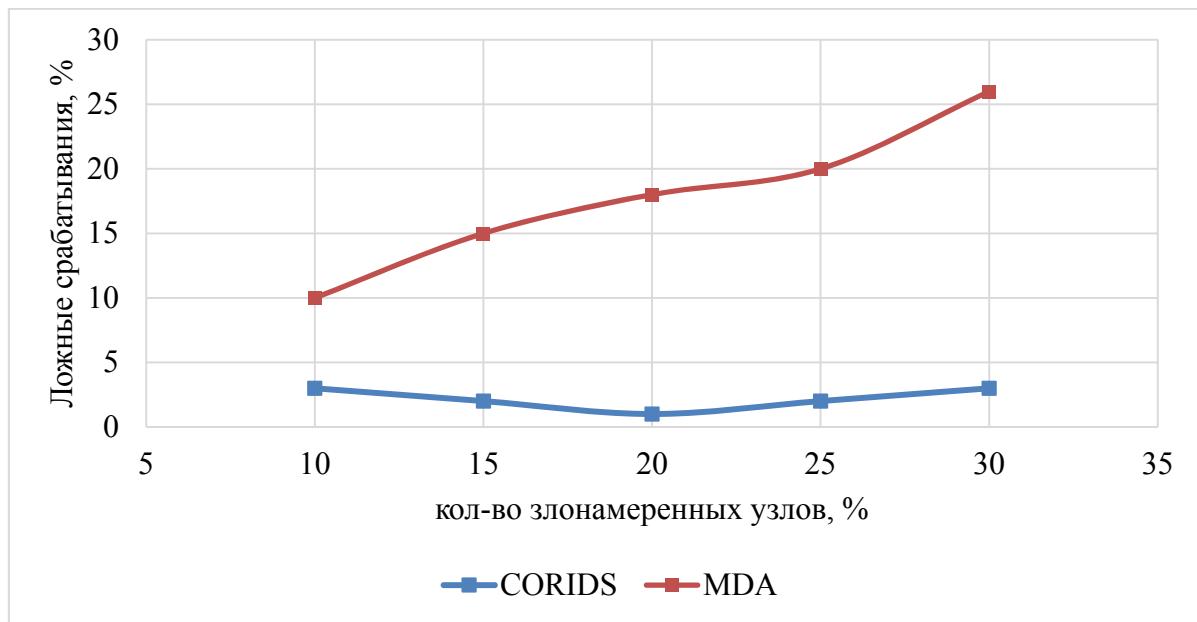


Рис. 2. Анализ ложных срабатываний

Как следует из результатов моделирования и сравнения [3] показателей ложных срабатываний, для CORIDS он предельно мал и находится в пределах 1–3 %. Для MDA график имеет линейную зависимость, обладая изначально высоким процентом ложных срабатываний и достигает значения 26 % при увеличении злонамеренных узлов в сети до 30 %. Таким образом, можно утверждать, что CORIDS работает с эффективностью, достигающей 90 %, в то время как эффективность MDA уменьшается линейно с

увеличением злонамеренных узлов в сети. Максимальная эффективность, которую показывает алгоритм MDA при сравнительном анализе – 60 % [1].

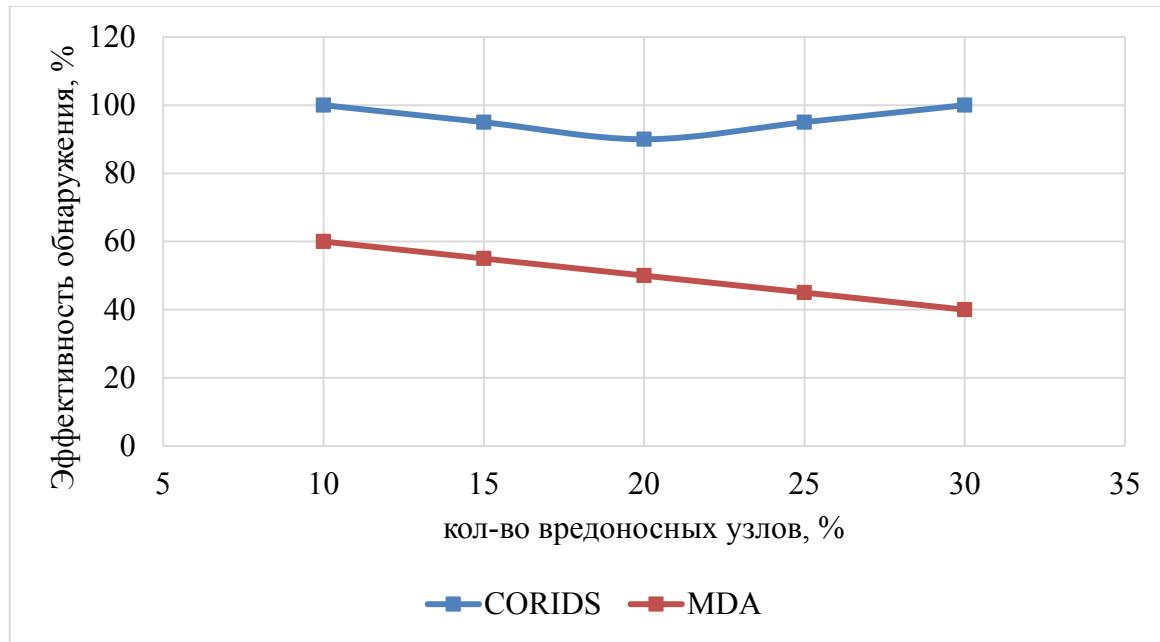


Рис. 3. Анализ эффективности обнаружения злонамеренных узлов

Алгоритм CORIDS использует небольшое количество управляющих сообщений и выполняется только на головных узлах кластеров. Учитывая, что он гораздо эффективнее и менее зависим от количества вредоносных узлов в сети, мы можем с уверенностью заявить, что он несомненно обладает большим преимуществом над алгоритмом MDA. Обладая при этом низким уровнем ложных срабатываний, он очень эффективен при Black-hole-атаках и вообще не имеет ложных срабатываний во время DDoS-атак [1].

### *Заключение*

Процесс развития современных сетей связи сопровождается повсеместным внедрением беспроводных сетей, особенно, на уровне доступа, при этом сети M2M являются одними из наиболее перспективных и активно развивающихся направлений в области телекоммуникаций. По оценке специалистов доля трафика сетей машина–машина к 2016 году составит около 5 % от общего объема трафика сетей связи [4]. В связи с этим представляется актуальным вопрос защиты беспроводных сетей, так как они часто используются для передачи конфиденциальной информации (например, номеров кредитных карт и т. п.), компрометация которой недопустима. Одним из способов повышения уровня защищенности БС является разработка и анализ новых алгоритмов для систем обнаружения вторжений. Рассмотренный алгоритм хорошо справляется с поставленной задачей, обладает хорошей производительностью при увеличении мобильности и

плотности узлов, а также разных соотношений доверенных и злонамеренных узлов. Таким образом, алгоритм CORIDS может представлять интерес для дальнейших научных исследований.

#### **Список используемых источников**

1. **Intrusion Detection in Wireless Ad-Hoc Networks** / N. Chaki, R. Chaki. – CRC Press, Taylor & Francis Group, 2014. – 264 с.
2. **QualNet** communications simulation platform (QualNet) – <http://web.scalable-networks.com/content/qualnet>.
3. **The Research on Dynamic Self-Adaptive Network Security Model Based on Mobile Agent** / J. Tao, L. Ji-ren, Q. Yang // 36th International Conference on Technology of Object-Oriented Languages and Systems (TOOLS-Asia'00). – 2000. – С. 134–140. – ISBN 0-7695-0875-8.
4. **Модели потоков трафика для сетей M2M** / А. И. Парамонов // Электросвязь. – 2014. – № 4. – С. 11–14.

*Статья представлена заведующим кафедрой «Инфокоммуникационные системы», д-ром техн. наук, профессором Б. С. Гольдштейном.*

**УДК 004.414.23**

**К. С. Варельджян (студентка группы СК-91 СПбГУТ)**  
**В. В. Фицов (ассистент кафедры ИКС СПбГУТ)**

### **СИМУЛЯЦИЯ РАБОТЫ АЛГОРИТМА МАРШРУТИЗАЦИИ AODV ПРИ ПОМОЩИ NETWORK SIMULATOR**

#### *Введение*

Беспроводной ad-hoc сетью называется совокупность узлов, которые общаются (*непосредственно*) друг с другом без вмешательства централизованных точек доступа. Также такие узлы способны динамически образовывать сеть не зависимо от какой-либо фиксированной инфраструктуры или централизованного администрирования [1].

Протоколы маршрутизации в таких сетях по принципу обновления маршрутной информации разделяются на реактивные, проактивные и гибридные. При *проактивной маршрутизации* каждый узел постоянно поддерживает маршрут до всех узлов сети. Построение и поддержание маршрута осуществляется при помощи обновлений (периодических или в следствии изменений в сети), получаемых с помощью дистанционно-векторного метода или метода состояния каналов (*link-state*) [2]. В противоположность проактивному протоколу, при *реактивной маршрутизации* (или маршрутизации по запросу) поиск маршрута происходит только то-

гда, когда действительно есть необходимость в передаче информационного трафика. *Гибридная маршрутизация* включает в себя только достоинства вышеуказанных стратегий протоколов маршрутизации. Как правило, гибридные протоколы маршрутизации разбивают сеть на множество подсетей, внутри которых функционирует проактивный протокол, а взаимодействие между подсетями осуществляется при помощи реактивных протоколов.

Одним из самых распространенных представителей реактивных протоколов маршрутизации является протокол AODV.

### Протокол маршрутизации AODV

Протокол маршрутизации AODV (*Ad Hoc On-Demand Distance Vector*) предназначен для использования мобильными узлами в ad hoc сети или в мобильной ad hoc сети (MANET – *Mobile Ad Hoc Network*). Официальный документ – RFC-3561 [3].

*Процедура обнаружения маршрута.* Когда одному узлу сети (источнику) требуется передать информацию другому узлу сети (узлу назначения), но ему не известен доступный маршрут до узла назначения, им запускается процедура поиска маршрута. Она заключается в том, что узел-источник широковещательно рассыпает по сети сообщения-запросы о маршруте – RREQ сообщения. Маршрут считается найденным, когда RREQ достигает либо самого узла назначения, либо промежуточного узла, который обладает «достаточно свежей» (“*fresh enough*”) информацией о маршруте до узла назначения. «Достаточно свежим» маршрутом считается такой маршрут, у которого последовательный номер (sequence number) больше или равен последовательному номеру, содержащемуся в RREQ. Маршрут становится активным, когда в ответ на RREQ от узла назначения приходит сообщение RREP [3].

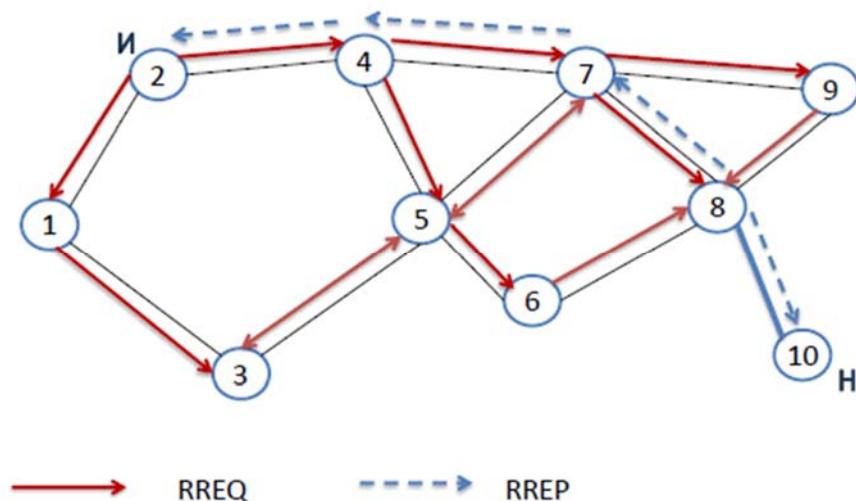


Рис.1. Процедура обнаружения маршрута в протоколе маршрутизации AODV

На рисунке 1 представлен пример реализации процедуры нахождения маршрута. Узлу 2 (Источнику) необходимо передать информацию узлу 10 (узлу-Назначения). Узлу 8 известен маршрут до узла 10. Узел 2 широковещательно рассыпает сообщения RREQ, затем рассылка повторяется его соседями и т.д. до тех пор, пока сообщение не достигнет узла 8. Затем узел 8 отправляет RREP первому узлу, от которого он получил сообщение RREQ (в данном примере таким узлом считается узел 7). Также узел 8 отправляет беспричинный ответ узлу 10, чтобы построился обратный маршрут от узла 10 к узлу 2. Далее узел 7 отправляет RREP узлу 4, который отправляет его узлу 2 (Источнику). На этом этап обнаружения маршрута считается завершенным.

### *Выбор средства симулирования*

Симулирование и моделирование являются важными подходами в разработке и оценке инфо-телекоммуникационных систем с точки зрения времени и затрат. Моделирование показывает ожидаемое поведение системы на основе его имитационной модели в различных условиях. Таким образом, цель имитационной модели заключается в том, чтобы определить точную модель и предсказать поведение реальной системы.

В настоящее время существует большое количество сетевых симуляторов, поддерживающих моделирование различных сетевых технологий, в том числе и ad hoc сетей. В данной работе были рассмотрены дискретно-событийные симуляторы Network Simulator 2 и 3. Стоит заметить, что NS-3 это не расширение NS-2, а самостоятельный симулятор, который сильно отличается от NS-2. В таблице представлено сравнение этих двух симуляторов по некоторым критериям.

ТАБЛИЦА. Сравнение сетевых симуляторов NS-2 и NS-3

Критерий сравнения	NS-2	NS-3
Используемые языки программирования	C++ (некоторые модули) OTcl (описание скриптов)	C++ Python Оба языка для описания и модулей, и скриптов
Возможность соединения с реальными сетями (генерация трафика)	нет	да
Использование, поддержка	23.04.2014 Последняя версия 2.35	23.04.2014 Последняя версия 3.19
Исходный код	Открытый	Открытый
Описание модулей	Самых модулей больше,	Модулей меньше, но не-

Критерий сравнения	NS-2	NS-3
	т. к. симулятор старше	которые более детально проработаны (популярные, такие как lte, Wi-Fi)
Визуализация сети	Специальный пакет NAM (Network Animator) – анимационная система, написана на языке Tcl	Специальный пакет PyViz – пакет визуализации в реальном времени, написан на языке Phyton

В данной работе будет использован сетевой симулятор NS-3 [4, 5], т. к. он более актуален (в связи с отсутствием новых версий NS-2 с 2011 года), обладает более удобным представлением результатов симуляции (в формате *pcap*-файлов) и поддерживает возможность генерации трафика из NS-3 в реальную сеть.

### *Симуляция работы протокола маршрутизации при помощи NS-3*

В рамках данной работы была смоделирована сеть протокола маршрутизации AODV, состоящая из десяти узлов, находящихся на расстоянии 100 м друг от друга. Топология моделируемой сети представлена на рисунке 2. В ходе симуляции был рассмотрен процесс обнаружения маршрута.

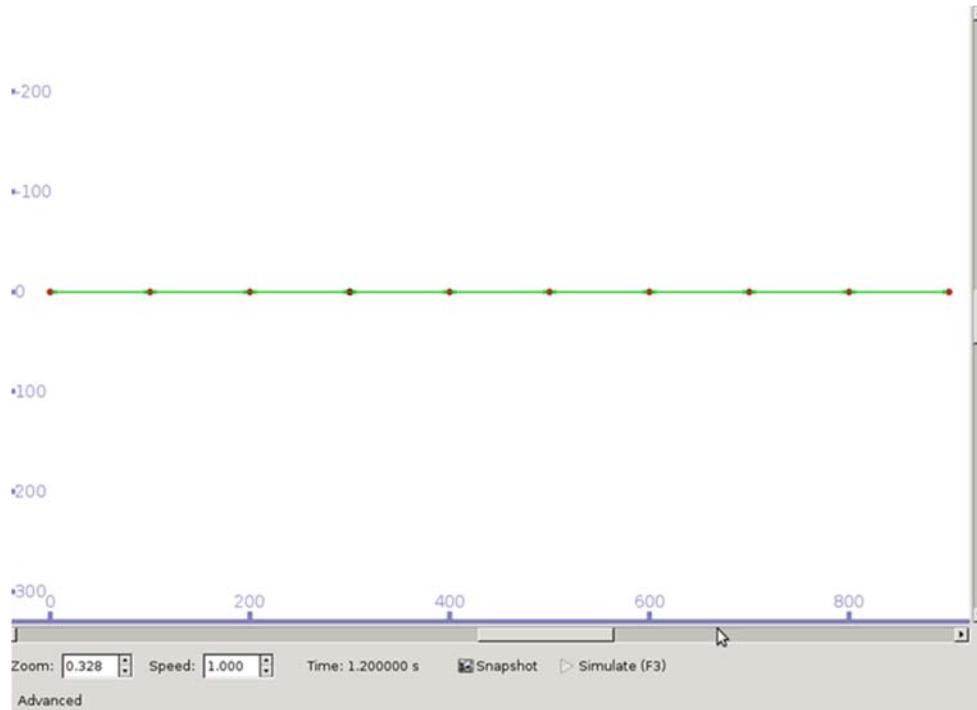


Рис. 2. Визуализация работы сети

В NS-3 используется понятие узла, под которым понимается компьютер, к которому добавляется различная функциональность, такая как приложения, стеки протоколов и т. д. При описании функциональности узлов, а также работы сети используется библиотека модулей, реализованная в NS-3, а также helper-ы – инструменты для упрощения процесса работы с модулями. Для моделирования исследуемой сети использовались следующие модули:

- AODV – описывает работу протокола маршрутизации AODV;
- Core – основной модуль, описывает работу самой симуляции;
- Network – описывает формат пакетов, модели ошибок в пакете, передачу пакетов между узлами;
- Internet – описывает стек протоколов TCP/IP, принципы маршрутизации, обнаружение соседей и др.;
- Mobility – описывает текущее положение узла, скорость объекта, размещение узлов;
- Wi-Fi – описывает создание сети на основе стандарта 802.11 (описывает физический и канальный уровни OSI).

Результаты моделирования представляются в формате pcap и могут быть открыты различными трафик-анализаторами. При этом результаты сохраняются для каждого узла в отдельности. В данной работе использовался трафик-анализатор Wireshark, работа которого показана на рисунке 3.

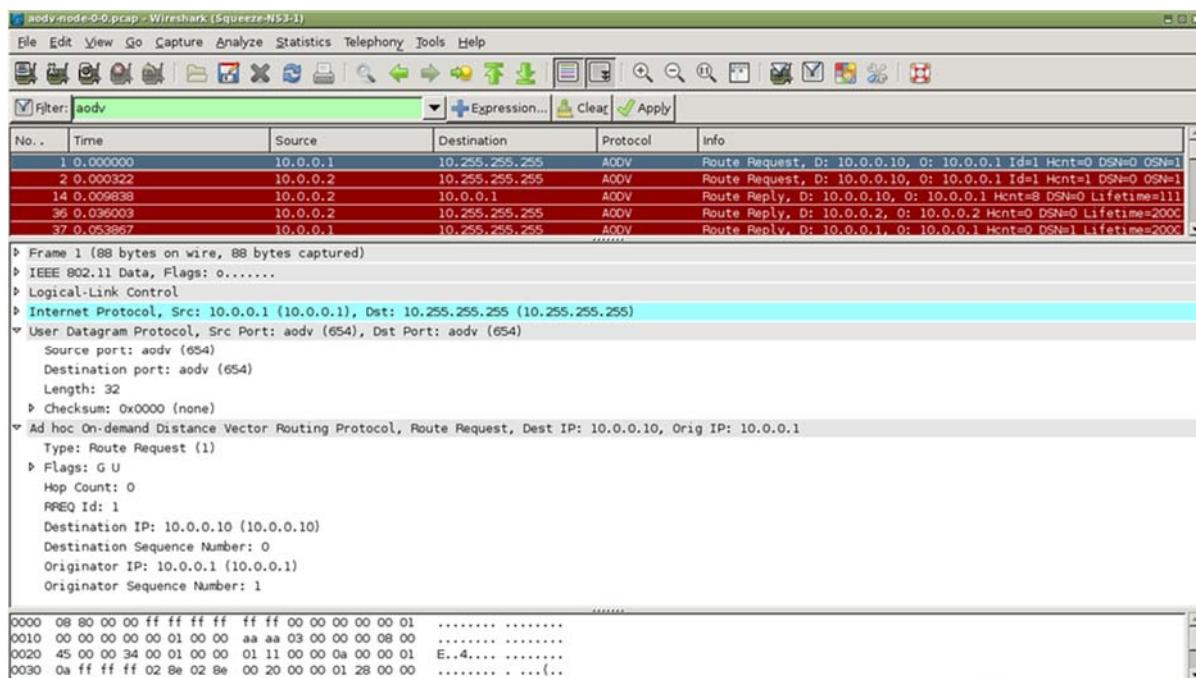


Рис. 3. Представление результатов моделирования при помощи Wireshark

## Заключение

В рамках данной работы была произведена симуляция работы протокола маршрутизации AODV при помощи сетевого симулятора NS-3. Работы по исследованию особенностей ad hoc сетей являются очень перспективными в связи с быстрым ростом популярности таких сетей и внедрением их в реальную жизнь. Созданная в данной работе сеть является очень полезным инструментом для реализации широкого спектра исследовательских работ и изучения различных технологий. В данном случае сконфигурированная сеть позволяет проводить исследовательские работы на тему маршрутизации в ad hoc сетях на примере протокола маршрутизации AODV, который широко используется в современных технологиях, например, в технологии ZigBee.

## Список используемых источников

1. **Classification** of Current Routing Protocols for Ad Hoc Networks – A Review [Электронный ресурс] / Beigh Bilal Maqbool, prof. M. A. Peer // International Journal of Computer Applications. – Vol. 7. – No 8. – С. 26–32. – Режим доступа: <http://www.ijcaonline.org/volume7/number8/pxc3871749.pdf> (Дата обращения 31.03.2014).
2. **Performance** analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator [Электронный ресурс] / S. Mohapatra, P. Kanungo // Procedia Engineering. – 2012. – Vol. 30. – С. 69–76. Режим доступа: <http://www.ijcaonline.org/volume7/number8/pxc3871749.pdf> (Дата обращения 31.03.2014).
3. **RFC 3561. Ad hoc On-Demand Distance Vector (AODV) Routing** [Электронный ресурс] / C. Perkins, E. Belding-Royer, S. Das – 2003. – Режим доступа: <http://www.ietf.org/rfc/rfc3561.txt> (Дата обращения 31.03.2014).
4. **NS-3 Manual** [Электронный ресурс]. – URL: <http://www.nsnam.org/docs/release/3.19/manual/html/index.html> (Дата обращения 31.03.2014).
5. **NS-3 Tutorial** [Электронный ресурс]. URL: <http://www.nsnam.org/docs/release/3.19/tutorial/html/index.html> (Дата обращения 31.03.2014).

*Статья представлена заведующим кафедрой «Инфокоммуникационные системы», д-ром техн. наук, профессором Б. С. Гольдштейном.*

**УДК 654.739**

**Е. В. Васильев (аспирант кафедры «Сети связи» СПбГУТ)**

## **АНАЛИЗ СПОСОБОВ САМООРГАНИЗАЦИИ В РОЕВЫХ СТРУКТУРАХ**

С развитием математики и алгоритмов одним из важнейших шагов к дальнейшей автоматизации стала самоорганизация. Самоорганизация – это механизм или динамический процесс, ведущий к возникновению, поддер-

жанию и изменению организации только за счет внутренних взаимодействий системы, без явного внешнего управления во время ее работы [1]. Алгоритмы самоорганизации хорошо подходят для сетей связи для автоматического добавления новых узлов к сети, изменения топологии сети в зависимости от условий и т. д. Самоорганизующиеся системы должны обладать следующими свойствами: автономность, открытость, глобальный порядок, эмерджентность, диссипация, адаптивность, сложность, простота правил взаимодействия, иерархическая структура.

В настоящее время для реализации самоорганизующихся систем используется парадигма мультиагентных систем. Мультиагентные системы (МАС) – это динамические экспертные системы, основанные на интеграции нескольких разнородных источников знаний. Эти источники обмениваются между собой получаемыми результатами в ходе решения задач. В МАС множество автономных агентов действуют в интересах различных пользователей и взаимодействуют между собой в процессе решения определенных задач. Примерами таких задач являются: управление информационными потоками и сетями, управление воздушным движением, поиск информации в сети Интернет, электронная коммерция, обучение, электронные библиотеки, коллективное принятие многокритериальных управлений решений и другие [2].

Классификация механизмов самоорганизации, описанная в [3], выглядит следующим образом:

– механизмы, основанные на кооперации. Этот механизм известен под названием AMAS-теория (*Adaptive Multi-Agent Systems theory*). В ней предполагается, что агенты обладают умениями, способностью к коммуникациям, знаниями о некоторых других агентах (соседях) и имеют критерии для обнаружения ситуаций, в которых возникают конфликты, разрешение которых требует специальных механизмов кооперации агентов. Самоорганизация поддерживается на основе локального взаимодействия агентов с целью кооперации. При этом агенты должны взаимодействовать в доброжелательной манере с элементами альтруизма;

– механизмы, основанные на использовании градиентных полей. Идея механизма была заимствована из физики, где примером градиентного поля являются электрическое или магнитные поля. Суть механизма заключается в том, что существует некоторая среда или структура, которая представляет собой вычислительное поле градиента. Поле можно представить в виде буфера, через который происходит обмен информацией между агентами. Распространение информации возлагается либо на само поле, либо на агентов. Таким способом в пространстве формируется некоторая форма поля, которая несет контекстную информацию, необходимую для координации. Ярким примером механизма является морфогенез;

– механизмы, основанные на рыночных взаимоотношениях. Механизм взят из рыночной экономики, а самоорганизация устанавливается за

счет покупки/продажи некоторого ресурса агентами, который ограничен в системе. При этом каждый агент может быть, как покупателем, так и продавцом. В системах, использующих модели самоорганизации на основе рыночных механизмов, макроэкономический уровень (равновесные цены и другие свойства, выводимые из ценовой информации) формируется как следствие эмерджентности, возникающей в результате локальных процессов на уровне микроэкономической модели. Именно поэтому в самоорганизующихся системах микроэкономический уровень, полностью заимствованный из экономической теории, играет главную роль;

– механизмы, основанные на обучении с подкреплением. Суть механизма заключается в том, что у каждого агента есть целевая функция, значение которой он хочет максимизировать. Самоорганизация возникает и поддерживается за счет взаимодействия с другими агентами в попытках оптимизировать свою целевую функцию. Также есть глобальная целевая функция, о которой ничего неизвестно элементам системы, но она зависит от целевых функций элементов системы, в результате чего могут возникать эмерджентные свойства;

– механизмы, использующие модель холонических систем. Парадигма холонических систем опирается на идею использования преимуществ централизованного подхода с одновременным увеличением автономности принятия решений отдельными элементами системы. В основе холонических организаций системы лежит термин «холон» (*holon*), предложенный А. Кестлером, и означающий дуалистичность сущности, являющейся одновременно и целым по отношению к ее элементам, и частью более общей системы [4]. Процессы объединения происходят динамически, а их результатом являются динамические структуры, составленные из иерархии холонов, которые называются холархиями. Холархии динамически изменяются в соответствии с изменениями внешней среды, и именно в этом состоит суть данного механизма самоорганизацию [5];

Возникновение модели самоорганизации и понятия самоорганизующейся системы во многом обязано примерам из биологических систем. Действительно, большинство механизмов самоорганизации, которые были предложены и которые в настоящее время уже практически используются в мультиагентных приложениях, заимствовано из биологических систем. Как правило, эти механизмы имеют в своей основе достаточно простые модели, которые укладываются в рамки приведенной выше классификации, хотя некоторые из них используют сразу несколько механизмов. Способы самоорганизации, заимствованные из природы:

– интеллект колонии муравьев. Заимствован механизм поиска пищи, который позволяет муравьям осуществлять перенос пищи в муравейник по самому короткому пути за счет выделения феромона. Эта модель положена в основу алгоритмов в задаче маршрутизации грузовиков при развозке гру-

зов в задаче коммивояжера в задаче маршрутизации пакетов в телекоммуникационных сетях, в задаче составления расписания и во мн. др.;

– молдинг. Суть этого механизма состоит в том, что специальный ресурс, доступный в среде, привлекает индивидуумов. Если ресурса много, то индивидуумы бродят и автономно его потребляют. Если ресурс скуден, то индивиды собираются вместе, формируя кластер. Потом кластер начинает перемещаться в среде как единое целое, как некоторый «суперорганизм», отыскивая место, более благоприятное с точки зрения наличия пищи. Когда оно находится, то ячейка снова рассыпается и начинается новый цикл. Практические применения механизма относятся к самосборке роботов для выполнения некоторой совместной деятельности;

– плетение сетей. Сеть плетется пауками для того, чтобы по ней было легко перемещаться и ловить добычу. Один из вариантов плетения сети реализуется пауками как коллективный самоорганизующийся процесс. Применяется в самоорганизующихся МАС, например, в качестве механизма быстрого просмотра распределенных данных в P2P-сетях, а также для решения задач маршрутизации в сети;

– сортировка особей. Самоорганизующийся механизм сортировки используется в биологических сообществах, например, для коллективной сортировки яиц, личинок и др. Практически этот механизм используется для организации базы данных и антивирусной защиты;

– сбор в стаи. Данный механизм может дать хорошее решение для большого разнообразия сценариев, например, для управления движением группы беспилотных летательных аппаратов;

– механизм кворума. Содержание этого механизма состоит в том, что индивиды организуют свое поведение в соответствии с поведением большинства. Примером является согласованная люминесценция светлячков;

– строительство гнезда. Идея самоорганизации при коллективном строительстве гнезда при отсутствии централизованного управления со стороны «мастера». Механизм находит широкое применение в коллективной робототехнике, в частности, для координации сотрудничества роботов в сборке конструкций.

– морфогенез. Именно этот механизм реализуется клетками в процессе самоорганизации для получения позиционной информации, а также информации о направлении при развитии эмбриона, суть которого состоит в следующем. На одном конце эмбриона клетки испускают морфоген, который распространяется по длине эмбриона с постепенным уменьшением концентрации, а потому значение концентрации может использоваться как источник информации о расстоянии клетки от начальной позиции эмбриона. Например, по этой информации клетки определяют, находятся ли они в районе головы, грудной клетки или в районе брюшной области эмбриона. Применяется в задачах управления самосборкой модульных роботов, генерирующих некоторое поле в качестве виртуального морфогена [4].

В таблице приведено сравнение биологических механизмов самоорганизации. В виду отсутствия количественных параметров для сравнения, были выбраны критерии, которые характеризуют основной базис для построения самоорганизации: тип взаимодействия (косвенное через среду или напрямую между агентами), тип передаваемой информации (как агенты передают информацию другим членам роя) и способ распространения информации внутри роя (по случаю – когда агент бесцельно блуждает, пока не наткнется на переданную информацию другим агентом; передача с помощью градиентного поля; диффузия – широковещательное распространение информации).

ТАБЛИЦА. Сравнение биологических механизмов и алгоритмов самоорганизации

	Тип взаимодействия	Тип информации	Реализация обмена информацией
Колония муравьев	Косвенное	Маркер	По случаю
Молдинг	Прямое	Маркер	Градиентное поле
Плетение сети	Косвенное	Смысловый	По случаю
Сортировка особей	Косвенное	Смысловый	По случаю
Сбор в стаи	Косвенное	Смысловый	Диффузия
Механизм кворума	Прямое	Маркер	Диффузия
Строительство гнезда	Косвенное	Маркер	Градиентное поле
Морфогенез	Косвенное	Маркер	Диффузия

Как видно из таблицы, большинство алгоритмов, принципы которых были заимствованы из природы, используют маркер, который обычно является феромоном. И, в зависимости от имитируемого способа, передается либо напрямую между агентами, либо распространяется через окружающую среду, через которую агенты обмениваются информацией, влияя друг на друга.

#### Список используемых источников

1. **Self-organisation** in multi-agent systems [Электронный ресурс] / G. Di Marzo Serugendo, M.-P. Gleizes, A. Karageorgos. – Режим доступа: [http://www.irit.fr/TFGSO/DOCS/TFG2/TFGIISO\\_LongReport.pdf](http://www.irit.fr/TFGSO/DOCS/TFG2/TFGIISO_LongReport.pdf) (Дата обращения 20.04.2014).
2. Интеллектуальные информационные системы : учебник / А. В. Андрейчиков, О. Н. Андрейчикова. – М. : Финансы и статистика, 2004. – 424 с.
3. **Self-organization** in multi-agent systems / G. Di Marzo Serugendo, M.-P. Gleizes, A. Karageorgos // J. Knowledge Engineering Review. – 2005. – V. 20. – № 2. – PP. 165–189.
4. **Многоагентные** производственные системы [Электронный ресурс] / А. В. Ахтеров // Современные системы искусственного интеллекта и их приложения в

науке. – 2013. – С. 127. – Режим доступа: [http://www.paxgrid.ru/proceedings\\_ai2013.pdf](http://www.paxgrid.ru/proceedings_ai2013.pdf) (Дата обращения 20.04.2014).

5. **Самоорганизация** и многоагентные системы. I. Модели самоорганизации и их приложения в программных инфраструктурах компьютерных сетей [Электронный ресурс] / В. И. Городецкий – Режим доступа: <http://ips-logistic.com/wp-content/uploads/2012/06/Self-organization-2011.pdf> (Дата обращения 20.04.2014).

*Статья представлена научным руководителем канд. техн. наук, доцентом О. А. Симониной.*

**УДК 004.056.57**

**А. А. Галицкий (студент группы СП-91 СПбГУТ)**

## **ОБНАРУЖЕНИЕ И ИЗМЕРЕНИЕ СТЕПЕНИ СХОДСТВА КОДА ПРИЛОЖЕНИЙ ДЛЯ ОС ANDROID**

В настоящее время операционная система Android фирмы Google является самой популярной операционной системой для смартфонов и планшетов, а в ближайшем будущем и любых носимых устройств-гаджетов (*Android Wear*). Доля устройств под управлением ОС Android оценивается в 70–80 % рынка. Ожидается, что к 2017 году их количество достигнет 1 миллиарда с более чем 50 миллиардами установленных приложений [1].

Исследования в области мобильных угроз и вирусов показали высокие темпы роста вредоносных приложений для данной мобильной платформы [2]. Так в период с 2012 по 2013 годы их число приближается к 718000. Летом 2012 года атаки Eurograbber показали, что вредоносные мобильные приложения являются очень прибыльным бизнесом, когда со счетов клиентов банков Италии, Германии, Испании и Нидерланд было украдено примерно 36 миллионов евро [3].

Помимо всего вышеупомянутого, каждый день выходит около 700 новых приложений для ОС Android, что делает актуальным и первостепенным вопрос о сходстве программного кода в приложениях для мобильных платформ и его автоматизированном анализе. Так, обнаружение и измерение степени сходства кода играет одну из определяющих ролей в эвристических алгоритмах нахождения потенциально опасного кода.

Основной целью доклада является исследование предметной области, методологии и математического аппарата для обнаружения и измерения сходства программного кода в приложениях для ОС Android. В данном докладе рассматривается код приложений для ОС Android, написанный на языке программирования Java, но методы обнаружения также могут быть

применимы и для любого другого программного кода, написанного на любом из языков программирования.

Большинство методов обнаружения похожего программного кода основаны на семантическом сходстве. Эти методы можно разделить на четыре категории: анализ на основе строк, анализ на основе токенов, анализ на основе деревьев, анализ на основе семантики кода с использованием графа зависимостей.

В качестве метрики можно выбрать одно из двух известных на сегодняшний день расстояний, используемых для анализа строк на сходство, в нашем случае программного кода. Это расстояния NCD [4] и Левенштейна [5]. Также существует модификация расстояния Левенштейна – расстояние Дамерау-Левенштейна.

Далее будем использовать расстояние Дамерау-Левенштейна, так как оно, в отличие от NCD, не зависит от алгоритма сжатия и от размера анализируемого куска кода, что дает более точную оценку схожести.

Метрика Дамерау-Левенштейна – это расстояние между двумя строками в теории информации и компьютерной лингвистике – определяется как минимальное количество операций вставки одного символа, удаления одного символа, операции перестановки и замены одного символа на другой, необходимых для превращения одной строки в другую.

Расстояние Дамерау-Левенштейна, как и метрика Левенштейна, является мерой «схожести» двух строк. Существует два алгоритма нахождения данного расстояния: упрощенный и корректный.

Далее будем рассматривать и использовать упрощенный алгоритм, который не решает задачу корректно, но бывает полезен на практике.

Здесь и далее будем использовать следующие обозначения:  $S$  и  $T$  – строки, между которыми требуется найти расстояние Дамерау-Левенштейна;  $M$  и  $N$  – их длины соответственно.

Рассмотрим алгоритм, отличающийся от алгоритма поиска расстояния Левенштейна одной проверкой (храним матрицу  $D$ , где  $D(i, j)$  – расстояние между префиксами строк: первыми  $i$  символами строки  $S$  и первыми  $j$  символами строки  $T$ ). Рекуррентное соотношение имеет вид:

$$D(M, N),$$

где

$$D(i, j) = \begin{cases} \min(A, D(i - 2, j - 2) + transposeCost); & i > 1, j > 1, S[i] = T[j - 1], S[i - 1] = T[j], \\ A; & otherwise, \end{cases}$$

$$A = \begin{cases} 0 ; i = 0, j = 0, \\ i; j = 0, i > 0, \\ j; i = 0, j > 0, \\ D(i - 1, j - 1); S[i] = T[j], \\ \min \left( \begin{array}{l} D(i, j - 1) + insertCost, \\ D(i - 1, j) + deleteCost, \\ D(i - 1, j - 1) + replaceCost \end{array} \right); j > 0, i > 0, S[i] \neq T[j]. \end{cases}$$

Таким образом, для получения ответа необходимо заполнить матрицу  $D$ , пользуясь рекуррентным соотношением. Сложность алгоритма:  $O(M^*N)$ . Затраты памяти:  $O(M^*N)$ .

Контрпример:  $S = "CA"$  и  $T = "ABC"$ . Расстояние Дамерау-Левенштейна между строками равно 2 ( $CA \rightarrow AC \rightarrow ABC$ ), однако функция, приведённая выше, возвратит 3. Дело в том, что использование этого упрощённого алгоритма накладывает ограничение: любая подстрока может быть редактирована не более одного раза. Поэтому переход  $AC \rightarrow ABC$  невозможен, и последовательность действий такая: ( $CA \rightarrow A \rightarrow AB \rightarrow ABC$ ). Условие многих практических задач не предполагает многократного редактирования подстрок, поэтому часто достаточно упрощённого алгоритма.

Например, для закодированных деревьев в виде строк:

123423412341234436467846786345876341847652367457862384534152  
6354913974694546597864987456452176423649872167364896349569  
123423412341234436467846786345876341847656567457862384534152  
6354943974694546597867687456452176423649872567364896049569

$NCD\ similarity = 63,043\% (bz2), 69,863\% (zlib).$

$DamerauLevenshtein\ similarity = 94,118\%.$

Так как каждый метод принадлежит определенному классу и имеет уникальный opcode, то можно представить, что совокупность всех системных методов в приложении для ОС Android – это алфавит, на который распространяется метрика (расстояние Дамерау-Левенштейна).

Алгоритм поиска схожих частей кода состоит в следующем:

- построение дерева методов и классов в процессе разбора .dex (*dalvik executable*) файла;
- нахождение редакционного расстояния Дамерау-Левенштейна между двумя деревьями;
- на основании вычисленного расстояния принимается решение о схожести двух сегментов кода в приложениях.

Данный алгоритм реализован на языке Python в виде библиотеки и составляющих ее модулей, что делает программу кроссплатформенной и удобной для многократного использования в других проектах.

Разработанный алгоритм позволяет находить схожие куски программного кода, написанного не только для ОС Android, но и на любом

другом языке программирования, разница заключается лишь в модуле построения дерева методов и классов. На данный момент существуют некоторые ограничения, связанные с отличием в синтаксисах языков программирования, использованием динамического построения кода и существованием интерфейсов, абстрактных классов и виртуальных методов.

### **Список используемых источников**

1. Over 1 billion Android-based smart phones to ship in 2017 [Электронный ресурс] / Canalys. – Режим доступа: <http://www.canalys.com/newsroom/over-1-billion-android-based-smart-phones-ship-2017>. – 2013.
2. Kindsight Security Labs Malware Report – Q2 2013 [Электронный ресурс] / Alcatel-Lucent. – Режим доступа: <http://www.kindsight.net/sites/default/files/Kindsight-Q2-2013-Malware-Report.pdf>. – 2013.
3. A Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware [Электронный ресурс] / Eran Kalige and Darrel Burkey. – Режим доступа: [http://www.cs.stevens.edu/~spock/Eurograbber\\_White\\_Paper.pdf](http://www.cs.stevens.edu/~spock/Eurograbber_White_Paper.pdf). – 2012.
4. The similarity metric, IEEE Trans. Inform / Th. M. Li, X. Chen, X. Li, B. Ma, P.M.B. Vitanyi. – 2004. – С. 34–36.
5. Двоичные коды с исправлением выпадений, вставок и замещений символов / В. И. Левенштейн // Доклады Академии Наук СССР, 1965. – С. 67–74.

*Статья представлена научным руководителем, доцентом О. Б. Петровой.*

**УДК 621.391**

**Гамиль Абдуллах (аспирант кафедры ИКС СПбГУТ)**

## **ОЦЕНКА ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК СИГНАЛЬНОГО ТРАФИКА В NGN НА БАЗЕ IMS**

Появление концепции IMS (*IP Multimedia Subsystem*) как решение, используемое при построении мультисервисных сетей, привело к эволюционным переходам сети связи общего пользования в пакетизации. Изначально технология IMS разрабатывалась консорциумом 3GPP для сетей мобильной связи третьего поколения 3G, а потом была предложена и для фиксированной сетей связи следующего поколения NGN (*Next Generation Network*). Для установления, управления и разъединений сессиями в подсистеме IMS используется протокол сигнализации SIP (*Session Initiation Protocol*), а при выполнении процессов авторизации, аутентификации и учета – протокол Diameter [1].

## Постановка задачи

В целях обеспечения анализа вероятностно-временных характеристик сети связи на базе подсистемы IMS, в данной работе производится оценка времени задержки сигнального трафика при регистрации пользователя в сети, как важного параметра качества обслуживания. Регистрация является необходимой процедурой при работе в сети IMS. Не зарегистрированным пользователям требуется аутентификация для доступа к услугам IMS.

Процесс регистрации начинается с момента, когда терминальное оборудование абонента передало всю информацию, необходимую для регистрации пользователя в сети, до момента, когда это оборудование получило сигнал о подтверждении успешной регистрации и аутентификации.

Диаграмма на рисунке 1 отображает процедуру регистрации пользователя в сети IMS при условии, что пользователь находится в гостевой сети.

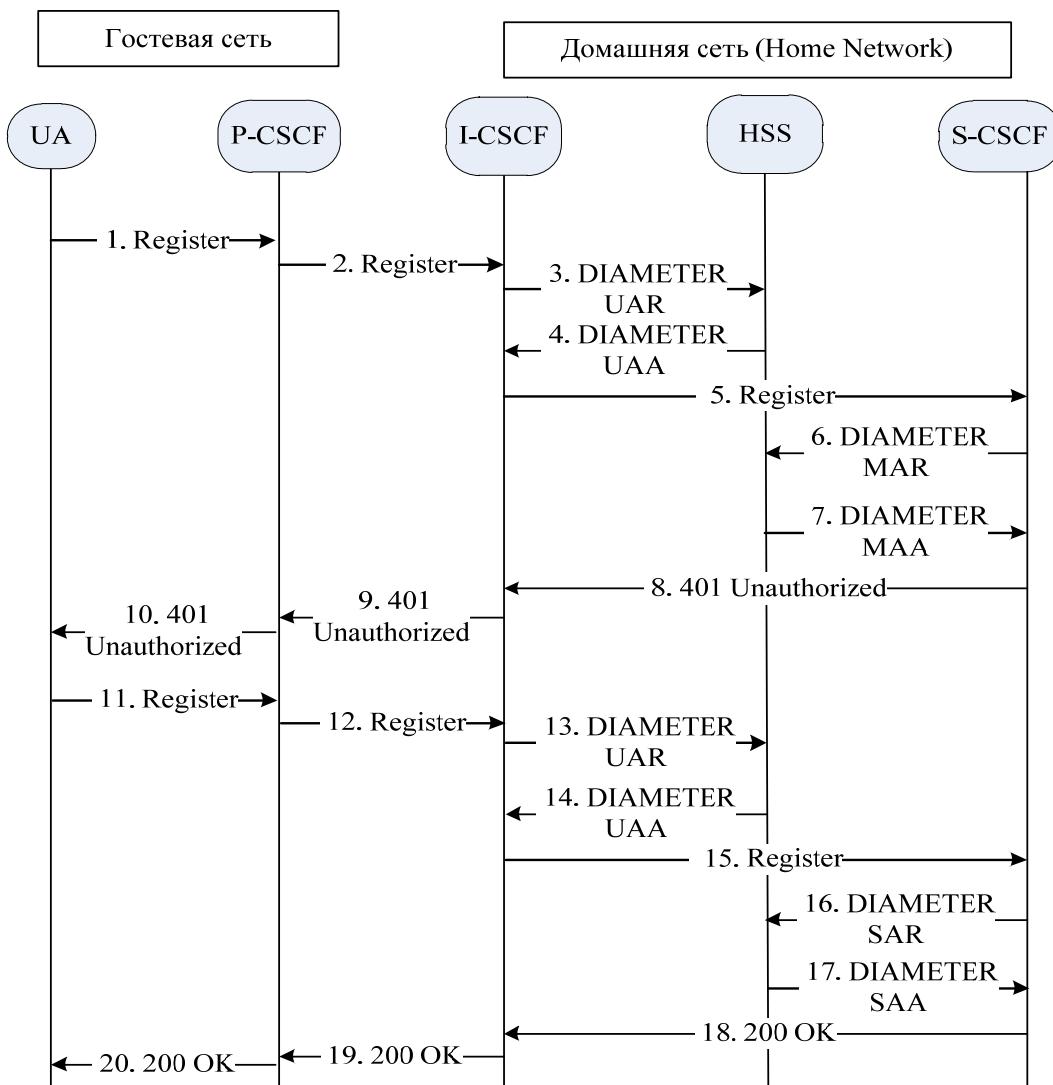


Рис. 1. Процедура регистрации в IMS

### *Анализ задержки сигнального трафика в IMS*

В этом разделе представлена модель анализа задержки сигнального трафика при регистрации пользователя в IMS сети. Анализ задержки сигнального обмена начинается с момента передачи оборудованием пользователя запроса протокола SIP Register, до момента подтверждения успешной регистрации ответом 200 OK. Задержка сигнального обмена в IMS при регистрации состоит из трех элементов:

$$\overline{D} = \overline{D}_t + \overline{D}_p + \overline{D}_q,$$

где,  $\overline{D}$  – общее среднее задержки IMS сигнализации,  $\overline{D}_t$  – средняя задержка передачи;  $\overline{D}_p$  – средняя задержка обработки;  $\overline{D}_q$  – средняя задержка ожидания в очереди.

*Задержкой передачи* является время, затраченное на трансляцию сигнального сообщения на транспортном уровне и по сети доступа, и зависит от размера сообщения, пропускной способности канала, расстояния между узлами сети и характеристиками канала. Можно предположить, что задержка передачи между узлами IMS незначительна из-за высокой доступной пропускной способности. Для задержки передачи в сети доступа это, как правило, не так. Во время процедуры регистрации, передача сигнальных сообщений по сети доступа происходит четыре раза между UA и сервером P-CSCF, расположенным в ядре сети IMS (Сообщения 1, 10, 11 и 20 на [рис. 1](#)). Задержка передачи сообщений  $\overline{D}_{t-imsreg}$  будет равна:

$$\overline{D}_{t-imsreg} = 4 \times \overline{D}_{t-an}.$$

*Задержка обработки* – время, в течение которого происходит анализ сигнального сообщения, его обработка и формирование следующего запроса, либо ответа. Основная длительность в задержке обработки вызвана поиском адреса в базе данных HSS, где хранятся записи пользователей на основе IP-адресов в адресных таблицах.

Задержка обработки при регистрации пользователя  $\overline{D}_{p-imsreg}$  определяется:

$$\overline{D}_{p-imsreg} = 2d_{p-ua} + 4d_{p-pcscf} + 6d_{p-icscf} + 4d_{p-hss} + 4d_{p-scscf}$$

где,  $d_{p-ua}, d_{p-pcscf}, d_{p-icscf}, d_{p-hss}, d_{p-scscf}$  обозначают задержки обработки пакетов на узлах UA, P-CSCF, I-CSCF, HSS, и S-CSCF, соответственно, а целые коэффициенты – это число сигнальных сообщений, обработанных в соответствующих узлах сигнализации при регистрации ([рис. 1](#)). Таким образом, задержка обработки в узле моделируется путем подсчета количества сообщений, полученных узлом.

*Задержкой очереди* является задержка, ожидания обслуживания в узлах сети. Анализ задержки очереди включает в себя все узлы сети, участвующие в процедурах сигнального обмена в IMS. Общая задержка пакетов в очереди является суммированием задержки во всех узлах сети массового обслуживания (СeМО), и зависит от числа пакетов в очереди в данный момент времени на этом узле.

В рамках предлагаемой математической модели, предположим, что поступающий поток заявок пуассоновский, обслуживание в узлах сети экспоненциальное и выполняется условие равновесного режима функционирования сети. Таким образом, построим модель сигнального трафика для процедуры перерегистрации в виде BCMP-сети [2, 3], представляющая собой открытую неоднородную СeМО с несколькими классами заявок и дисциплинами обслуживания M/M/1 во всех узлах сети. BCMP – это сокращение от первых букв фамилий авторов предложенного метода анализа подобных СeМО: Baskett, Chady, Muntz и Palacios. Метод BCMP позволяет получить уравнения равновесия (глобального баланса) для сетей, обслуживающих заявки разных классов. При этом сеть включает в себя узлы нескольких типов, которые различаются количеством обслуживающих приборов  $M = \{1, \dots, M\}$ , между которыми циркулируют заявки из конечного множества различных классов  $R = \{1, \dots, R\}$ . Анализ ВВХ можно продолжить на основании теоремы BCMP [2].

Классы BCMP-заявок, используемых при построении модели перерегистрации выглядят следующим образом: Register – (1), UAR – (2), UAA – (3), SAR – (4), SAA – (5), 200 OK – (6). Рисунок 2 изображает сеть BCMP для процедуры перерегистрации пользователя в IMS.

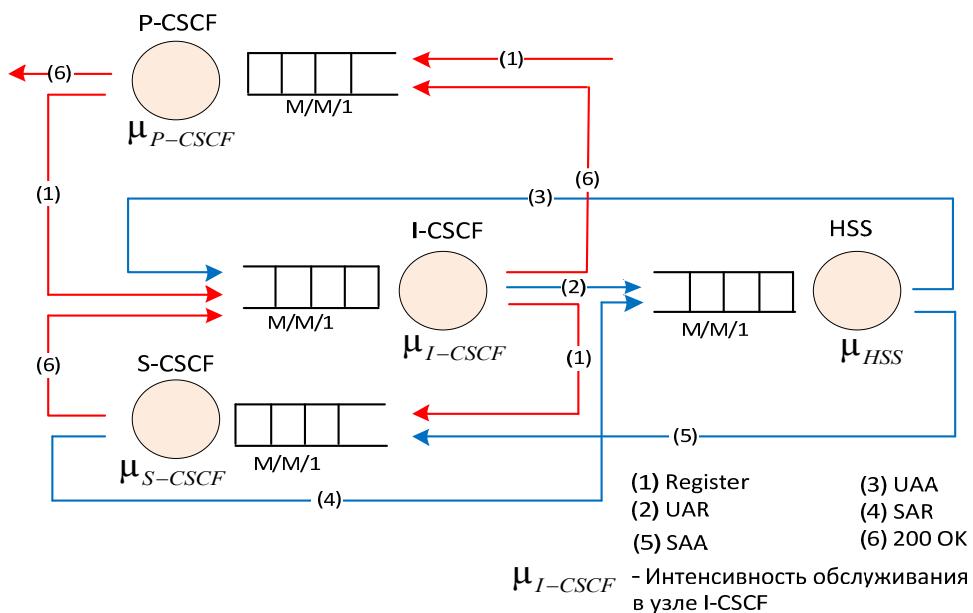


Рис. 2 . Модель процедуры перерегистрации

Таким образом, задержка очереди в узлах сети при перерегистрации  $\overline{D}_{q-imsreg}$  [4]:

$$\overline{D}_{q-imsreg} = 4d_{q-pcscf} + 6d_{q-icscf} + 4d_{q-hss} + 4d_{q-scscf},$$

где  $d_{q-pcscf}, d_{q-icscf}, d_{q-hss}, d_{q-scscf}$  обозначают задержки пакетов в очереди на узлах P-CSCF, I-CSCF, HSS и S-CSCF, соответственно.

Каждой заявке, поступающей в систему, соответствует маршрут, который отслеживает путь следования заявки между узлами с учетом изменения ее класса. Данный путь описывается квазистохастической маршрутной матрицей:

$$\Theta' = (\theta_{ir,js}); i, j \in M; r, s \in R,$$

где  $\theta_{ir,js}$  – вероятность того, что после окончания обслуживания  $(i,r)$  – заявка может стать  $(j,s)$ -заявкой. Если обозначим,  $\lambda_{ir}$  – интенсивность поступающего потока заявок на узел  $i$  класса  $r$ , то уравнение равновесия для интенсивности потоков в узлах сети равняется:

$$\lambda_{ir} = \sum_{(j,s) \in \Omega} \lambda_{js} \theta_{js,ir}, i, r \in \Omega$$

где  $\Omega$  – множество всех допустимых заявок обслуживаемых в сети.

Средняя задержка пакетов в очереди на  $i$ -узле IMS является [5]:

$$d_i = \frac{\rho_i}{\mu_i(1-\rho_i)},$$

где  $\rho_i = \lambda_i / \mu_i$  – интенсивность нагрузки в  $i$ -узел IMS,  $\mu_i$  – интенсивность обслуживания в узле  $i$ ,  $\lambda_i$  – интенсивность поступающего потока заявок в  $i$ -узле. Интенсивность прибытия заявок в  $i$ -узле  $\lambda_i$  можно рассчитать через нагрузки и связанное с ним время пребывания в очереди.

Таким образом, общая задержка при регистрации в IMS вводится следующим:

$$\overline{D}_{imsreg} = \overline{D}_{t-imsreg} + \overline{D}_{p-imsreg} + \overline{D}_{q-imsreg}$$

Важно отметить, что если пользователь не зарегистрирован в сети IMS, то он должен пройти процесс регистрации в сети до установления сеанса связи.

### Список используемых источников

1. IP Multimedia Subsystem: принципы, стандарты и архитектура / Г. Г. Яновский // Вестник связи. – 2006. – № 3. – С. 71–76.
2. Теоретические основы проектирования компьютерных сетей / В. М. Вишневский. – М. : Техносфера, 2003. – 512 с.

3. **Open, Closed and Mixed Networks of Queues with Different Classes of Customers /** F. Baskett, K. Chandy, R. Muntz and F. Palacios // Journal of the ACM. – 1975. – Vol. 22. – No 2. – P. 248–260.

4. **Разработка** вероятностной модели для анализа показателей качества протокола инициирования сеансов связи / К. Е. Самуилов, М. В. Лузгачев, О. Н. Плаксина // Вестник Российской университета дружбы народов. Серия Математика. Информатика. Физика. – 2007. – № 3–4. – С. 53–63.

5. **Задачи** планирования сетей электросвязи / Н. А. Соколов. – СПб. : Протей, 2012. – 432 с.

*Статья представлена научным руководителем д-ром техн. наук, профессором Б. С. Гольдштейном.*

**УДК 654.739**

**Л. Р. Гарапова (студентка СПбГУТ)**

**В. И. Коржик (профессор кафедры ЗСС СПбГУТ)**

## **ИССЛЕДОВАНИЕ МЕТОДОВ ОТРИЦАЕМОГО ШИФРОВАНИЯ**

Отрицаемое шифрование представляет собой криптографическое преобразование, обеспечивающее достаточно высокую стойкость к принуждающим атакам. В атаках такого типа предполагается наличие у атакующего некоторого ресурса воздействия на отправителя, получателя или хранителя криптоGRAMМЫ, который обеспечивает принуждение владельцев криптоGRAMМЫ представить ключ дешифрования криптоGRAMМЫ.

Первый метод отрицаемого шифрования основывается на шифре Вернама.

Сообщение и ключ представляют собой  $n$ -битовые двоичные цепочки:

$$m = m_1 m_2 \dots m_n \in \{0,1\}^n,$$

$$k = k_1 k_2 \dots k_n \in \{0,1\}^n.$$

Ключ в данном шифре является истинно случайным, все его варианты равновероятны, ключ совпадает по размеру с исходным сообщением и применяется только один раз [1].

Преобразование исходного сообщения  $m$  выглядит как формирование криптоGRAMМЫ  $c = c_1 c_2 \dots c_n \in \{0,1\}^n$  побитовым сложением последовательности сообщения и ключа:

$$c_i = m_i \oplus k_i,$$

где  $1 \leq i \leq n$ .

Процедура дешифрования засекреченного сообщения имеет двойственный характер.

Легитимный пользователь с помощью истинного ключа способен получить исходное сообщение согласно формуле:

$$m = c \oplus k.$$

В случае оказания принуждения к любой стороне данной симметричной крипtosистемы, атакующему для проведения процедуры дешифрования выдается ложный ключ. Ложный ключ формируется на основе ложного сообщения, не являющегося секретным. Длина бинарной последовательности ложного сообщения должна быть равна длине последовательности исходного сообщения:

$$\begin{aligned} m &= m_1 m_2 \dots m_n \in \{0,1\}^n, \\ m_f &= m_{f_1} m_{f_2} \dots m_{f_n} \in \{0,1\}^n. \end{aligned}$$

Генерирование ложного ключа производится с помощью операции сложения по модулю 2 по формуле:

$$k_f = c \oplus m_f.$$

Созданная в результате шифрования по данной схеме криптограмма  $c$  передается получателю по открытому (незащищенному) каналу связи. Дешифрование атакующим производится по формуле

$$m_f = k_f \oplus c.$$

Крипtosистема отрицаемого шифрования на основе шифра Вернама является абсолютно стойкой ко всем видам атак [1].

Особенностью данного криптоалгоритма является то, что длина ключа всегда должна быть равна длине сообщения, и не допускается повторное использование ключа для засекречивания разных сообщений. Следовательно, в случае необходимости шифрования информации большой по объему, возникает проблема хранения и обращения столь длинного ключа.

Рассмотрим метод отрицаемого шифрования на коротких ключах, основанный на китайской теореме об остатках, сформулированной для двоичных многочленов. Данная математическая модель отрицаемого шифрования является модифицированной версией модели, описанной в [2].

Выбранный алгоритм состоит из следующих этапов:

1. Первичное шифрование осуществляется симметричным блочевым упрощенным подстановочно-перестановочным шифром. Входные 16-ти битовые блоки, представленные в бинарном виде, зашифровываются пятью раундовыми ключами по схеме, приведенной в [1]. Результатом являются две криптограммы:  $C_1$  – для истинного сообщения и  $\bar{C}_1$  – для ложного:

$$C_{11} = f(K_1, M_1), \quad (1)$$

$$\overline{C_{11}} = f(\overline{K_1}, \overline{M_1}),$$

где  $f(,)$  – функция шифрования ППШ,  $M_1, \overline{M_1}$  – первые блоки истинного и ложного сообщений,  $K_1, \overline{K_1}$  – истинный и ложный подключи (первые).

2. Вторичный этап шифрования осуществляется с использованием секретного ключа в виде подключей  $K_2, \overline{K_2}$  и двух простых чисел  $p$  и  $\overline{p}$ . Шифрование блоков  $C_{11}$  ( $p > C_{11}$ ) и  $\overline{C_{11}}$  ( $\overline{p} > \overline{C_{11}}$ ) осуществляют путем вычисления значения  $C_{12}$  по формуле:

$$C_{12} = [C_{11}] \cdot K_2 \bmod p, \quad (2)$$

вычисления значения  $\overline{C_{12}}$  по формуле:

$$\overline{C_{12}} = [\overline{C_{11}}] \cdot \overline{K_2} \bmod \overline{p}, \quad (3)$$

где двоичные последовательности  $C_{11}$  и  $\overline{C_{11}}$  представлены числами  $[C_{11}]$  и  $[\overline{C_{11}}]$ , не превосходящими  $2^n$ , где  $n$  – длина блокового шифра,  $K_2, \overline{K_2}$  – истинный и ложный подключи (вторые),  $K_2, \overline{K_2} < 2^n$ ,  $p, \overline{p}$  – истинный и ложный подключи (третьи),  $p, \overline{p} > 2^n$ ,  $\gcd(p, \overline{p}) = 1$ .

3. Формирование общего блока криптоматы  $C$ , которое является решением системы сравнений:

$$\begin{cases} C_1 = [C_{12}] \bmod p; \\ C_1 = [\overline{C_{12}}] \bmod \overline{p}, \end{cases}$$

Криптомату можно записать в виде:

$$\begin{cases} C_1 = [C_{11}] \cdot K_2 \bmod p; \\ C_1 = [\overline{C_{11}}] \cdot \overline{K_2} \bmod \overline{p}. \end{cases} \quad (4)$$

В соответствии с китайской теоремой об остатках [1] решение системы сравнений (4) вычисляется по следующей формуле:

$$C_1 = C_{11} \cdot \overline{p} \cdot ((\overline{p})^{-1} \bmod p) \bmod (p \cdot \overline{p}) + p \cdot (p^{-1} \bmod \overline{p}) \bmod (p \cdot \overline{p}). \quad (5)$$

Заметим, что эта общая криптоматма блока может иметь длину большую, чем  $n$ -длину блокового шифра.

4. Дешифрование секретного сообщения  $M_1$  выполняется с использованием ключа, представляющего собой тройку значений  $(K_1, (K_2)^{-1} \bmod p, p)$  по формуле:

$$M_1 = g(K_1, [C_1 \cdot (K_2)^{-1} (\bmod p)]^{-1}),$$

где  $g$  – функция дешифрования для блокового шифра (ППШ),  $[ \dots ]^{-1}$  – означает преобразование десятичного числа в двоичный блок.

5. Пусть для раскрытия при вынуждающей атаке предназначено сообщение  $\overline{M}$ . Рассмотрим дешифрование первого блока сообщения  $\overline{M_1}$ . Тогда атакующему предоставляется в качестве ключа шифрования тройка

значений ( $\overline{K_1}$ ,  $(\overline{K_2})^{-1} \bmod \overline{p}$ ,  $\overline{p}$ ). Процедура получения сообщения по известной криптограмме производится как:

$$(\overline{M_1} = g(\overline{K_1}, [C_1 \cdot \overline{K_2}^{-1} (\bmod \overline{p})]^{-1}).$$

Атакующему известен алгоритм шифрования (2) и (3), известна функция дешифрования блокового шифра  $g(\dots)$ . Скрытие алгоритма формирования общей криптограммы (4) обеспечивает невозможность возникновения подозрений по поводу существования в данной криптограмме еще какой-либо информации кроме полученного ложного сообщения.

Приведем доводы, которые могут возникнуть у атакующего:

- увеличение длины зашифрованного текста по сравнению с первоначальным текстом;
- неполное использование криптограммы в процессе дешифрования;
- невозможность получения по приведенным формулам криптограммы «обратным» шифрованием сообщения.

Для правдоподобного объяснения процесса шифрования атакующему необходимо выдать используемый алгоритм отрицаемого шифрования за вероятностное шифрование. При вероятностном шифровании длина криптограммы по сравнению с исходным сообщением увеличивается за счет использования случайного числа, которое уничтожается после формирования криптограммы [1].

Проведем совмещение отрицаемого шифрования с вероятностным в едином алгоритме. Получение при зашифровывании сообщения  $\overline{M_1}$  вероятностным способом шифротекста, совпадающего с криптограммой, полученной в результате зашифрования двух различных сообщений по различным ключам по формулам (1), (2), (3), возможно с использованием randomизации.

Схема выглядит как формирование криптограммы сообщения  $\overline{M_1}$  (1) и (3) с последующим дополнительным вероятностным преобразованием для повышения криптографической стойкости:

$$C_1 = [\overline{C_{12}} + \overline{p} \cdot R],$$

где  $R$  – случайное число, которое потом стирается и по этой причине оно не может быть предоставлено атакующему.

Чтобы показать, что значение  $R$  не является случайным, атакующий должен вычислить истинные подключи  $(K_1, (K_2)^{-1} \bmod p, p)$  и с их помощью расшифровать сообщение  $M$ . Однако при выборе чисел  $K_1, K_2$  и  $p$  размером 256 бит их вычисление по криптограмме  $C$  и ложным подключами  $(\overline{K_1}, (\overline{K_2})^{-1} \bmod \overline{p}, \overline{p})$  является вычислительно невыполнимой задачей.

Перечисленные выше методы были успешно реализованы на практике. Требования к стойкости и неотличимости от подменяемого метода шифрования удовлетворяются.

## Список используемых источников

1. Основы криптографии / В. И. Коржик, В. П. Просихин. – СПб. : Линк, 2008. – 250 с.
1. Способ отрицаемого шифрования / А. Н. Березин, А. Р. Биричевский, Н. А. Молдовян // Вопросы защиты информации – 2013. – № 2. – С. 18–21.

**УДК 004.056**

**В. Ю. Гойхман (доцент кафедры ИКС СПбГУТ)**

**Т. Ю. Лушникова (студентка группы СП-91 СПбГУТ)**

## АТАКИ НА ПРОТОКОЛЫ МАРШРУТИЗАЦИИ *AD HOC* СЕТЕЙ

Сетями ad hoc называют одноранговые беспроводные сети передачи данных с переменной топологией и отсутствием четкой инфраструктуры, где каждый узел может выполнять функции маршрутизатора и принимать участие в ретрансляции пакетов данных. Отличительной особенностью этих сетей является их самоорганизация, позволяющая узлам устанавливать соединения по мере их необходимости, и не предполагающая фиксированной инфраструктуры. Из-за того, что узлы обмениваются информацией в беспроводной среде передачи, а также могут быть подвижны и вынуждены доверять друг другу, не имея координатора, следящего за маршрутизацией, ad hoc сети используют протоколы маршрутизации, передающие в общий канал сведения о топологии сети, что делает их привлекательной мишенью для реализации различного рода атак [1, 2].

Выделяют три основных аспекта обеспечения безопасности: обеспечение конфиденциальности, целостности и доступности информации. Любое злонамеренное действие, призванное нарушить безопасность системы, называется атакой.

По виду оказываемого воздействия атаки можно разделить на пассивные и активные [3, 4]. Во время пассивных атак злоумышленники не вмешиваются в работу сети, а только прослушивают передаваемую информацию, не изменяя ее. Активные, в свою очередь, изменяют данные, предназначенные для других узлов, либо каким-либо образом влияют на маршрутизацию сети и отсылают пакеты другим узлам.

В зависимости от расположения злонамеренного узла атаки можно также разделить на внешние и внутренние [4]. При внешних атаках злоумышленник не принадлежит самой сети и воздействует на нее извне. Подобные угрозы могут быть предотвращены запретом внешнего доступа к большинству узлов. В свою очередь, при внутренних атаках злонамерен-

ный узел сам является участником сети. Внутренние атаки наиболее опасны для сети. Кроме того, их трудно обнаружить. Именно эта группа наиболее многочисленна. Атаки на протокол маршрутизации имеют три основные цели: маршрутные сообщения, информационные пакеты и таблицы маршрутизации (или кэшируемые таблицы).

На основе атакуемого объекта, а также целей, преследуемых злумышленниками, можно охарактеризовать известные атаки протоколов маршрутизации беспроводных ad hoc сетей следующим образом.

### *Атаки на таблицы маршрутизации*

В зависимости от используемого в сети протокола это могут быть атаки *переполнения таблиц маршрутизации* (*Routing table overflow attack*) для проактивных протоколов (например, DSDV) или *порча кэшируемой таблицы маршрутизации* (*Routing cache poisoning attack*) для реактивных протоколов (таких как AODV). Эти атаки наносят ущерб доступности информации, делая невозможным создание новых маршрутов в сети, используя фабрикацию сообщений.

В ходе этих атак узел, желающий навредить, рассыпает поддельную маршрутную информацию, чтобы испортить таблицы других узлов этой сети. Поскольку при получении новых сообщений о неизвестных маршрутах узлы обновляют информацию в хранимых ими таблицах маршрутизации, большое количество ложных сообщений очень быстро приведет к переполнению таблицы маршрутизации, что, возможно, не позволит сети правильно работать, поскольку места для настоящих маршрутов уже не останется. При разовом применении это навредит работе сети на некоторое время (до тех пор, пока, следя политике работы с переполненными таблицами маршрутизации, узлы не освободят место для новых записей, удаляя наименее использующиеся или старые маршруты). Если же политика работы с переполненной таблицей такова, что узел каждый раз увеличивает место под хранящиеся маршруты за счет свободной памяти устройства, то атака может полностью парализовать работу узла.

### *Византийские атаки*

Византийскими называют атаки, получающие полный контроль над устройствами, прошедшими аутентификацию в сети. К этому типу атак относят атаки «черная дыра» (*Blackhole attack*) и ее различные модификации (*Grayhole*, *Sinkhole*), а также *стремительный натиск* (*Rushing attack*) и атаку «червоточина» (*Wormhole attack*). Их общая цель – нарушить передачу других узлов в сети вне зависимости от собственного потребления ресурсов. Византийские атаки нарушают доступность и целостность информации в сети, используя для этого фабрикацию и изменение маршрутных сообщений.

Для византийских атак достаточно характерно, что в качестве злоумышленника выступает не один узел, а несколько. Это только осложняет задачу поиска злонамеренного участника сети, поскольку все скомпрометированные узлы объединяют свои усилия, чтобы скрыть факт наличия атаки в сети.

В ходе атаки «черная дыра» зловредный узел, используя протокол маршрутизации, всегда предлагает самый короткий путь до желаемого узла, даже если на самом деле его не существует, а затем отбрасывает передаваемую через него информацию, не перенаправляя пакеты дальше, прерывая все маршруты, проходящие через него.

Для осуществления атаки «червоточина» необходимы минимум два узла, расположенных, как правило, на разных концах сети. Злоумышленники в обход общего канала (и часто даже по другой технологии) открывают собственное высокоскоростное соединение, не существующее для сети, но позволяющее им обмениваться информацией друг с другом. В случае с реактивными протоколами, когда узлы, создавая при необходимости новый маршрут, рассылают запросы по сети, злонамеренные узлы транслируют эти запросы на другой конец сети без увеличения счетчиков, влияющих на выбор маршрута. Кроме того, доставка запроса по червоточине гораздо быстрее, что также увеличивает вероятность выбора этого пути, а обеспечив прохождение большей части сообщений через собственное соединение, злоумышленники получают контроль над трафиком сети, имея возможность изменять передающуюся информацию и реализовывать другие атаки, и парализуют работу маршрутизаторов.

*Атаки с фальсификацией личности* используют добавление и изменение сообщений протокола, чтобы нарушить все три аспекта обеспечения безопасности. К этим атакам можно отнести *спуфинг* (*Spoofing attack*), в котором злоумышленник представляется другим узлом этой сети [3, 4], и «колдовскую» атаку (*Sybil attack*), где злонамеренный узел подделывает некоторое число идентификаторов и выдает себя за несколько узлов сразу. Очень часто фальсификация личности является также начальным этапом для осуществления других, более сложных атак.

Поскольку беспроводные мобильные самоорганизующиеся сети в силу своих особенностей обеспечивают простое подключение новых узлов к сети и, как правило, не имеют специального центра авторизации, реализация атак с фальсификацией личности достаточно проста. Используя поддельную личность, злоумышленник может вмешиваться в отношения между другими узлами. Например, некоторые сети используют механизм деидентификации для прекращения связи между двумя участниками соединения и посыпают для этого специальные сообщения, не требующие проверки на подлинность. Подделывая адреса узлов, злоумышленник получает возможность посыпать от их имени любые сообщения, в том числе и сообщения, разрывающие соединения между узлами. Излишне говорить, что

это нарушает маршрутизацию сети, поскольку обрыв соединения может привести к ошибкам и вынужденному поиску нового маршрута. Таким образом, многократно повторяя эту атаку от имени одного из участников соединения, злонамеренный узел может полностью изолировать какой-либо узел и препятствовать его работе в сети.

Кроме того, перехватывая сообщения идентификации, злоумышленник может украсть адреса реальных узлов сети и отправлять от их имени сообщения, заглушая сигнал реальных хозяев этих адресов (т.е. осуществляя атаку на физическом уровне), или заполнить сеть поддельным трафиком от имени других узлов, формально оставаясь при этом безучастным к происходящему.

### *Отказ в обслуживании (Denial of Service)*

Это один из самых известных типов атак, влияющий на доступность информации. Классическим примером является различного вида *флуд* (*HELLO flooding*, *RERR flooding*). Еще один из способов реализации этого типа атак – *работа «эгоистичного» узла (selfish node)*, отказывающегося перенаправлять чужие сообщения, чтобы не тратить собственные ресурсы [4].

Узлы-«эгоисты» не заинтересованы в нападении на другие узлы, они просто стараются не тратить энергию, пропускную способность сети и ресурсы процессора ради передачи чужих пакетов, однако пользуются чужими ресурсами, что отличает их от неисправных узлов сети. Очень часто эгоистичные узлы ведут себя как обычные узлы сети до тех пор, пока запас их энергии больше определенного уровня. Однако если заряд падает ниже, они сначала отказываются транслировать сообщения других узлов, а затем и не участвуют в процессах обслуживания сети.

Действия узлов-«эгоистов» приводят к опасной для ad hoc сетей изоляции узлов, что исключает возможность соединения между разными частями и делает работу сети невозможной.

В настоящее время существует множество методик обнаружения и предотвращения атак, основанных на модификациях существующих протоколов маршрутизации, но каждая направлена на защиту от одной из групп, так что создание протокола, позволяющего обезопасить сеть от нескольких типов атак, и при этом способного изменяться под требования технологии сети – по-прежнему объект дальнейших исследований.

### **Список используемых источников**

1. Security issues in routing protocols in MANETs at network layer / P. Joshi // Procedia Computer Science. – 2011. – № 3 – P. 954–960.
2. Routing Attacks in Mobile Ad hoc Networks / P. Narendra Reddy, CH. Vishnuvardhan, V. Ramesh // IJCSMC. – May 2013. – Vol. 2. Issue. 5. – P. 360–367.

3. **Intrusion Detection in Wireless Ad-Hoc Networks** / Edited by N. Chaki, R. Chaki. – CRC Press, 2010. – 258 p.

4. **A Literature Review of Security Attack in Mobile Ad hoc Networks** / Priyanka Goyal, Sahil Batra, Ajit Singh // International Journal of Computer Applications. (0975 – 8887). 2010. – Vol. 9, № 12.

**УДК 004.725.4**

**К. Э. Есалов (ассистент кафедры ИКС СПбГУТ)**  
**Е. В. Золотарев (студент группы ИКТК-19 СПбГУТ)**

## **АНАЛИЗ ИСПОЛЬЗОВАНИЯ ПРИ *DPI* СИГНАТУР ПОТОКОВ ПАКЕТОВ СЕРВИСОВ ПЕРЕДАЧИ СООБЩЕНИЙ**

Deep Packet Inspection (*DPI*, глубокий анализ пакетов) – технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому. Данная технология проводит анализ на верхних уровнях модели взаимодействия открытых систем (*OSI*), а не только по стандартным номерам портов. Помимо изучения пакетов по стандартным шаблонам будь то srcIP:port-dstIP:port, частота открытия новых сессий, и др. система *DPI* проводит так называемый эвристический (поведенческий) анализ трафика, что позволяет детектировать приложения не использующие заранее известные заголовки и структуры данных.

Технология *DPI* может быть реализована по-разному: программно, как отдельно законченное функциональное устройство (*standalone* решения) и как интегрированные в маршрутизаторы решения *DPI*. К программным относят OpenDPI, Hippie (*Hi-Performance Protocol Identification Engine*), L7-filter, SPID (*Statistical Protocol IDentification*), pfSense и IPP2P, последний больше не поддерживается. Из производителей программно-аппаратных комплексов стоит отметить Cisco (*Cisco SCE 8000 Series Service Control Engine*), Huawei (*SIG9800-X Series*), Sandvine (*PTS; Policy Traffic Switch*), Протей (Центр наблюдения СОРМ-2) и др. Интегрированные решения являются достаточно компромиссными и зачастую не могут предоставить весь спектр услуг *standalone* продуктов.

Системы *DPI* имеют несколько разных областей применения.

Во-первых, этими устройствами интересуются операторы связи. Ставятся они на границе сети за пограничными маршрутизаторами, что позволяет мониторить и анализировать весь входящий и исходящий трафик в сети оператора (если оператор хочет контролировать не только внешние каналы, но и внутренние, системы могут спускаться ближе к пользователю). Раньше QoS осуществлялся на основе служебных полей в заголовках

различных протоколов: Class of Service (*CoS*) для MPLS, Priority для IEEE 802.1Q (*VLAN*), Type of Service (*ToS*) для IPv4, Class of Traffic (*CoT*) для IPv6. Это позволяло трафику типа Best Effort (негарантированная доставка) оставаться без контроля, что давало возможность тому же BitTorrent забирать себе всю свободную полосу, что приводило к деградации других приложений. С появлением DPI у оператора появляется возможность распределения канала между различными приложениями и тут все ограничивается только его фантазией. Например, можно ограничивать трафик BitTorrent днем, а ночью предоставлять большую полосу. Можно блокировать или ограничивать Skype-трафик и любые виды SIP-телефонии, с последующей деградацией качества сервиса, предоставляемого приложением, чтобы вынудить клиента платить либо за услуги традиционной телефонии, либо за пакет услуг, разрешающий доступ к VoIP сервисам. Все это нужно для контроля за бесконечным расширением каналов, ведь экономически целесообразней купить систему DPI и контролировать их утилизацию. Так же на основании глубокого анализа пакетов оператор может осуществлять целевой маркетинг (реклама, основанная на поведении пользователя в сети).

Во-вторых, эти устройства находят себе применение в крупных компаниях, в качестве одной из компонент DLP-систем (*Data Lost Prevention*, защита от утечек), с целью защиты секретной информации от инсайдерских атак. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

В-третьих, DPI успешно используется в различных спецслужбах в СОРМ (система оперативно-розыскных мероприятий). СОРМ обеспечивается полный доступ ко всей передаваемой информации в сети связи оператора. Дополнительно обеспечивается передача на пункт управления СОРМ информации о выделенных абоненту IP-адресах до реализации преобразования (NAT), местоположении оконечного оборудования [1].

Детектирование трафика того или иного приложения основывается на сигнатурах. Под сигнатурами понимают последовательность байтов при статистическом анализе, и некоторую модель поведения, характерную только для данного приложения, при эвристическом [2]. Их разработка трудоемкий и кропотливый процесс, который не поддается автоматизации, а частота их обновлений является важным критерием для заказчика системы DPI. Разные вендоры делают это по-разному: кто-то раз в неделю, кто-то раз в месяц. Если же требуется критическое обновление, то оно вполне может выйти раньше календарного срока.

Было рассмотрено несколько мультимедийных сервисов: Viber, LINE, SIPnet, Facebook Messenger, Whatsapp и Telegram (табл. 1–2).

ТАБЛИЦА 1. Сервисы и предоставляемые услуги

	SMS	Voice	Video	Data
Viber	✓	✓	✓	✓
LINE	✓	✓	✓	✓
SIPnet	✓	✓	✓	✓
Facebook Messenger	✓	✓	✗	✓
Whatsapp	✓	✗	✗	✓
Telegram	✓	✗	✗	✓

Первые 4 приложения можно отнести к технологии OTT (*Over The Top*). Данная технология подразумевает доставку видео- и аудиоконтента к пользователю без прямого контакта с оператором связи, т. е. без гарантированного QoS.

ТАБЛИЦА 2. Сервисы и используемые протоколы

	TCP	HTTP	TLSv1	SSL	STUN	UDP	DNS
Viber	✓	✓	✓	✗	✗	✓	✓
LINE	✓	✓	✓	✗	✗	✓	✓
SIPnet	✓	✓	✓	✗	✓	✓	✓
Facebook Messenger	✓	✓	✗	✗	✓	✓	✓
Whatsapp	✓	✗	✓	✗	✗	✗	✓
Telegram	✓	✗	✓	✓	✗	✗	✓

Стоит отметить тот факт, что Viber и LINE обходят NAT (*Network Address Translation*, механизм преобразования IP-адресов транзитных пакетов; используется для преобразования локального адреса во внешний с привязкой к порту), не используя для этого протокол STUN (используется для определения своего внешнего IP-адреса и порта, путем обращения к серверу STUN), в отличие от SIPnet и Facebook Messenger. Представляет интерес и то, что если клиенты находятся в одной сети, то общение происходит в рамках этой же сети, не привлекая сервера приложения. Это справедливо для Viber и Facebook Messenger.

Особенности использования протокола UDP (выявленные сигнатуры):

Блок данных имеет похожую структуру для всех четырех сервисов, предоставляющих услуги телефонии; общий вид:

<*Constant Bytes*> <*Counter's Bytes*> <*Payload*>.

Голосовой вызов:

1. Viber:

*XX XX 80 6b 00 <Counter's Byte> <Payload>*, где *XX XX* выбираются произвольно для каждого вызова, но остаются неизменными в ходе всего разговора. Счетчик стартует со значения 01.

2. LINE:

*b6 0b 00 XX 80 78 <Counter's 2 Bytes> <Payload>*, где *XX* выбирается произвольно для каждого пакета. Счетчик стартует с произвольного значения.

3. SIPnet:

*80 78 <Counter's 3 Bytes> <Counter's 2 Bytes> <Payload>*. Счетчики стартуют с нулевых значений всех байтов.

4. Facebook Messenger:

*80 67 <Counter's 2 Bytes> <Payload>*. Счетчик стартует с произвольного значения.

Видеовызов:

1. Viber:

*XX XX 80 60 <Counter's 2 Bytes> <Payload>*, где *XX XX* выбираются произвольно для каждого вызова, но остаются неизменными в ходе всего разговора. Счетчик стартует со значения 01.

2. LINE:

*b6 0c 05 6e 80 67 <Counter's 2 Bytes> <Payload>*. Счетчик стартует с произвольного значения.

3. SIPnet:

*80 23 <Counter's 2 Bytes> <Payload>*. Счетчик стартует с нулевых значений всех байтов.

Счетчики увеличивают свое значение на 1 с каждым пакетом. Счетчики в пакетах на сервер и в пакетах с сервера не совпадают.

Особенности использования протокола TLSv1 (выявленные сигнатуры).

Данный протокол используется для обеспечения безопасности (шифрования) транспортного уровня. Отличительными чертами являются выбранный сервером метод шифрования (серверы разных приложений делают разные выбор) и последовательность в сертификате (обычный ASCII-код), передающемся в ходе хэндшейка:

1. Viber:

Протокол используется только в ходе общения с сервером обновлений. Сертификат содержит: *update.viber.com*. Метод шифрования: *TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA*.

2. LINE:

Последовательность в сертификате зависит от того, к кому серверу обращается приложение. Может быть: *\*.line.naver.jp* или *\*.line-apps.com*. Метод шифрования: *TLS\_RSA\_WITH\_RC4\_128\_MD5*.

3. SIPnet:

Сертификат содержит: *\*.sipnet.ru*. Метод шифрования зависит от того, к какому серверу обращается приложение. Может быть: *TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA* или *TLS\_RSA\_WITH\_RC4\_128\_SHA*.

4. Facebook Messenger:

Поскольку FB использует в качестве платформы доставки контента *Akamai Technologies*, сертификаты разнятся. Для серверов *Akamai* сертификат содержит: *a248.e.akamai.net*. Для всех остальных серверов последовательность: *\*.facebook.com*. Метод шифрования один и тот же: *TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA*.

5. Whatsapp:

Сертификат содержит: *\*.whatsapp.net*. Методы шифрования разные: *TLS\_RSA\_WITH\_RC4\_128\_SHA* (*v.whatsapp.net*), *TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA* (сервера обмена сообщениями), *TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA* (сервера обмена контентом).

6. Telegram:

Протокол используется при общении с серверами Google (что само по себе интересно). Последовательность в сертификате: *\*.google.com*. Метод шифрования: *TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA*. Стоит отметить, что для передачи сигнальной информации и текста Telegram использует протокол SSL.

В перспективе ожидается сборка лабораторного стенда ([рисунок](#)) с использованием программного маршрутизатора и OpenDPI поверх него. В OpenDPI будут включены полученные сигнатуры ранее озвученных сервисов, разработаны алгоритмы взаимодействия с маршрутизатором для управления потоками трафика. Для реализации сей задачи максимально близкой к реальности, трафик представленных приложений будет агрегирован с потоками других данных. С помощью этого можно будет попробовать себя в роли оператора связи.

### Список используемых источников

1. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 27.05.2010 № 73 «Об утверждении Требований к сетям электросвязи для проведения оперативно – розыскных мероприятий. Часть II. Требования к сетям передачи данных» [Электронный ресурс]. – 2010. – С. 1–2. – Режим доступа: [http://minsvyaz.ru/ru/doc/?id\\_4=206](http://minsvyaz.ru/ru/doc/?id_4=206) (Дата обращения 04.04.2014).

2. Новые решения СОРМ для Skype [Электронный ресурс] / Б. С. Гольдштейн, В. С. Елагин // Вестник связи. – 2010. – № 9. – С. 36–40 – Режим доступа: <http://niits.ru/public/2010/2010-018-pp.pdf> (Дата обращения 06.04.2014).

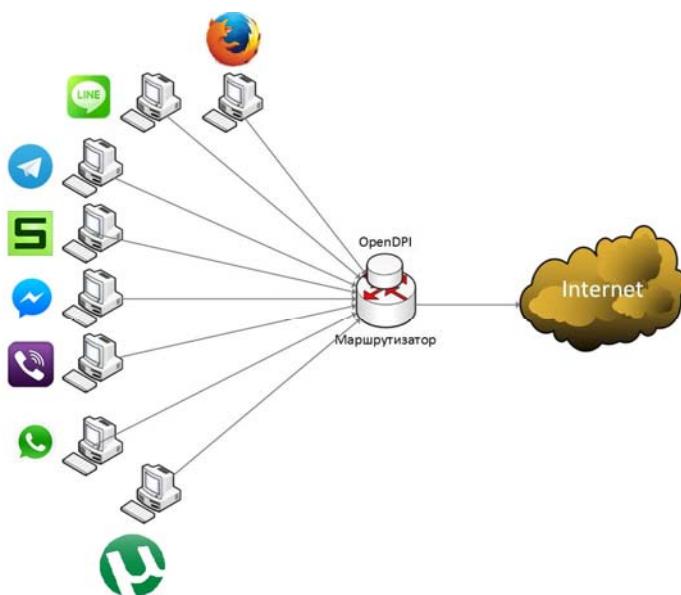


Рисунок. Схема лабораторного стенда

*Статья представлена заведующим кафедрой «Инфокоммуникационные системы», д-ром техн. наук, профессором Б. С. Гольдштейном.*

**УДК 004.942**

**Е. В. Ефимова (студентка группы СК-91 СПбГУТ)**  
**И. А. Небаев (ассистент кафедры ОПДС СПбГУТ)**

## **РЕАЛИЗАЦИЯ АЛГОРИТМОВ ОБРАБОТКИ ИНФОРМАЦИИ И ИМИТАЦИОННОЙ МОДЕЛИ КАНАЛА ПЕРЕДАЧИ ДАННЫХ ДЛЯ БЕСПРОВОДНЫХ СЕТЕЙ СТАНДАРТА 802.11**

Технология Wi-Fi впервые представлена в 1991 году (*NCR Corporation/AT&T*), и первоначально рассматривалась как способ беспроводного объединения портативных миникомпьютеров и БД логистического назначения [1]. Однако со временем области внедрения Wi-Fi приобрели более широкий, массовый характер, и в первую очередь в качестве средства обеспечения радиопередачи данных между портативными компьютерными устройствами общего назначения. Номенклатура устройств Wi-Fi радиосвязи и гибкая архитектура топологии позволяют реализовывать беспроводные сети различного масштаба и возможностей. Наиболее распространенные на данный момент беспроводные сети передачи данных, основанные на стандартах IEEE 802.11 (Wi-Fi), представлены в таблице [2].

ТАБЛИЦА. Беспроводные сети передачи данных стандарта 802.11(Wi-Fi)

Документ	Дата принятия	Частотный диапазон, ГГц	Ширина полосы частот канала, МГц	Скорость передачи данных, Мбит/с
802.11a	1999	5	20	54
802.11ac	2013	5	40/80/160	6930
802.11ad	2012	60	2160	6760
802.11b	1999	2,4	20	11
802.11g	2003	2,4	20	54
802.11n	2009	2,4/5	20/40	600

Используя техническую документацию, представленную в стандартах IEEE 802.11 [3–5] в рамках данной работы произведен подбор общих алгоритмов и методов обработки информации, применяемых в беспроводных сетях 802.11 (*a, b, g, n*). Представленная реализация имитационной модели в основном базируется на рекомендациях стандарта 802.11 *b*. Однако разработанная модель может быть расширена для поддержки практически полного спектра стандартов 802.11.

Реализованная модель предназначена для статистических испытаний по методу Монте-Карло. Программная часть модели выполнена в среде визуального программирования MATLAB Simulink (8.1). В схеме модели (рис. 1) реализованы блоки:

- генерации информационной последовательности (1);
- сверточного кодирования (2) и декодирования (14);
- матричного перемежения (3) и деперемежения (13);
- блоки расширения (4) и сужения (12) спектра;
- блоки модуляции (5) и демодуляции (11);
- квазистатический канала с замираниями (6) и АБГШ (7);
- блоки цифровой осциллографии (8,9,10);
- блок отбрасывания обнуляющих бит (15);
- блок подсчета битовых ошибок и вывода на экран (16).

В имитационной модели реализованы некоторые общие методы обработки и передачи информации характерные для набора стандартов 802.11 [6]:

- помехоустойчивое сверточное кодирование кодом  $[155,137]_8$  ( $R = 1/2, K = 7, m = 6, S = 64$ );
- матричное перемежение;
- расширение спектра методом прямой последовательности (DSSS);

- квадратурная фазовая модуляция (QPSK).

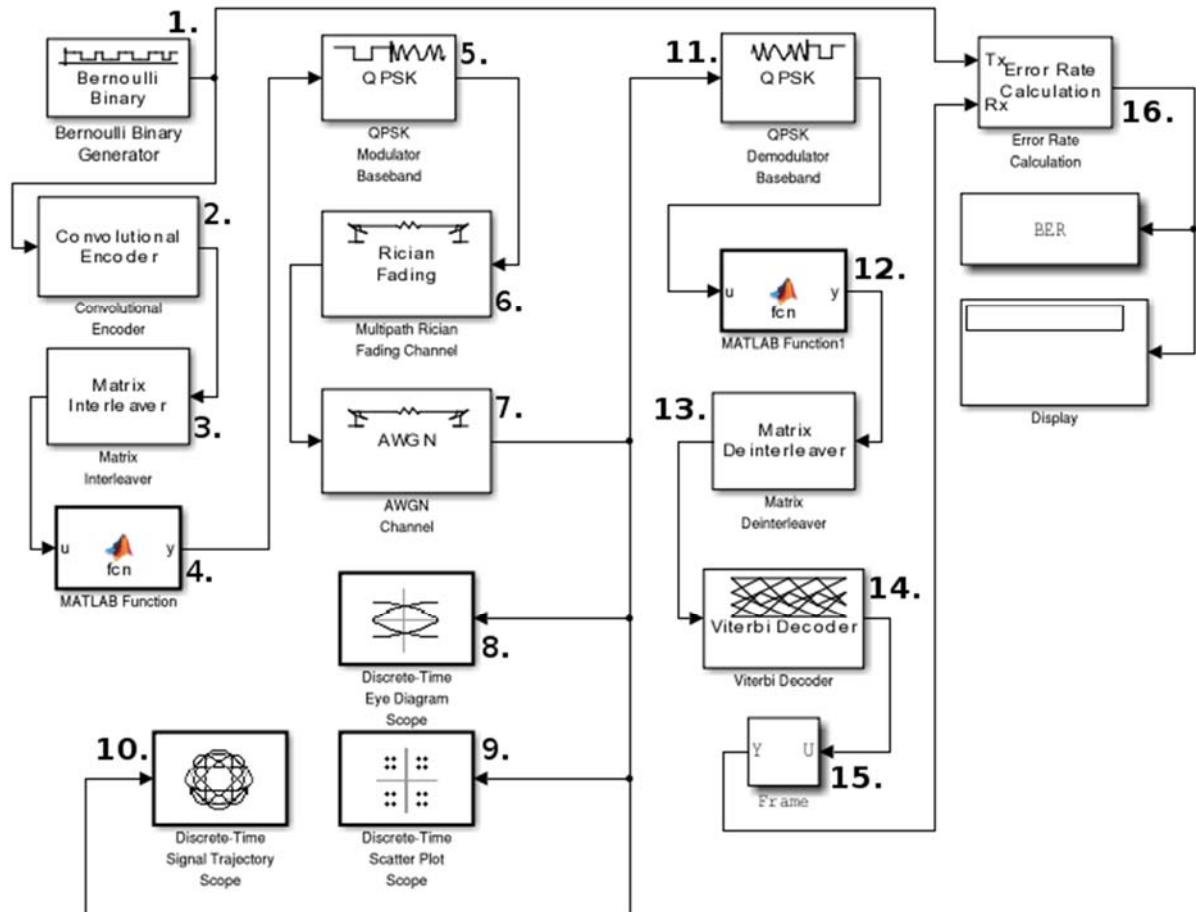


Рис. 1. Схема имитационной модели в среде Simulink

Рассмотрим подробнее процесс обработки информации сверточным кодером и параметры модели канала. Кодер сверточного кода [155,137]<sub>8</sub> функционирует в режиме терминирования кодовой решетки. По завершении кодирования к кодовой последовательности добавляется 6 «хвостовых» бит, обнуляющих кодер и переводящих его в состояние  $S_0$ . Таким образом, можно вычислить общую длину кодового сообщения при усредненной длине информационного кадра (2313 бит):

$$\frac{n(L+m)}{k} = \frac{2(2312+6)}{1} = 4636, \quad (1)$$

где  $n$  – число кодовых выходов кодера,  $k$  – число информационных входов,  $L$  – длина исходного сообщения,  $m$  – память кодера. Схема сверточного кодера [155,137]<sub>8</sub> изображена на [рисунке 2](#). Сверточный кодер памяти шесть ( $m = 6$ ) хранит 6 информационных бит, загруженных за предыдущие такты работы схемы. Выходные биты, формируемые в сверточном кодере, определяются операцией сложения по  $mod2$ , между значениями входного бита  $X_i$  и битами, хранящими в запоминающих ячейках  $M_i$ , подключенных к соответствующему сумматору. Таким образом, значение каждого форми-

руемого выходного бита ( $G_i^{(0)}$ ,  $G_i^{(1)}$ ) зависит не только от входящего информационного бита, но и от  $m$ -предыдущих бит.

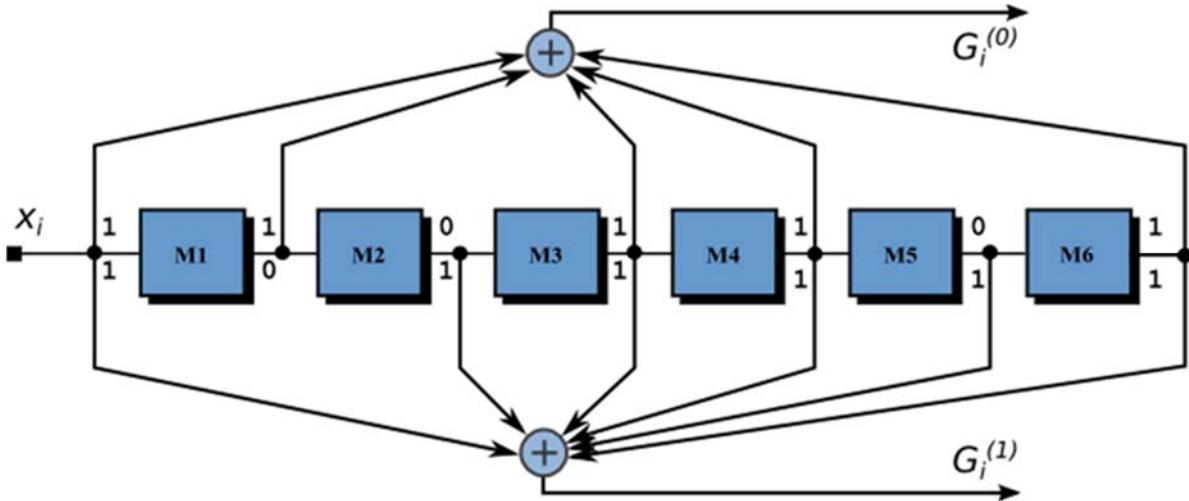


Рис. 2. Кодер сверточного кода  $G=[155,137]_8$

В разработанной имитационной модели используется квазистатичный [6] беспроводной канал с замираниями и ошибками по распределению Райса, характеризующийся следующими параметрами:

- коэффициент Райса  $K_R = 1 \dots 10$ ;
- частота несущего колебания  $f_c = 2,4$  ГГц;
- скорость движения объекта  $v = 1$  м/с;
- скорость передачи данных  $R_B = 1 \dots 10$  Мбит/с.

Для реализованного квазистатичного канала характерно достаточно большое время когерентности:

$$\tau = \frac{1}{100f_d}, \quad (2)$$

где  $f_d$  – частота доплеровского смещения. Частота смещения, при учете параметров модели указанных выше, может быть вычислена следующим образом:

$$f_d = \frac{vf_c}{c} = \frac{1 \cdot 2,4 \cdot 10^9}{3 \cdot 10^8} = 8, \quad (3)$$

где  $v$  – скорость движения портативного объекта (точка доступа стационарна),  $f_c$  – частота несущего колебания,  $c$  – скорость света.

Используя представленные выражения можно рассчитать количество информации  $B_i$ , передаваемой за время, в течение которого канал обладает инвариантностью параметров. Учитывая выражение (2) и (3) для  $R_b = 10$  Мбит/с получим в бит:

$$B_i = \left(\frac{1}{100f_d}\right) \cdot R_b = \left(\frac{c}{100vf_c}\right) \cdot R_b = 12500. \quad (4)$$

На последующих рисунках, полученных с помощью блоков цифровой осциллографии, демонстрируется эффект воздействия канала на информацию закодированную сверточным кодом и предаваемую с помощью сигналов QPSK. На рисунке 3 под литерой (А) изображено исходное сигнальное созвездие QPSK созданное модулятором передатчика.

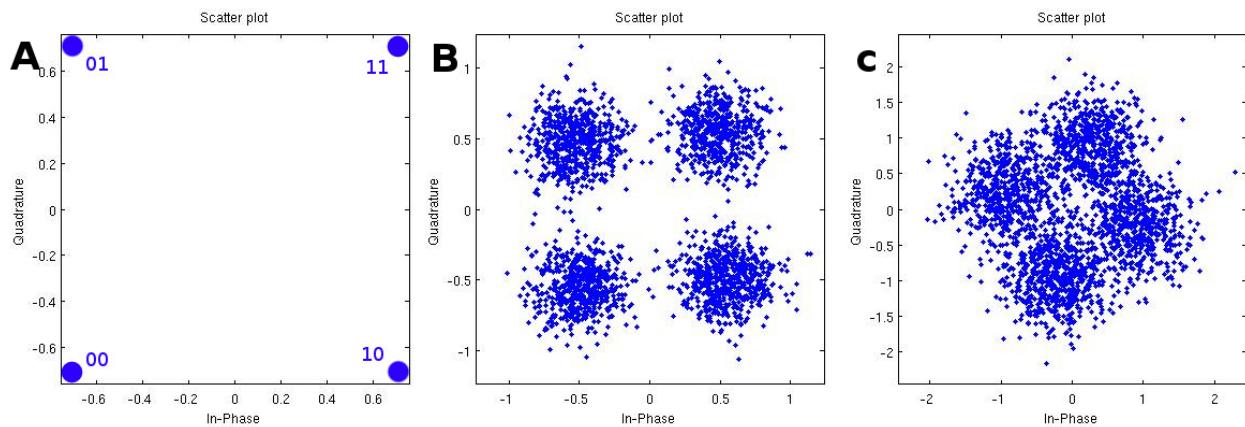


Рис. 3. Графики рассеяния сигнального созвездия QPSK

Под литерами (В) и (С) представлено рассеяние сигнального созвездия QPSK принятого сигнала после передачи по каналу с замираниями и АБГШ при соотношении  $E_b/N_0 = 10$  дБ и  $K_R = 5$  и соотношении  $E_b/N_0 = 5$  дБ и  $K_R = 3$ . Рисунок 4 демонстрирует флюктуацию соотношения С/Ш ( $E_b/N_0$ ) в имитируемом канале при  $K_R = 3$  (D) и  $K_R = 5$  (E), соответственно.

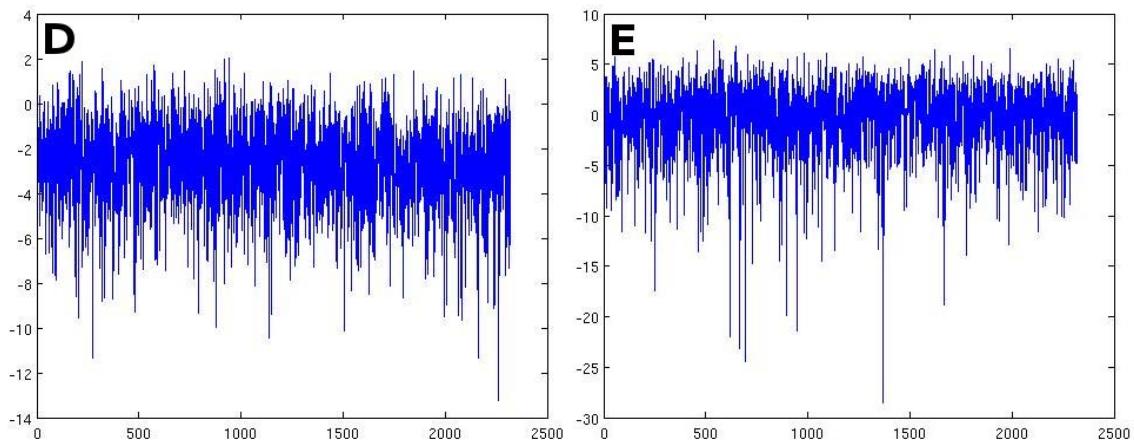


Рис. 4. Изменение соотношения  $E_b/N_0$  в канале

Как уже было отмечено ранее, беспроводные сети передачи данных, построенные по стандартам 802.11, имеют широкое распространение и достаточно глубоко внедрены в процесс деятельности техники и человека. Не смотря на достаточно длительный срок разработки и совершенствования технологий беспроводной передачи данных, до сих пор существует ряд

важных задач, таких как увеличение помехоустойчивости информации, расширение пропускной способности каналов, повышение спектральной эффективности сигналов и т. д. Для решения данных задач применяются различные методы компьютерного имитационного моделирования, позволяющие выявить важные свойства новых и устоявшихся технологий, провести анализ результатов реализации различных алгоритмов обработки информации и оценить эффективность их применения [7].

Имитационная модель системы беспроводной передачи, представленная в данной работе, реализует часть важных алгоритмов, характерных для всего набора стандартов 802.11. В связи с этим, представленная модель беспроводного канала может быть использована в работах, посвященных указанным направлениям исследований, а при необходимости, достаточно просто расширена и усложнена. В заключении следует отметить, что исходные тексты программной реализации модели для среды MATLAB доступны для загрузки по электронному адресу – <ftp://ftp.radiocoder.net>.

### Список используемых источников

1. **Основы** построения беспроводных локальных сетей стандарта 802.11/ П. Рошан, Дж. Лиери: пер. с англ. – М. : Издательский дом «Вильямс», 2004. – 304 с. – ISBN 5-8459-0701-2 (рус).
2. **Беспроводные** сети Wi-Fi : учебное пособие / А. В. Пролетарский и др. – М. : Интернет-Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2013. – 215 с. – ISBN 978-5-9474-737-9.
3. **Стандарт** 802.11-2007 – IEEE Standard for Information Technology [Электронный ресурс]. – 2007. – Режим доступа: <http://www.ieee802.org/11/> (Дата обращения 16.05.2014).
4. **Стандарт** IEEE SA – 802.11af-2013 – IEEE Standard for Information technology [Электронный ресурс]. – 2013. – Режим доступа: <http://www.ieee802.org/11/> (Дата обращения 16.05.2014).
5. **Стандарт** IEEE Std 802.11-1997 specifies a single Medium Access Control (MAC) sub layer and 3 Physical Layer Specifications [Электронный ресурс]. – 1997. – Режим доступа: <http://www.ieee802.org/11/> (Дата обращения 16.05.2014).
6. **Новые** алгоритмы формирования и обработки сигналов в системах подвижной связи/ А. М. Шлома, М. Г. Бакулин; под редакцией профессора А. М. Шломы. – М. : Горячая линия – Телеком, 2008. – 344 с. – ISBN 978-5-9912-0061-5.
7. **Компьютерное** моделирование системы кодирования параллельным сверточным турбокодом для повышения уровня достоверности передачи данных в непрерывном канале/ И. А. Небаев // Вестник компьютерных и информационных технологий. – 2013. – № 8. – С. 41–45.

УДК 621.397

**Ю. С. Ефремова (студентка группы СК-01 ПГУТИ)**

## **МЕТОДИКА ВЫБОРА ЭФФЕКТИВНОЙ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ ДЛЯ ИДЕНТИФИКАЦИИ ЛИЦА**

Согласно рекомендации МВД РФ Р 78.36.008-99. – 1999 г. различаются следующие целевые задачи видеоконтроля: обнаружение, различение и идентификация. Для нас интересно записать высококачественное изображение лица, которое может быть использовано для доказательства идентичности<sup>1</sup>.

Процесс распознавания лиц обычно состоит из двух этапов: поиск области лица на изображении, и сравнение найденного лица с лицами, находящимися в базе данных. В настоящее время метод Виолы-Джонса является самым популярным методом для распознавания лиц в режиме реального времени. Он разработан и представлен в 2001 году Полом Виолой и Майклом Джонсом.

Детектор лица Виолы-Джонса основан на основных идеях:

- интегральное представление изображения;
- признаки Хаара;
- бустинг;
- каскады признаков.

Интегральное представление изображения позволяет вычислить быстро необходимые объекты, рассчитывать суммарную яркость произвольного прямоугольника на данном изображении, причем какой бы прямоугольник не был, время расчета неизменно. Интегральное представление изображения – это матрица, совпадающая по размерам с исходным изображением. В каждом элементе ее хранится сумма интенсивностей всех пикселей, находящихся левее и выше данного элемента. Элементы матрицы рассчитываются по следующей формуле:

$$L(x, y) = \sum_{i=0, j=0}^{i \leq x, j \leq y} I(i, j),$$

где  $I(i, j)$  – яркость пикселя исходного изображения.

Каждый элемент матрицы  $L[x, y]$  представляет собой сумму пикселей в прямоугольнике от  $(0, 0)$  до  $(x, y)$ , т. е. значение каждого пикселя  $(x, y)$  равно сумме значений всех пикселей левее и выше данного пикселя  $(x, y)$ . Расчет матрицы занимает линейное время, пропорциональное числу пик-

---

<sup>1</sup> Проектирование и монтаж систем охранного телевидения и домофонов / Рекомендация МВД РФ Р 78.36.008-99. – 1999.

селей в изображении, поэтому интегральное изображение просчитывается за один проход. Расчет матрицы возможен по формуле (1):

$$L(x,y) = I(x,y) - L(x-1,y-1) + L(x,y-1) + L(x-1,y). \quad (1)$$

Пусть на рисунке 1 в прямоугольнике  $ABCD$  есть интересующий нас объект  $D$ :

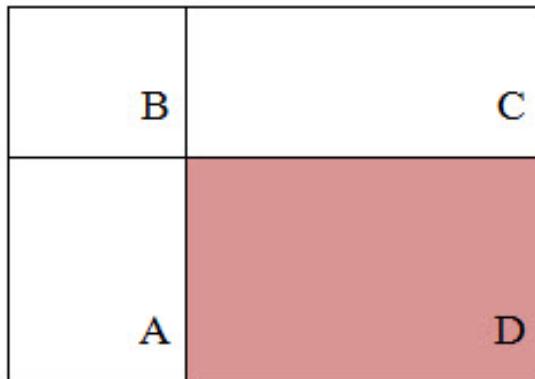


Рис. 1. Интересующий объект  $D$

Из рисунка 1 понятно, что сумму внутри прямоугольника можно выразить через суммы и разности смежных прямоугольников по следующей формуле (2):

$$S(ABCD) = L(A) + L(C) - L(B) - L(D). \quad (2)$$

С помощью признаков Хаара происходит поиск нужного объекта (в данном контексте, лица и его черт). В стандартном методе Виолы-Джонса используются прямоугольные признаки, изображенные на рисунке 2, они называются примитивами Хаара:

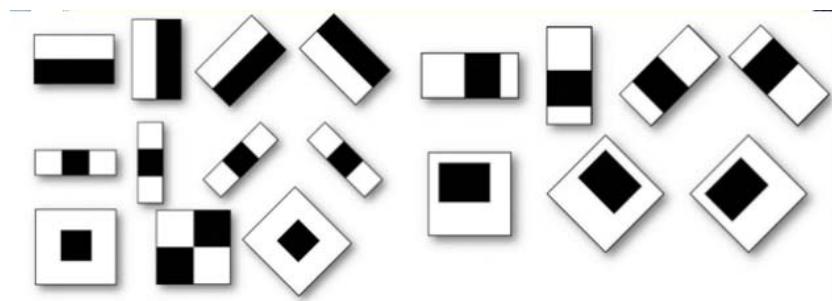


Рис. 2. Примитивы Хаара

Они представляют собой результат сравнения яркостей в двух прямоугольных областях изображения. Предположим, что задано множество объектов –  $A$  и множество допустимых ответов –  $B$ . Пусть  $g:A \rightarrow B$  – называется решающей функцией. Решающая функция  $g$  должна допускать эффективную компьютерную реализацию, по этой причине её также называют

ют алгоритмом. Признак (*feature*)  $f$  объекта  $a$  – отображение  $f:A \rightarrow Df$ , где  $Df$  – множество допустимых значений признака. В частности, любой алгоритм  $g:A \rightarrow B$  также можно рассматривать как признак. Если задан набор признаков  $f_1, \dots, f_n$ , то вектор  $x = (f_1(a), \dots, f_n(a))$  называется признаковым описанием объекта  $a \in A$ . Признаковые описания допустимо отождествлять с самими объектами. При этом множество  $A = Df_1 \times \dots \times Df_n$  называют признаковым пространством.

Вычисляемым значением такого признака будет:  $F = U - V$ , где  $U$  – сумма значений яркостей точек, закрываемых светлой частью признака, а  $V$  – сумма значений яркостей точек, закрываемых темной частью признака.

В методе Виолы-Джонса признаки Хаара организованы в каскадный классификатор. Преимущество использования признаков Хаара является наибольшая, по сравнению с остальными признаками, скорость. При использовании интегрального представления изображения, признаки Хаара могут вычисляться за постоянное время.

Построение классификатора основан на алгоритме бустинга. Бустинг (от англ. *boost* – улучшение, усиление) для выбора наиболее подходящих признаков для искомого объекта на данной части изображения. В результате работы алгоритма бустинга на каждой итерации формируется простой классификатор вида:

$$h_j(z) = \begin{cases} 1, & \text{если } p_j f_j(z) > p_j \theta_j \\ 0, & \text{иначе,} \end{cases}$$

где  $p_j$  – показывает направление знака неравенства;  $\theta_j$  – значение порога;  $f_j$  – вычисленное значение признака.

Полученный классификатор имеет минимальную ошибку по отношению к текущим значениям весов, задействованным в процедуре обучения для определения ошибки. Все признаки поступают на вход классификатора, который даёт результат «верно» либо «ложь». Используются каскады признаков (рис. 3) для быстрого обнаружения информативных областей в изображении.

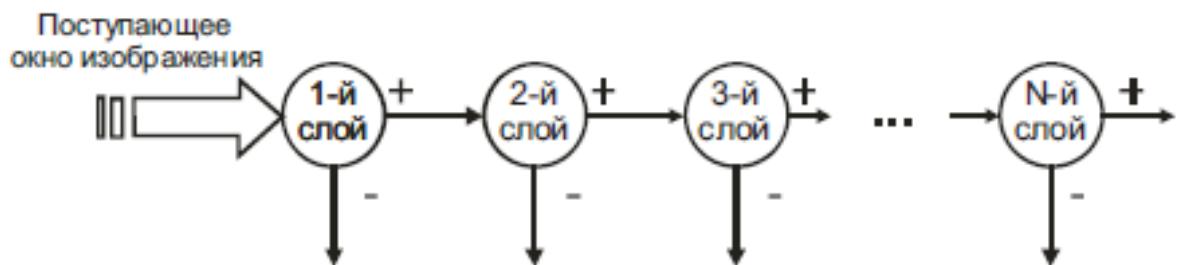


Рис. 3. Структура каскадного детектора

Решим задачу, используя пакет IP Video System Design Tool.

В пограничном контрольном пункте необходимо установить камеру. Рассмотрим, какие параметры необходимо учесть при выборе камеры и её монтаже. Подберем параметры камеры: угол обзора (фокусное расстояние объектива) или разрешение камеры, таким образом, чтобы в целевой области была возможна идентификация человека (рис. 4), при которых вся интересующая нас область была окрашена розовым цветом зоны идентификации.

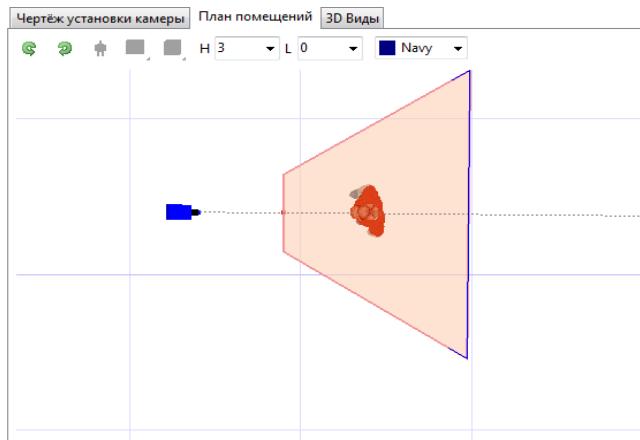


Рис. 4. Зона идентификации

#### *Высота установки камеры*

Исходя из задания нам нужно, чтобы относительная высота человека в процентах от высоты кадра была равна 120 %, для этого камеру устанавливаем на высоте  $L = 2$  м.

#### *Фокусное расстояние объектива камеры*

Для матрицы 1/3" дюйма фокусное расстояние вычислим по формуле (3):

$$f = 4,9 \times D \div H, \quad (3)$$

где  $f$  – фокусное расстояние, мм;  $D$  – максимальное расстояние до объекта, м;  $H$  – высота объекта, м.

Подставив значения в формулу (3) получаем:  
 $f = 4,9 \times 1,6 \div 1,75 = 4,5$  мм.

#### *Определение расстояния между человеком и видеокамерой*

Чтобы получить изображение, отвечающее требованиям, расстояние между человеком и видеокамерой не должно превышать значения:

$$a = f \times 70,6 \div h,$$

где  $h$  – горизонтальный размер ПЗС-матрицы.

Таким образом, при использовании видеокамеры и объектива формата 1/3" при его фокусном расстоянии, равном 4,5 мм, расстояние между видеокамерой и человеком должно быть примерно 1м.

Расчёт угла обзора объектива производиться по формуле (4):

$$\alpha = 2\arctg\left(\frac{d}{2f}\right), \quad (4)$$

где  $\alpha$  – угол обзора объектива, град.;  $d$  – размер матрицы по горизонтали и вертикали, мм.

Если соотношение сторон камеры 4:3 [мм], то:

– угол обзора видеокамеры по вертикали:

$$\alpha = 2\arctg(3/(2 \times 4,5))=43,6^\circ.$$

– угол обзора видеокамеры по горизонтали:

$$\alpha=2\arctg(4/(2 \times 4,5))=56,1^\circ.$$

*Наклон камеры представлен на рисунке 5.*

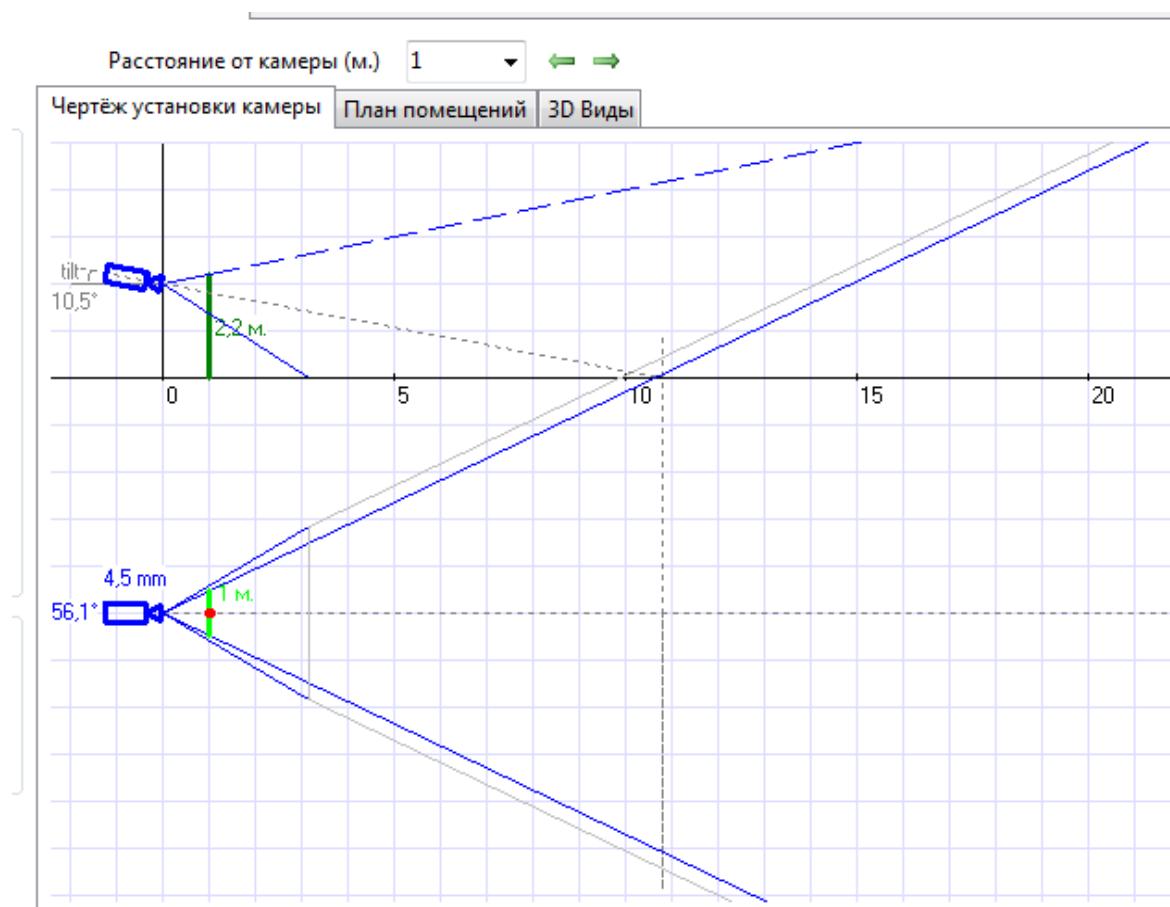


Рис. 5. Наклон камеры

$$\psi = \arcsin f/L,$$

где  $L$  – высота установки камеры, м.

Это отношение весьма мало  $\psi = \arcsin 0,45/2 = 10,5^\circ$ .

Для данного случая выбирается камера с разрешением  $1600 \times 1200$  ( $2Mp$ ), чтобы чётко видеть все детали лица.

По проделанной работе можно сделать вывод, что рассчитав необходимые параметры камеры, можно идентифицировать личность по характерным для нее признакам.

*Статья представлена научным руководителем,  
профессором А. В. Росляковым (ПГУТИ).*

**УДК 654.739**

**Д. А. Жукова (студентка группы СИС-22м СПбГУТ)**

## **ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ ОТ ОШИБОК В СОВРЕМЕННЫХ ШИРОКОПОЛОСНЫХ КАНАЛАХ РАДИОСВЯЗИ**

Сети WiMAX являются реализацией технологии широкополосного беспроводного доступа Broadband Wireless Access стандарта IEEE 802.16. Основное предназначение данных сетей – это оказание услуг абонентам по беспроводной передаче данных на расстояния в несколько десятков километров. Сети на основе WiMAX, способна предоставлять услуги не только телефонной связи, но также и высокоскоростной передачи данных (доступ в *Internet*), передачи видео, в том числе услуги мобильного телевидения. На канальном (*MAC*) уровне сети WiMAX используют Time Division Multiply Access (*TDMA*) протокол мультиплексирования каналов при множественном доступе к среде передачи данных. Высокая эффективность сетей WiMAX достигается за счет совместного применения протокола TDMA на канальном уровне и модуляции QAM на физическом уровне [1]. Схемы модуляции до QAM64 позволяют добиться высокой эффективности использования радиочастотного спектра (до 5 бит/с/Гц). Скорость передачи составляет до 37,7 Мбит/с в полосе частот 10 МГц. Тип модуляции может изменяться адаптивно от BPSK до QAM64, в зависимости от дальности абонента и условий распространения сигнала. Для повышения помехоустойчивости на физическом уровне применяется каскадное кодирование: внешним кодом Рида-Соломона и внутренним кодом БЧХ (например, блоковый циклический код Хемминга). Стандарт предусматривает опциональ-

ное применение блоковых турбокодов основанных на кодах Хемминга и контроле четности. Обязательные для поддержки в стандарте IEEE 802.16 варианты каскадного кодирования приведены в таблице [2].

ТАБЛИЦА. Обязательные схемы кодирования/модуляции в режиме OFDM

Модуляция	BPSK	QPSK	16-QAM	64-QAM
Кодер Рида-Соломона	(12,12,0)	(32,24,4); (40,36,2)	(64,48,8); (80,72,4)	(108,96,6); (120,108,6)

BPSK (*Binary Phase Shift Keying* – бинарная фазовая манипуляция).  
QPSK (*Quadrature Phase Shift Keying* – квадратурная фазовая манипуляция).  
16, 64-QAM (*Quadrature Amplitude Modulatio* – квадратурная (амплитудная) модуляция).

Достоинством каскадных кодов является то, что они позволяют заменить декодирование длинного кода декодированием нескольких значительно более коротких кодов. Каскадные коды строятся по принципу поэтапного применения двух или более процедур кодирования  $k$  – последовательности передаваемых информационных символов. При этом символами кода следующего этапа (ступени) кодирования являются слова кода предыдущей ступени. Процедура кодирования двоичным каскадным кодом представлена на [рисунке 1](#) и сводится к следующему. Последовательность двоичных символов передаваемого сообщения разбивается на  $K$   $k$ -элементных блоков. Каждый  $k$ -элементный блок рассматривается как символ нового  $k$ -ичного алфавита, например, как элемент поля  $GF(2^k)$ , и подлежит кодированию  $(N, K)$   $k$ -ичным кодом. В результате реализации процедуры кодирования  $(N, K)$ -кодом к  $K$   $k$ -элементным блокам добавляется  $N - K$  избыточных  $k$ -элементных блоков, элементов  $GF(2^k)$ . Очевидно, что эти избыточные символы имеют представление в виде  $k$ -элементных двоичных последовательностей.  $(N, K)$ -код получил название кода второй ступени или внешнего кода. Затем каждый из  $N$   $k$ -элементных символов внешнего кода кодируется двоичным  $(n, k)$ -кодом первой ступени. Код первой ступени называют также внутренним кодом, результате такого двухступенчатого кодирования получается двоичный блок длиной  $N*n$ , являющийся кодовой комбинацией каскадного кода [3].

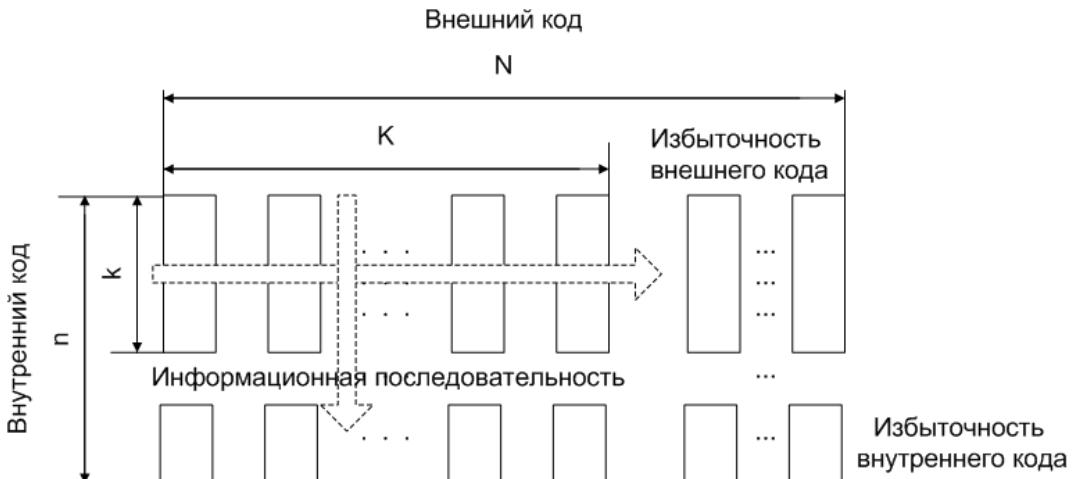


Рис. 1. Структурная схема каскадного кода

Процедура декодирования (рис. 2) начинается с декодирования внутреннего кода БЧХ. Блок данных передается по каналу и поступает во внутренний декодер. Поток данных обрабатывается внутренним декодером, а результат поступает на внешний декодер. На выходе внешнего декодера формируются блоки, поступающие к потребителю информации.

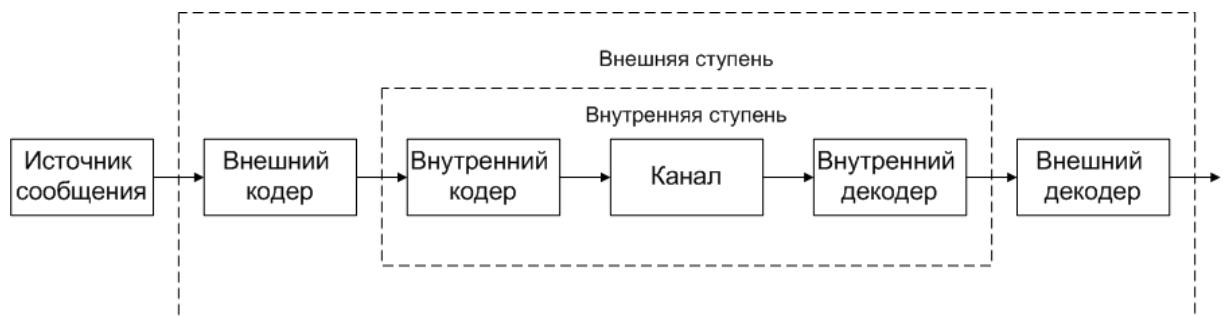


Рис. 2. Схема процедуры декодирования каскадного кода

В процессе работы были проанализированы обязательные для стандарта IEEE 802.16 параметры внутреннего и внешнего кодов и выбран для дальнейшего более подробного исследования вариант каскадного кодирования, где внешним кодом выбран РС-фыкод (32,24) с  $d_{min} = 9$  и внутренним – циклический код Хемминга. На основе стандарта IEEE 802.16 код БЧХ должен содержать 8 информационных элементов, а число избыточных кратно 8, таким образом, в качестве внутреннего выбран код Хемминга (16,8) с  $d_{min} = 4$  и возможностью исправления 1 ошибки, являющейся кодом БЧХ.

На практике декодирование внутренним кодом реализуется по схеме приведенной на рисунке 3.

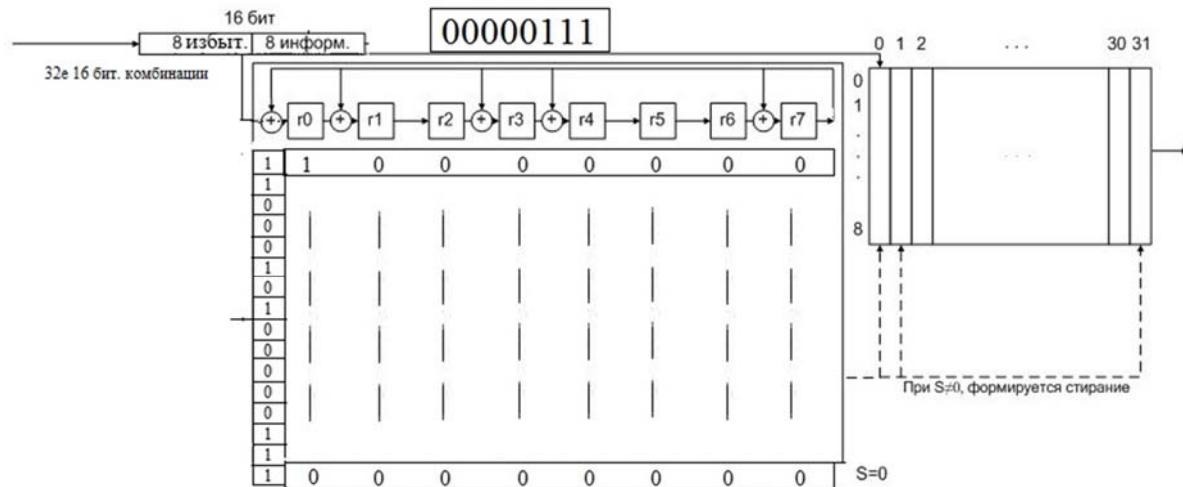


Рис. 3. Схема декодера внутреннего кода

Задача декодера внутреннего кода обнаружить искаженные блоки. Обнаружение происходит путем деления комбинации внутреннего кода на порождающий многочлен. Информационная часть кодовой комбинации записывается в массив внешнего кода. При обнаружении искаженных блоков формируется стирание и информационная часть заменяется нулевой комбинацией с соответствующей меткой. Сформированный таким образом в массиве отправляется на внешнюю ступень декодирования.

Для получения исходных данных (кодовых комбинаций для каналов со слабым и сильным группированием ошибок) были смоделированы и проанализированы различные варианты появления искаженных блоков. Моделирование проводилось с использованием программного приложения кафедры «Обработка и передача дискретных сообщений» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. После проведения испытаний и исследования вероятности появления ошибок в каналах со слабым и сильным группированием ошибок был построен следующий график (рис. 4). Из графика определяем три области: область не обнаружения ошибок, область исправления до 6 стираний и возможности исправления 1 ошибки (если она возникнет), область исправления до 8 стираний без исправления ошибок.

Определение этих областей дает возможность сделать следующие выводы:

Для канала со слабым группированием ошибок  $\alpha = 0,3$  возможно исправление до 6 стираний и 1 ошибки при  $P = 0,03$ , при  $P = 0,04$  возможно исправление до 8 стираний (элементов РС-кода).

Для канала с сильным группированием ошибок  $\alpha = 0,7$  возможно исправление до 6 стираний и 1 ошибки при  $P = 0,09$ , при  $P = 0,1$  возможно исправление до 7 стираний (элементов РС-кода).

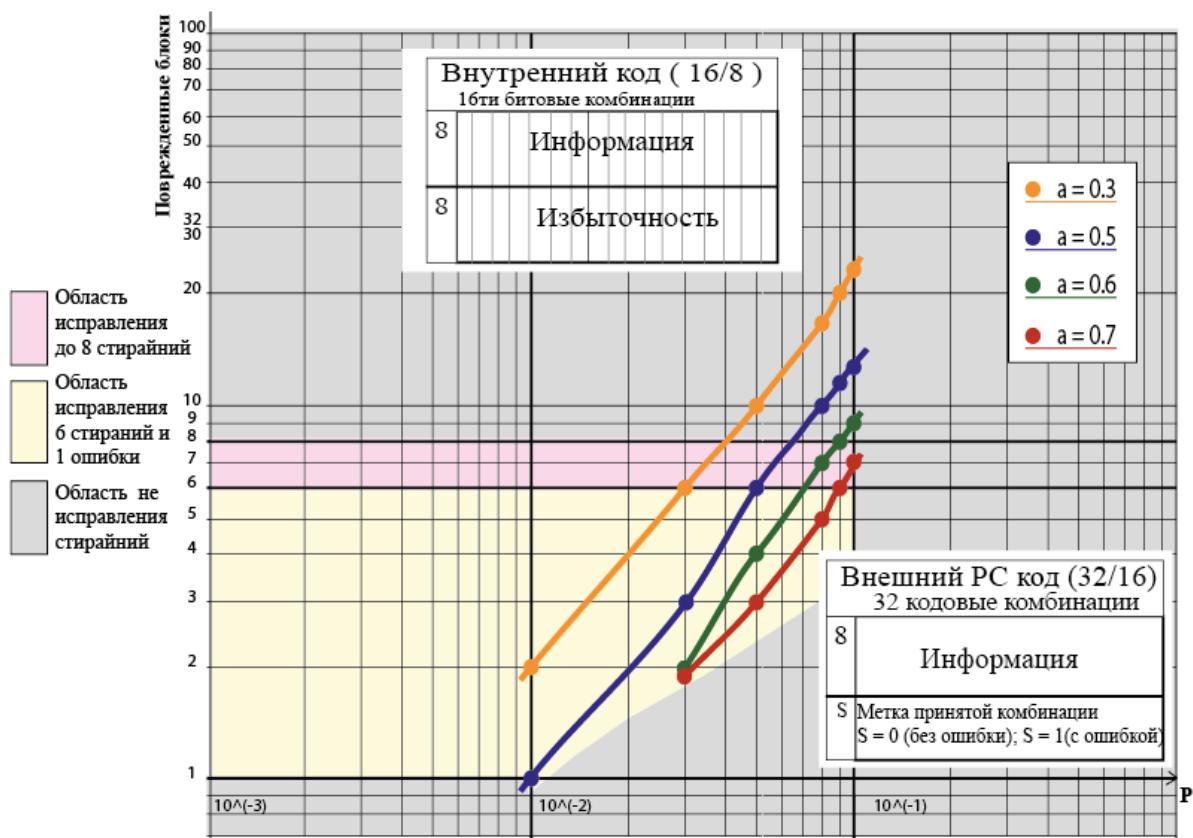


Рис. 4. Зависимость появления искаженных блоков в каналах со слабым и сильным группированием ошибок

### Выходы

- 1) Каскадные коды более эффективны в каналах с сильным группированием ошибок, чем в каналах со слабым группированием.
  - 2) Исправление большего числа стирианий при слабом группировании ошибок в канале требуют большей избыточности кода Рида-Соломона.
  - 3) Рекомендации по совершенствованию внутреннего кода:
    - а) Возможно применение методов итеративного декодирования на основе мягких решений на внутренней ступени для исправления ошибок с целью уменьшения числа стирианий в канале со слабым группированием.
    - б) Применение решающей обратной связи на внутренней ступени исправления ошибок с целью получения данных с меньшим количеством искажений.
- Реализация рекомендаций для внутреннего кода может привести к большим временным задержкам. Целесообразно проверить возможность применения решающей обратной связи для исправления ошибок во внутреннем коде. Необходим дополнительный анализ методов итеративного декодирования и методов исправления ошибок с применением решающей

обратной связи с целью определения метода с наименьшей временной задержкой.

#### **Список используемых источников**

1. **Технология** фиксированного широкополосного беспроводного доступа Wi-MAX стандарта IEEE 802.16-2004 [Электронный ресурс] / В. Г. Васильев // ЮНИДАТА – 2009. – С. 91. Режим доступа: file:///C:/Users/dzhukova/Desktop/%D1%8F/Wi-MAX\_technology.pdf (Дата обращения 17.04.2014).
2. **Современные** технологии беспроводной связи / И. В. Шахнович // М. : Техносфера, 2006. – 288 с. – ISBN 5-94836-070-9.
3. **Построение** каскадных кодов на основе кодов Рида-Соломона и Боуз-Чоудхури-Хоквингема / В. М. Охорзин, Д. С. Кукунин, М. С. Новодворский. – СПб. : СПбГУТ им. проф. М. А. Бонч-Бруевича, 2004. – С. 62.

*Статья представлена научным руководителем канд. техн. наук, профессором В. М. Охорзином.*

**УДК 004.942**

**А. А. Исаков (аспирант кафедры РВКС СПбГПУ)**

## **ПРОЕКТ *OPENMVL*. КОМПОНЕНТНЫЕ МОДЕЛИ И РЕШЕНИЕ БОЛЬШИХ РАЗРЕЖЕННЫХ СИСТЕМ**

### *Введение*

Работа над проектом OpenMVL ведется на кафедре «Распределенные вычисления и компьютерные сети» Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный политехнический университет» с 2009 года. Цель проекта – создание общедоступной, открытой на уровне программных кодов, среды моделирования сложных динамических систем OpenMVLShell.

В проекте OpenMVL сделана попытка выделить ключевые проблемы, возникающие при построении визуальных сред моделирования, и предлагаемые методы их решения. Открытые программные реализации отобранных методов, используемые в среде моделирования (*OpenMVLShell*), становятся доступными не только разработчикам подобного программного обеспечения, но и любому желающему познакомиться с основами объектно-ориентированного моделирования.

Современные среды визуального моделирования – это сложные комплексные программы, использующиеся годами и требующиеся постоянной модификации и совершенствования. Проводить эксперименты и сравни-

вать различные предлагаемые усовершенствования в таких сложно устроенных профессиональных комплексах часто оказывается трудным даже для разработчиков этих комплексов. Более того, из-за закрытости кодов, практически невозможно познакомиться с работами коллег, даже если речь идет о математических проблемах. По этой причине в проекте OpenMVL ставится задача объединить усилия исследователей при решении общих проблем моделирования, создав открытый и доступный всем набор «кубиков», из которых можно «собирать» среду моделирования, и модифицировать только свой собственный блок, оценивая влияние новых решений на свойства всей среды.

Создаваемая среда уже используется и как исследовательский инструмент при решении научных и технических проблем, возникающих при построении пакетов компьютерного моделирования, и как учебный пакет.

Над проектом работают студенты и аспиранты кафедры РВКС. Автор проекта получил диплом победителя на Всероссийском конкурсе в номинации «Иновационные технологии в образовательном процессе» в 2011 году. Исследование возможности применения итерационных методов с предобусловливанием было поддержано правительством Санкт-Петербурга в виде гранта в 2012 году. В 2014 году научно-исследовательская среда моделирования сложных динамических систем OpenMVLShell была зарегистрирована Федеральной службой по интеллектуальной собственности (свидетельство об официальной регистрации программы для ЭВМ № 2014611908 от 23.04.2014).

На настоящем этапе развития проекта OpenMVL ставится задача исследования возможности применения прямых методов решения больших разреженных систем, возникающих при компонентном моделировании. В подпрограмме MA28 [1], предусмотрена возможность приводить систему к системе с блочной нижне-треугольной матрицей с помощью алгоритма Тарьяна [2]. В связи с этим актуальным является исследовать на базе открытого пакета OpenMVLShell эффективность использования алгоритма Тарьяна при решении разреженных задач и сделать вывод о его эффективности применительно к этапу структурного анализа в пакетах компьютерного моделирования.

### *Цели и задачи*

Целью работы на данном этапе развития проекта OpenMVL является исследование эффективности использования алгоритма Тарьяна поиска сильно-связных компонент на графе [2] применительно к выделению в совокупной алгебраической системе блочной нижне-треугольной структуры в средах визуального моделирования сложных динамических систем.

Задачи исследования:

1. Реализация алгоритма Тарьяна в исследовательском пакете OpenMVLShell.

2. Реализация возможности подключения алгоритма Тарьяна на этапе исполнения модели (автоматический структурный анализ).

3. Выявление независимых компонент системы, распараллеливание вычислений на основе полученной информации.

4. Сравнение на различных классах задач получаемого времени решения со временем решения без алгоритма Тарьяна, сравнение по производительности с академической лицензией подпрограммы MA28.

### *Актуальность исследуемой проблемы*

Широко распространенной и востребованной на практике является такая возможность пакетов компьютерного моделирования, как декомпозиция моделируемой сложной динамической системы на подсистемы – компоненты, объединяемые различными видами топологических связей [3] (*Matlab/Simulink*, *Anylogic*, *MvStudium*, *Ptolemy*, *Dymola* и пр.). Такая возможность наряду с большинством профессиональных сред моделирования реализована и в *OpenMVLShell*. Многокомпонентные модели естественным образом приводят к блочной матрице структуры, диагональным блокам которой соответствуют определенные пользователем компоненты. Связи между компонентами такой системы соответствуют ненулевым элементам вне диагональных блоков. Если совокупная модель спроектирована таким образом, что связей между компонентами относительно немного (классический случай), это означает, что, скорей всего, матрица структуры окажется сильно разреженной (небольшое число элементов вне блоков на диагонали). То есть для реализации эффективных вычислений требуется уметь выделять компоненты системы на матрице структуры совокупной системы. В таких условиях ожидается, что алгоритм Тарьяна позволит:

1. Выделить компоненты системы в матрице структуры (сильно-связные компоненты в терминах алгоритма Тарьяна).

2. Выявить те из них, которые независимы (подготовка для параллельных вычислений).

3. Упорядочить те из них, которые имеют «внешние» связи [3], в том порядке, в котором следует выполнять решение системы (подготовка к сведению исходной задачи к последовательному решению задач, как правило, много меньшей размерности).

Для каждой компоненты распознается форма с тем, чтобы в автоматическом режиме выбрать решатель, который наилучшим образом подходит для разрешаемой компоненты. Для распознавания будут использованы следующие критерии: наличие дифференциальных уравнений, наличие алгебраических уравнений, структурные особенности (ленточная, разреженная или плотная формы). Кроме того, даже если пользователь определил компоненту, которая в действительности может быть разделена на подзадачи (подкомпоненты меньшей размерности), алгоритм Тарьяна распознает данную ситуацию и позволит выполнить расщепление исходной компо-

ненты на меньшие (снижение вычислительной нагрузки, расходов оперативной памяти). Механизм организации вычислений схематично изображен на рисунке.

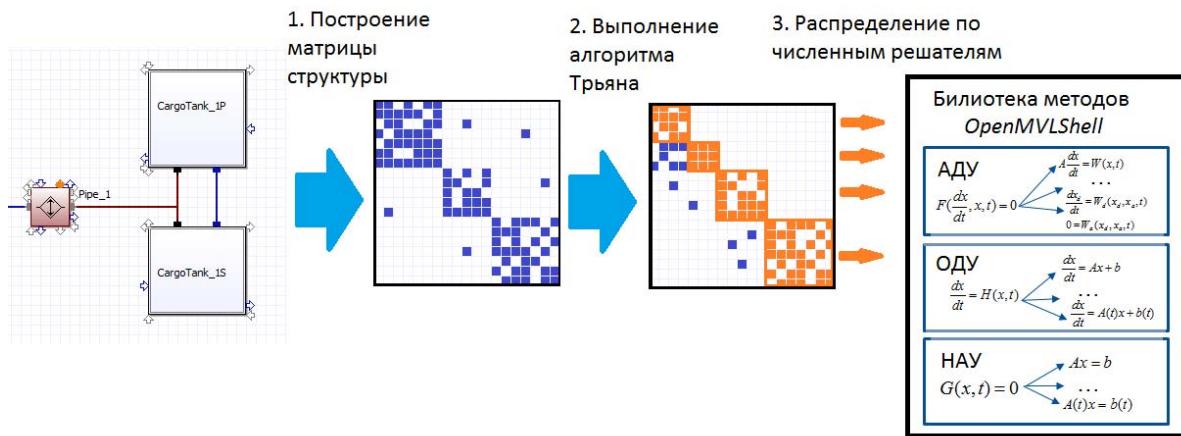


Рисунок. Примерная схема реализуемой организации вычислений для многокомпонентной модели в пакете OpenMVLShell

Предварительные тесты показали простоту реализации алгоритма Тарьяна, а также экономичность использования оперативной памяти. Этот факт и то, что подпрограмма MA28 [1] для разреженных задач, судя по опыту ее использования в различных приложениях, работает достаточно эффективно, является основанием реализовать алгоритм Тарьяна в пакете OpenMVLShell и сделать оценку эффективности его внедрения в условиях проведения всех этапов численного эксперимента, выполняемых пакетом автоматически (построение программы модели, запуска двигателя модельного поведения, поддержка работы гибридного автомата и пр.).

### Планируемые результаты

По результатам исследований, проводимых на различных классах задач, будут сделаны выводы об эффективности использования алгоритма Тарьяна применительно к автоматической структурной обработке совокупной математической системы. Эффект от использования алгоритма Тарьяна на стадии структурного анализа системы (работает до численных методов) будет сравниваться с использованием подпрограммы MA28 с академической лицензией (алгоритм Тарьяна используется внутри численного метода). Для обоих вариантов будет построен анализ зависимостей следующих коррелирующих факторов:

1. Разреженность исходной задачи (количество связей многокомпонентной модели).
2. Отношение числа определенных пользователем компонент к совокупной размерности системы.

3. Трудоемкость выполнения алгоритма Тарьяна (относительная доля по времени выполнения).

4. Трудоемкость выполнения численного решения (относительная доля по времени выполнения).

На основании взаимосвязи данных факторов, будет сделан вывод о том, на каком классе задач алгоритм Тарьяна является достаточно эффективным инструментом в сравнении с «традиционным» подходом организации вычислений непрерывного потока задач, возникающего при моделировании многокомпонентной гибридной системы.

### *Области возможного использования результатов*

Результаты проведенных исследований будут опубликованы в сети Интернет [4] и доступны любому заинтересовавшемуся проектом. Причем доступ возможен на уровне исходных текстов, что важно с точки зрения воспроизводимости полученных результатов. Выводы, сделанные в исследовании, могут быть взяты на вооружение разработчиками профессиональных сред моделирования, которые, в свою очередь, самостоятельно могут привлекать оболочку OpenMVLShell в качестве вспомогательного практического инструмента, подтверждающего сделанные в работе выводы. В частности, результаты проведенной исследовательской работы будут обсуждаться совместно с коллективом разработчиков MvSodium Group на предмет внедрение апробированных решений в профессиональный пакет компьютерного моделирования Rand Model Designer [5]. Для этого будут исследованы разработанные промышленные модельные приложения, подготовленные компанией ЗАО «Транзас Технологии» на предмет эффективности применения на них реализованного подхода.

### **Список используемых источников**

1. Технология разреженных матриц / С. Писсанецки – М. : Мир, 1988. – 410 с.
2. Depth-first search and linear graph algorithms / R. E. Tarjan // SIAM Journal on Computing. – 1972. – Vol. 1 – С. 146–160.
3. Моделирование систем. Практикум по компьютерному моделированию / Ю. Б. Колесов, Ю. Б. Сениченков. – СПб. : БХВ-Петербург, 2007. – 352 с.
4. Проект OpenMVL в сети Интернет. – URL: <https://dcn.ftk.spbstu.ru/index.php?id=276> (Дата обращения 29.05.2014); <https://dcn.ftk.spbstu.ru/redmine/projects/openmvl> (Дата обращения 29.05.2014, требуется регистрация).
5. Группа разработчиков Rand Model Designer. – URL: <http://mvstudium.com> (Дата обращения 29.05.2014).

*Статья представлена заведующим кафедрой «Распределенные вычисления и компьютерные сети» СПбГПУ, д-ром техн. наук, профессором Ю. Г. Карповым.*

**УДК 654.739**

**Ле Чан Дык (студент группы МТ-95 СПбГУТ)**

## **МОДЕЛЬ МЕЖДОМЕННОГО ВЗАИМОДЕЙСТВИЯ В SDN С ИСПОЛЬЗОВАНИЕМ ДВУХ КОНТРОЛЛЕРОВ**

### *Введение*

Управление мультисервисной сетью является сложной задачей, для решения которой предлагается достаточно много подходов. Использование программно-конфигурируемых сетей (*SDN*) позволяет снизить издержки на управление и упростить его за счет предсказуемости параметров. При этом вопросы междоменного взаимодействия на основе *SDN*-контроллеров решены слабо.

### *Анализ существующих решений масштабируемости SDN*

Существует два основных метода взаимодействия между отдельными *SDN*-контроллерами в разных доменах. Либо использовать протокол или специальный модуль для непосредственного соединения и обмен информацией между *SDN*-контроллерами, либо создание отдельного сервера или базы данных для сохранения сетевой информации.

*ALTOserver* [1] использует выделенных сервер для собора сетевой информации от доменов через *SDN*-контроллеры с помощью Pull/Push модели. Однако, расчет оптимальных путей всей сети сосредоточен только на сервере, что приводит к невысокой производительности. В *ALTO*-модели отсутствует механизм обновления, а наличие автопереговоров существенно увеличивает задержку.

*HyperFlow* [2] использует мульти-контроллеры для построения распределенной плоскости управления, и каждый контроллер отвечает за небольшую область сети. Каждый контроллер *HyperFlow* имеет право распоряжаться сетевыми событиями в определенном сегменте сети, и события, которые влияют на глобальную сеть, реализуются путем лавинной рассылки. Такой подход ориентирован на события, которые не встречаются часто, например, изменения статуса ссылки.

*SDNi* [3] – протокол обмена сообщениями программно-конфигурируемых сетей через мультисубсетевые домены. Этот протокол предназначен для определения нескольких основных типов сообщений обмена данными между контроллерами, таких как информация о достижимости, процессы настройки потока, обновления.

*SDN* имеет много достоинств, но на сети с преобладанием потокового трафика необоснованно полагаться на централизованное программное обеспечение контроллера, которое устанавливает правила работы на осно-

ве первого пакета каждого потока. Несколько попыток было сделано, чтобы решить проблему масштабирования SDN путем разработки распределенных решений, например, DevoFlow [4] и DIFANE [5]. Суть этих методов состоит в идее возвращения части функционала управления коммутаторам, чтобы уменьшить нагрузку в плоскости управления. DIFANE пытается разгрузить сеть путем передачи части функций от контроллера к специальным коммутаторам (authority switches). Используя этот подход, сетевые операторы могут снизить нагрузку на контроллере и уменьшить задержку установки правил. DevoFlow вводит новые механизмы в коммутаторах чтобы управлять гораздо меньше «важными» событиями в плоскости управления.

Анализ механизмов и протоколов, задействованных у междоменном взаимодействии в SDN, показал наличие у всех рассмотренных решений следующих недостатков:

- отсутствие механизма взаимодействия между другими типами SDN-контроллеров;
- ориентированность только на топологию сети и игнорирование других типов информации;
- вычисление, расчет пути при маршрутизации обычно сосредоточен на одном устройстве;
- обновление сетевой информации пассивно, SDN-контроллеры обычно должны провести обмен служебной информацией прежде чем установить пути, хотя они уже обладают информацией о маршрутизации;
- регулярное появление новых модулей, которые отвечают за новые функции, что приводит к несогласованности решений различных производителей.

### *Модель организации междоменного взаимодействия с использованием двух контроллеров*

В представленном решении предпринята попытка избавится от указанных недостатков путем введения нового механизма обмена сетевой информацией. Основная идея предлагаемой модели состоит во введении в домен второго контроллера специально для обеспечения междоменного взаимодействия. Обмен обновлениями между этими доменами происходит с использованием специальных пакетов, при этом непрерывно и равномерно. На [рисунке 1](#) представлена архитектура предлагаемого сетевого решения. В каждом домене реализовано два контроллера: Домен 1 –  $C_1$  и  $C_1'$ ; домен 2 –  $C_2$  и  $C_2'$ ; домен 3 –  $C_3$  и  $C_3'$ . В дальнейшем для удобства приняты обозначения без указания номера домена:  $C_1$ ,  $C_2$ ,  $C_3$  общим назначением  $C$ , а  $C_1'$ ,  $C_2'$ ,  $C_3'$  –  $C'$ .

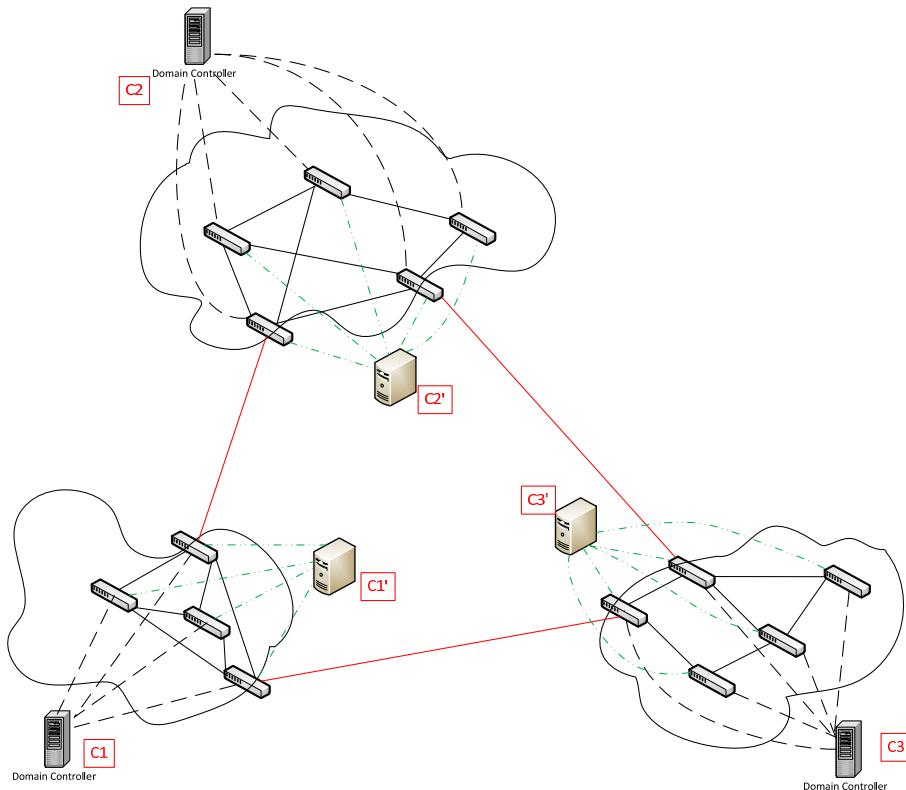


Рис. 1. Архитектура SDN-сети с использованием двух доменов

В каждом домене контроллер  $C$  отвечает за внутренние функции домена, например, маршрутизация между коммутаторами своего домена, вычисление кратчайших путей, установление правил в таблицах потока. Можно сказать, что контроллеры  $C$  выполняют работу обычного SDN-контроллера.

Контроллеры  $C'$  отвечают за взаимодействие между доменами. Каждый из  $C'$  обновляет сетевую информацию, вычисляет наилучший путь до точки назначения, сохраняет глобальную информацию о междоменном взаимодействии.

### *Механизмы обновления информации*

#### *1. Внутри домена*

В сетевом домене под управлением контроллера  $C$  после того, как соединения между контроллером и OpenFlow-коммутаторами были успешно установлены, запускается процесс LLDP (Link Layer Discovery Protocol). В результате передаются основные сведения об узлах. Чтобы узнать остальную сетевую информацию домена, такую как версия OpenFlow, номер таблицы потоков на каждом узле и др. используется расширение LLDP.

После этого, контроллер  $C$  начинает вычислять пути. Результаты вычисления и специальная доменная информация сохраняется в базе данных Database\_1 контроллера  $C$ . После информации из Database\_1, необходимая для междоменного взаимодействия передается периодически на контрол-

лер  $C'$  с интервалом  $T1$ . Это обновление осуществляется по следующему алгоритму: информация из Database\_1 формируется как пакет  $P1$  и через период  $T1$  этот пакет передается на коммутатор, в котором заранее установлена специальная запись в таблице потоков. Эта запись указывает коммутатору как передать приходящий пакет  $P1$  на контроллер  $C'$  (рис. 2).

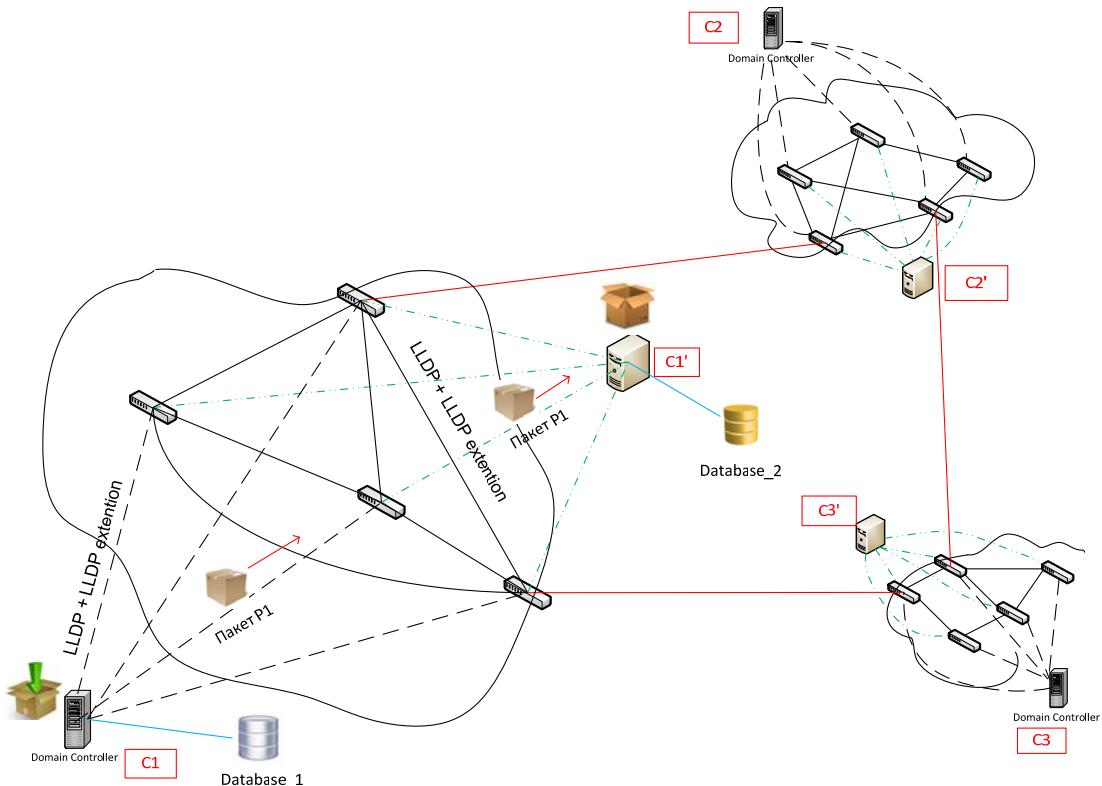


Рис. 2. Механизм обновления информации внутри домена

## 2. Междоменное обновление

Контроллер  $C'$  после получения пакета  $P1$  сохраняет внутридоменную информацию в своей базе данных Database\_2. Контроллер  $C'$  также вычисляет внешнюю доменную информацию и сохраняет в этой же базе. Затем  $C'$  выполняет обновление междоменной информации периодически по определенному периоду  $T2$ . Для этого  $C'$  упаковывает обновления Database\_2 в формате пакетов  $P2$  и передает их на граничные узлы домена. На этих узлах в таблице потоков прописаны:

- запись маршрута передачи  $P1$  от граничного узла через установленный порт в другой домен;
- специальная запись для осуществления функции передачи обновленного пакета  $P2$  от другого домена на контроллер  $C'$ .

После того, как пакеты  $P2$  от  $C'$  данного домена передаются на другие домены через граничные узлы, они передаются на домашние контроллеры доменов с помощью специальных записей в таблице потоков. После получения обновлений контроллер  $C'$  обновляет записи в Database\_2 и вычис-

ляет пути и требования на маршрутах между доменами. После результаты сохраняются в Database\_2. В завершении контроллер  $C'$  устанавливает новые правила в таблице потоков коммутаторов (рис. 3).

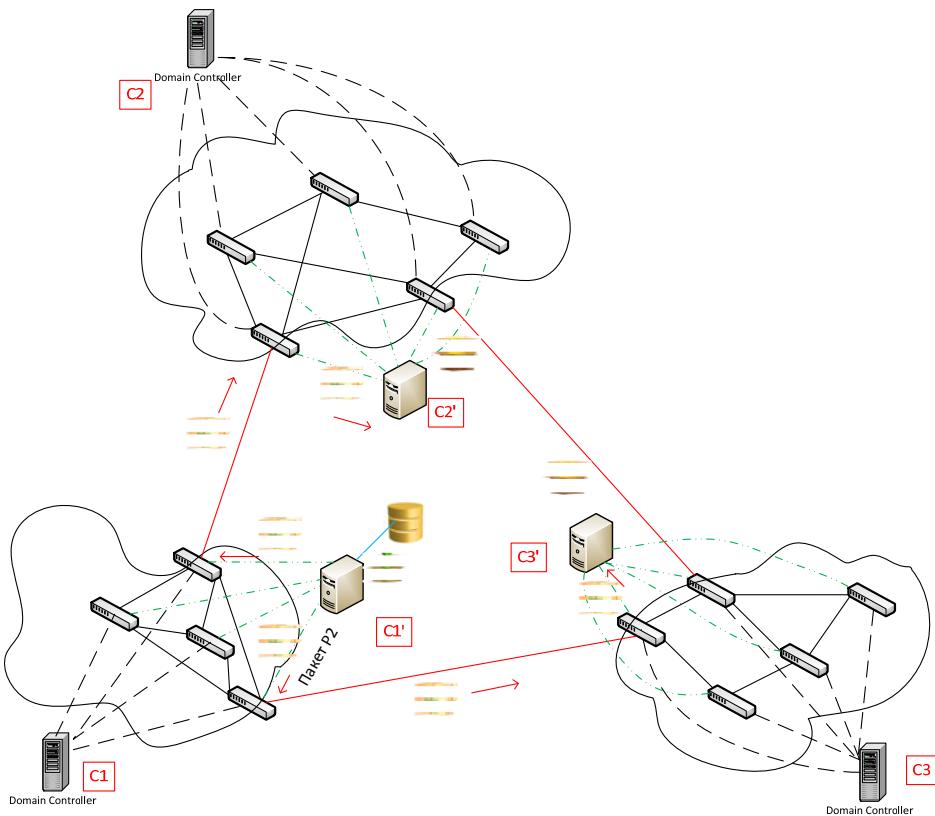


Рис. 3. Механизм обновления сетевой информацией между доменами

Процессы обновления внутри и между доменами продолжаются через периоды  $T1$  и  $T2$ . Отметим, что вычисления в  $C$  и  $C'$  происходят только после обновлений в базах данных Database\_1 и Database\_2.

### 3. Лучший путь – Best path

В предлагаемой модели понятие лучший путь (Best path) модифицируется. При этом лучший путь не совпадает с кратчайшим путем в IP-маршрутизации. Теперь:

$$\text{Best path} = \text{Best\_path\_внутридомена} + \text{Best\_path\_междомена}$$

Best\_path\_внутридомена: зависит от требования пользователей или сетевых приложений, выбирается по заданному критерию.

Best\_path\_междомена: в качестве критерия используется количество промежуточных доменов для выбора лучшего пути.

### Выход

В предложенной модели междоменного взаимодействия в SDN с использованием двух контроллеров реализуется новый подход, ориентиро-

ванный на делегирование функций управления между однородными устройствами – контроллерами SDN. В работе также предлагается использовать комбинированную метрику для определения лучшего пути при междоменном взаимодействии.

#### **Список используемых источников**

1. **Defining Data Flow Paths in Software-Defined Networks with Application-Layer Traffic Optimization** / H. Yin, Z. Ting, X. Haiyong // U.S. Patent Application 13/915, 410. – C. 3–5.
2. **Hyperflow:** a distributed control plane for openflow / A. Tootoonchian, G. Yashar // Proceedings of the 2010 internet network management conference on Research on enterprise networking. – USENIX Association, 2010. – C. 1–4.
3. **SDNi:** A message exchange protocol for software defined networks (SDNs) across multiple domains / H. Yin et al. // Submitted to IETF Internet-draft, Dec (2012). – C. 10–11.
4. **DevoFlow:** scaling flow management for high-performance networks / Andrew R. Curtis et al. // ACM SIGCOMM Computer Communication Review. – Vol. 41. – No. 4. ACM, 2011. – C. 6–7.
5. **Scalable** flow-based networking with DIFANE / M. Yu et al. // ACM SIGCOMM Computer Communication Review 40.4 (2010): 351–362. – C. 1–3.

*Статья представлена научным руководителем канд. техн. наук, доцентом О. А. Симониной.*

**УДК 004.421**

**К. С. Орлов (студент группы СП-01 СПбГУТ)**  
**А. А. Шолохов (студент группы СП-01 СПбГУТ)**

#### **КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ДЛЯ ПОДГОТОВКИ К ОЛИМПИАДЕ ПО СПОРТИВНОМУ ПРОГРАММИРОВАНИЮ**

Международная студенческая олимпиада по программированию (в английском принят сокращение *ACM/ICPC* или просто *ICPC*) – крупнейшая студенческая командная олимпиада попрограммированию, которая уходит своими корнями в соревнование, проводившееся в Техасском университете в 1970. Начиная с 1977 года, когда был проведен первый финал в рамках ежегодной конференции ACM по информатике, проводится ежегодно.

Олимпиада – командное соревнование. Каждая команда состоит из трёх студентов. К участию допускаются студенты высших учебных заведений, а также аспиранты первого года обучения. Студенты, дважды

участвовавшие в финальной стадии олимпиады, или пятикратно принимавшие участие в региональном отборе, не допускаются к участию.

Каждой команде выдаётся один компьютер и от восьми до двенадцати задач, условия которых, в силу международного формата соревнования, написаны на английском языке, на пять часов. Таким образом, в связи с сильной ограниченностью ресурсов, навыки эффективной и слаженной командной работы выходят на первый план.

Команды пишут решения на языках программирования C, C++ или Java и посылают их на тестирующий сервер, который проверяет решение на большом количестве подготовленных тестов, заранее неизвестных для участников.

Побеждает команда, решившая правильно наибольшее число задач. Если несколько команд решают одинаковое количество задач, то их положение в рейтинге определяется штрафным временем. Изначально штрафное время каждой команды равно нулю. За каждую правильно сданную задачу к штрафному времени команды прибавляют время, прошедшее с начала соревнования до момента сдачи задачи. Кроме того, если зачтённой попытке предшествовало несколько неудачных попыток сдать ту же задачу, то за каждую из них к штрафному времени прибавляют двадцать минут. За неудачные попытки сдать задачу, которую команде в итоге так и не удалось решить, штрафного времени не начисляется.

На тестирующий сервер установлено специальное ПО, называемое «электронный судья». В задачи такого судьи входит:

- организация очереди проверки задач;
- проверка задачи на различном наборе тестов;
- контроль безопасности, времени исполнения и потребление памяти решения команды;
- оповещение участников о результате проверки.

Электронный судья обладает большим набором утилит для измерения метрики предложенного решения. В связи с этим, существует несколько возможных результатов проверки задачи:

- *Ошибка компиляции (Compilation error)* – серверу не удалось скомпилировать предложенное участниками решение. Параметры компиляции для каждого соревнования указываются в соответствующем разделе регламента проведения олимпиады.
- *Нарушение безопасности (Security violation)* – решение использует запрещенные возможности (ассемблерные вставки, попытка записи в системные области памяти, использование сети). При выявлении нарушения команда, отправившее такое решение, дисквалифицируется.
- *Превышен лимит времени (Time limit exceeded)* – решение работает слишком долго. Это значит, что выбран не оптимальный алгоритм решения или программа зациклилась.

- *Превышен лимит памяти (Memory limit exceeded)* – программа попыталась выделить больше оперативной памяти, чем это допустимо по условию задачи.
- *Превышен лимит бездействия (Idleness limit exceeded)* – программа не потребляет процессорного времени, например — ожидается ввод из пустого файла или входного потока.
- *Ошибка во время исполнения (Runtime error)* – решение заканчивается с не нулевым кодом возврата. Возможно обращение к несуществующему элементу массива, деление на ноль, и.т.п.
- *Ошибка представления (Presentation error)* – ответ на задачу выведен в отличном от указанного формата.
- *Неверный ответ (Wrong answer)* – неверный ответ на некотором наборе входных данных. Обычно, указывается номер теста, на котором программа работает некорректно.
- *Принято (Accepted)* – программа успешно прошла все тесты, решение корректно.

Для подготовки студентов первых-вторых курсов к олимпиадам по программированию был разработан следующий план занятий:

- *Основы языка C++* – вводное занятие. Рассчитано на тех, кто никогда не сталкивался с языком C++;
- *STL* – лекция посвящена стандартной библиотеке. Умение пользоваться готовыми контейнерами и функциями поможет сэкономить время и избавит от дополнительных ошибок [1];
- *Структуры данных* – стандартные контейнеры не всегда подходят, поэтому необходимо уметь реализовывать модифицированные версии списков, очередей или стеков для конкретной задачи. Также знание реализации структур данных необходимо для вычисления сложности алгоритма и корректной оценки времени;
- *Динамическое программирование* – понимание принципов динамического программирования поможет оптимизировать код и эффективно использовать временные ресурсы;
- *Графы* – тема, которая служит основой не только для олимпиадного программирования. Маршрутизация, поиск кратчайших путей, поиск оптимальных путей, задача оптимизации — все это явно или нет сводится к графам [2]. Кроме того, в теории любой алгоритм можно представить в виде конечного автомата.
- *Деревья* – частная форма графа. На деревьях основываются такие оптимальные структуры данных как куча, дерево поиска, красно-черное дерево и др.

Рассмотрим следующую типичную задачу такой олимпиады [3]: необходимо посчитать сумму всех элементов массива на промежутке от  $a$  до  $b$ .

Самый простой и очевидный способ – каждый раз считать сумму начиная с индекса  $a$  и заканчивая индексом  $b$ . В худшем случае такой алгоритм будет работать за  $O(n)$  (Прим.: худшим случаем будет случай, когда  $a$  будет индексом первого элемента в массиве, а  $b$  – последнего).

Усложним задачу: найдем  $m$  сумм для различных пар  $a$  и  $b$ . Теперь наш алгоритм будет работать за  $O(m * n)$ , что при больших значениях  $m$  и  $n$  неизбежно приведет к большим затратам процессорного времени и вердикту «Лимит времени» от электронного судьи.

Очевидно, требуется некоторая оптимизация. Исходный массив не меняется на протяжении задачи, меняются только интервалы, на которых необходимо вычислить сумму элементов. Заведем массив, в котором будем хранить суммы элементов исходного массива по следующему правилу: в  $i$ -й позиции нового массива будем хранить сумму всех элементов исходного массива начиная с первого элемента и заканчивая элементом с номером  $i$ :

$$\text{новый массив}[i] = \sum_{0}^i \text{исходный массив}[i]$$

Теперь, для того, чтобы вычислить сумму какого-либо интервала  $a - b$  в исходном массиве, необходимо вычислить разность нового массива с индексом  $b$  и нового массива с индексом  $a$  (сумма элементов исходного массива от 0 до  $b$  без суммы элементов исходного массива от 0 до  $a$  ).

Сложность этого алгоритма состоит из двух частей:

1. Заполнение нового массива за  $O(n)$ .
2. Вычисление  $m$  сумм промежутков (или в нашем случае разностей) за  $O(m * 1)$ .

Таким образом, общая сложность будет равна  $O(n + m)$ , и даже при больших значениях  $m$  и  $n$  наша задача будет решаться за оптимальное время.

#### Список используемых источников

1. **Искусство программирования** / Д. Кнут; пер. с англ. – М. : Вильямс, 2009. – 760 с.
2. **Теория графов** / Ф. Харари; изд. 2-е. – М. : Едиториал УРСС, 2003. – 237 с.
3. **Олимпиадные задачи по программированию** / Ф. В. Меньшиков. – СПб. : Питер, 2006. – 230 с.

*Статья представлена научным руководителем, доцентом О. Б. Петровой.*

УДК 621

**А. Г. Радченко (студентка группы СП-92 СПбГУТ)**

## **МАТЕМАТИЧЕСКАЯ И ПРОГРАММНАЯ МОДЕЛЬ ОБРАБОТКИ ИЗОБРАЖЕНИЙ МИКРОСРЕЗОВ КОЖНОГО ПОКРОВА**

### *Введение*

Зрение является наиболее совершенным из наших органов чувств, потому не удивительно, что зрительные образы играют важную роль в человеческом восприятии. Однако, в отличие от людей, способных воспринимать электромагнитное излучение лишь в видимом диапазоне, машинная обработка охватывает практически весь спектр. Обрабатываемые изображения могут порождаться такими источниками, как, например, ультразвуковые изображения, изображения получаемые в электронный микроскоп или генерируемые компьютером.

Естественным этапом перехода от обработки изображений к их анализу выступает распознавание отдельных областей или объектов на изображении. Теория распознавания образов применяется, в том числе, в вычислительных машинах, помогающих поставить медицинский диагноз и рекомендующих лечение. Методами теории распознавания можно анализировать и классифицировать такие клинические данные, как ультразвуковые изображение, изображения полученные в электронный микроскоп и т. п.

### *Особенности обработки микросрезов кожного покрова*

Изображение микросрезов (рис. 1) кожного покрова представляет собой близко расположенные, не структурированные объекты, что не дает возможности точного определения границ этих объектов, а, следовательно, является препятствием для анализа состояния клеток и процессов, происходящих в кожном покрове.

Необходимо четко представлять, что в качестве цифрового изображения хранится только двумерный массив чисел того или иного формата. В простейшем случае каждый элемент массива имеет скалярное целочисленное значение, пропорциональное значению функции яркости в донной точке плоскости изображения. Нужный формат без труда можно трансформировать из любого представления графической информации в виде матрицы, в которой каждый элемент соответствует пикселю с определенной градацией цветности (например, формат BMP).



Рис. 1. Исходное изображение микросреза кожного покрова

Для решения данной задачи используется подход, при котором распределение градаций цветности рассматриваются в виде полевых структур. Он дает возможность оперировать таким понятием, как особые точки.

Особые точки в любом изображении играют большую роль и фактически создают облик изображения, хотя число этих точек, как правило, существенно меньше обычных пикселей. Не смотря на это, в дальнейшем стоит учитывать, что в общем случае создаваемое изображение, без сглаженного поля, имеет искаженную цветовую гамму. Это связано с тем, что источники, которые служат строительным материалом для поля особых точек, определяются перепадами градаций цветности, а не значениями.

Наборы последовательных особых точек объединяются в цепочки, которые являются границами перепадов цветности - кромками изображения. Эти кромки представляют собой линейные объекты, объединенные в список.

Обычно для определения границ используются базовые операции усреднение изображения и выделение контуров. В [1] представлена обработка изображения, полученного космическим телескопом «Хаббл» и предоставленного авторам указанного источника Р. Гонсалису и Р. Вудсу Агентством NASA.

Элементы исходного изображения представляют собой неструктурированные объекты, границы которых без дополнительной обработки невозможно определить. Поэтому в качестве первого шага авторами приведенного источника для улучшения структурирования объектов была использована операция усреднения фильтром с маской  $15 \times 15$  элементов.

В случае обработки изображение микросреза кожного покрова подобному плану решения препятствует плотность анализируемых элементов. При применении маски с большим числом элементов все объекты сливаются в единое целое, а при применении масок с малым числом элементов не происходит достаточного усреднения. На рисунке 2 приведен пример обработки изображения маской  $15 \times 15$ .



Рис. 2. Изображение микросреза кожного покрова после обработки сглаживающим фильтром с маской  $15 \times 15$

Очевидно, что данное изображение не пригодно для дальнейшего анализа. Изображение размытое, не структурированное.

При обработке изображения маской  $1 \times 1$  (рис. 3) в результате фильтрации на визуальном уровне изменений (также, как и в обычном фильтре) не наблюдаются, но в отличие от других фильтров в полевом фильтре в силу его нелинейности происходит упорядочивание информации, которое можно обнаружить косвенным способом [2].



Рис. 3. Изображение микросреза кожного покрова после обработки сглаживающим фильтром с маской  $1 \times 1$

Подобная фильтрация является высокочастотной, со следующими свойствами:

- в результате обработки объекты изображения становятся более структуризованными;
- обработка упорядочивает изображение в радиусе одного пикселя.

При многократном повторении фильтрации с маской  $1 \times 1$  все объекты сохраняют свои очертания, разделены, являются более распознаваемыми. На основе данного изображения не сложно произвести пороговую обработку.

После предварительной фильтрации и пороговой обработки на изображении (рис. 4) сформировались четко выраженные объекты, представляющие собой кромки [3].

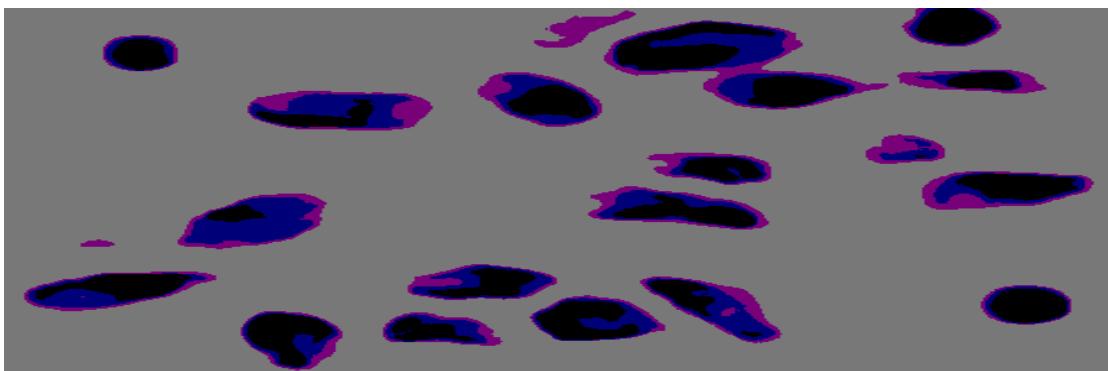


Рис. 4. Изображение микросреза кожного покрова после пороговой обработки

На рисунке 4 расположены 21 кромка. С программной точки зрения каждая кромка начинается с кода размером один байт, который записывается в начало и определяет направление перепадов градаций цветности в особых точках. Далее в кромке идет последовательное перечисление каждой особой точки, которая в нее входит, для описания точки используется 7 байт, из которых 4 байта определяют координаты относительно начала изображения и 3 байта информацию о цветовой градации в формате RGB. Окончание кромки фиксируется кодом из двух байт. На основе информации об особых точках можно сделать вывод о форме кромки (например, клетка вытянута или имеет более круглую форму), а соответственно и клетки.

В зависимости от поставленной задачи, можно проводить анализ изображений клеток. Например, нормальная клетка имеет форму, при которой соотношение длины и ширины составляет  $2/1 \pm 10\%$ . При просмотре информации о кромках, можно получить координаты особых точек относительно начала координат изображения, а соответственно путем не сложных вычислений определить, какие клетки имеют не нормальную форму и где они расположены.

#### Список используемых источников

1. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М. : Техносфера, 2005. – 1072 с.
2. Сглаживание изображений на основе решения краевой задач / Ю. Ф. Болтов, И. А. Волков // Телекоммуникации. – 2010. – № 5. – С. 17–25.
3. Обработка визуальной информации на основе ее представления в виде скалярных или векторных полей: концепция, математические модели и алгоритмы: монография / Ю. Ф. Болтов. – СПб. : СПбГУТ, 2010. – 183 с.

*Статья представлена научным руководителем, канд. техн. наук, доцентом Ю. Ф. Болтовым.*

УДК 654.739

**В. В. Скачкова (студентка группы МБИ-22м СПбГУТ)**

## **РАЗРАБОТКА ПРЕДЛОЖЕНИЯ ПО ВЫБОРУ ИЗОБРАЖЕНИЙ ДЛЯ ГРАФИЧЕСКОГО ПАРОЛИРОВАНИЯ**

Важным и необходимым аспектом информационной безопасности вычислительной системы является подсистема управления доступом пользователей. Несмотря на развитие аппаратных средств и методов защиты от несанкционированного доступа, незаменимым остается паролирование.

Основным недостатком численно-буквенных паролей является то, что они должны заключать в себе два противоречивых требования: с одной стороны, пароль должен быть достаточно легко запоминаемым, с другой стороны устойчивым к атаке подбора пароля, т. е. пароль должен быть длинным случайным, а значит трудно запоминаемым.

С увеличением аккаунтов у одного пользователя количество оригинальных паролей возрастает, тем самым объем информации, которую должен запомнить человек возрастает соответственно.

Альтернативой численно – буквенным системам паролирования стала система аутентификация на основе графического пароля. С точки зрения психологии, простота запоминания графического пароля обуславливается тем, что человеку легче запомнить информацию, когда она тесно связана с контекстом, так как ассоциативная память у человека развита сильнее.

Все системы аутентификации на основе графического пароля делятся на две группы – распознавание предметов [1] и воспроизведение действий [2]. Распознавание предметов заключается в том, что человеку необходимо определить ранее видимое им изображение, а воспроизведение действий требует воссоздание объекта идентичного созданному при регистрации пользователя. Классической системой, основанной на распознавании, является схема Блондера [3], на основе которой и было произведено наше исследование.

В этой системе в процессе регистрации пользователь выбирает некоторое изображение и задает в нем несколько парольных элементов. Обычно парольным элементом может быть одна точка (1 пиксел) на изображении. В процессе аутентификации пользователю предлагается найти ранее заданные им элементы на изображении и отметить их, например, кликнув по ним указателем мыши. Процесс аутентификации считался корректным, если все элементы выбраны верно.

Для того чтобы лучше запомнить выбранные элементы, графический материал иметь смысловую нагрузку. Абстрактные изображения запоминаются хуже [4], так как долговременная память человека запоминает основной смысл изображения, а не всю картинку целиком. Таким образом,

для успешного сохранения в памяти информация должна иметь конкретный смысл.

Подбор и оценка графического материала для графического пароля является важным вопросом.

Оценку пригодности материала (изображения) для систем аутентификации на основе графического паролирования можно производить двумя способами: визуально и автоматически. Визуальная оценка изображения является долгой и субъективной, а также требующая детального анализа от специалиста. Поэтому мы сосредоточим свое внимание на системах автоматизированной оценки пригодности изображения для его использования в качестве графического пароля. Для этого сначала проанализируем, как формируется зрительный образ объекта у человека.

Исследования человеческого зрения и механизмов запоминания объектов показали, что представление формы объекта хранится в памяти отдельно от представления способов его использования и назначения, следовательно, это разные характеристики объекта. Так же только зрение может породить некоторое внутреннее описание формы рассматриваемого объекта, причем даже в том случае, когда его назначение не установлено. Таким образом, если рассматривать изображение как двумерный эскиз, то человек имеет представление главным образом об изменении яркости и геометрических свойствах их распределения – то есть о контурах.

Поэтому основным параметром, по которому можно автоматически оценивать изображение – это количество так называемых контуров [5] (границ объектов) на изображении. Контуры, которые мы будем применять для анализа, это контуры, определяющие форму, поскольку они являются двумерными, сообщающими информацию о трехмерной форме объектов [6].

Однако контуры могут быть образованы также поверхностью объекта, это так называемая текстура. Текстура (от латинского *textura* – ткань) – скопление цветовых точек, в массе своей создающих какое – либо изображение. Например, изображение шерсти животных, песка, и т. д.

Текстуры чаще всего могут быть мелкими, однообразными, а, следовательно, объектами сложными для запоминания и использования в качестве составляющей пароля, поэтому они не могут рекомендоваться для выбора точек в графическом пароле. Следовательно, текстура должна быть удалена в аппаратном анализе изображений.

Таким образом, можно предположить, что пригодность изображения для использования в качестве графического пароля зависит от количества и длины контуров на изображении. То есть пригодность можно выразить в формуле:

$$P_{\text{пр}} = \frac{L_{\text{конт}}}{N_{\text{пикс}}}, \quad (1)$$

где  $P_{\text{пр}}$  – коэффициент пригодности изображения,  $L_{\text{конт}}$  – длина всех контуров в пикселях,  $N_{\text{пикс}}$  – количество пикселей на всем изображении.

На основе этого подхода для автоматизированного анализа пригодности изображения для графического паролирования, была разработана программа «Контурный анализ» в среде C++. Программа находит контура в изображении, измеряет их длину и рассчитывает коэффициент пригодности. Программа содержит функцию выделения текстур, что позволяет отслеживать текстуры визуально. Для уменьшения влияния текстур введен режим фильтрации, параметры которого (минимальная площадь) настраиваются вручную.

Весь графический материал, предназначенный для анализа пригодности его использования для паролирования, был разделен на 7 групп:

1. Портрет – это изображение, выполненное средствами изобразительного искусства – живописи, гравюры, скульптуры, фотографии.

2. Графика – это вид изобразительного искусства, использующий в качестве основных изобразительных средств линии, штрихи пятна и точки.

3. Пейзаж – это тип изображения, представляющий природу или какую-либо местность, естественную или преображенную человеком: городские и сельские ландшафты, виды городов, зданий.

4. Интерьер – это изображения архитектурного и художественного оформленного внутреннего пространства здания, обеспечивающее человеку эстетическое восприятие и благоприятные условия жизнедеятельности.

5. Монохромное изображение – это изображения, содержащие свет одного цвета, воспринимаемый как один оттенок.

6. Натюрморт – это изображение предметов.

7. Карта – это изображение земной поверхности в уменьшенном виде, или ее участка на плоскости, имеющее свои условные обозначения, а также названия улиц, городов, номера домов и т. д.

Проведен детальный анализ каждого типа изображений на выборке из десяти образцов. Результаты исследования: коэффициент пригодности по каждому образцу, а также математическое ожидание и дисперсия по каждому типу изображения приведены в таблице.

ТАБЛИЦА. Результаты исследования видов изображений

Портрет												
№	1	2	3	4	5	6	7	8	9	10	Мат. ожид.	Дисп
$P_{\text{пр}}$	0,08	0,02	0,04	0,02	0,08	0,09	0,08	0,06	0,04	0,05	0,056	0,0006
Графика												
№	1	2	3	4	5	6	7	8	9	10	Мат. ожид.	Дисп.
$P_{\text{пр}}$	0,05	0,11	0,09	0,04	0,02	0,15	0,15	0,13	0,16	0,07	0,096	0,0024

Пейзаж												
№	1	2	3	4	5	6	7	8	9	10	Мат. ожид.	Дисп.
$P_{\text{пр}}$	0,07	0,06	0,04	0,07	0,05	0,07	0,09	0,08	0,05	0,06	0,063	0,0002
Интерьер												
№	1	2	3	4	5	6	7	8	9	10	Мат. ожид.	Дисп.
$P_{\text{пр}}$	0,09	0,04	0,07	0,13	0,11	0,04	0,04	0,03	0,04	0,02	0,061	0,0013
Монохромное												
№	1	2	3	4	5	6	7	8	9	10	Мат. ожид.	Дисп.
$P_{\text{пр}}$	0,11	0,09	0,08	0,07	0,10	0,02	0,04	0,08	0,13	0,01	0,073	0,0013
Натюрморт												
№	1	2	3	4	5	6	7	8	9	10	Мат. ожид.	Дисп.
$P_{\text{пр}}$	0,14	0,16	0,12	0,15	0,17	0,11	0,17	0,15	0,11	0,16	0,143	0,0051
Карта												
№	1	2	3	4	5	6	7	8	9	10	Мат. ожид.	Дисп.
$P_{\text{пр}}$	0,11	0,10	0,15	0,12	0,10	0,13	0,12	0,06	0,07	0,14	0,196	0,0674

На основе этих результатов разработана «шкала пригодности» (рисунок). Изображения с величиной коэффициента ниже 0,06 были признаны непригодными. За нижний порог  $P_{\text{пр}}$  была принято значение, полученное для изображения типа «портрет». (Если этот тип изображения использовать в качестве материала для графического пароля то, ассоциативно человек при вводе пароля выбирает глаза, уши, и т. д. и, следовательно, такой пароль будет легко угадываемым). Диапазон  $P_{\text{пр}}$  от 0,06 до 0,08 соответствует низкой стойкости. В этот диапазон попадают изображения типа «пейзаж», них очень много текстур. В результате фильтрации последних уменьшается длина возможных контуров. Диапазон  $P_{\text{пр}}$  от 0,08 до 0,10 – соответствует средней стойкости, а диапазон выше 0,10 – высокой. Этим диапазонам соответствуют изображения типа карта, натюрморт, графика. Такие пароли сложно угадать, поскольку в изображении достаточное количество деталей и соответственно контуров.



Рисунок. Шкала пригодности изображения

В тоже время следует отметить, что некоторые группы изображений имеют большую дисперсию. Значительный разброс от среднего показывает на высокую неоднородность графического материала в группе. Это графика, интерьер, натюрморт. Такие изображения целесообразно разбить на подгруппы, в каждой из которых графический материал будет более однородным. Среди этих типов изображений натюрморт является самым надежным видом графического материала, так как имеет большое количество деталей и логику их выбора угадать достаточно сложно.

Изображения типа «карта» также пригодны для использования, поскольку для него  $P_{\text{пр}} = 0,196$ , однако для этого типа, и большая дисперсия  $P_{\text{пр}}$ . Из объектов для выбора парольных точек следует исключить сильно заметные топографические ориентиры (вершины гор, озера, станции метро, памятники архитектуры), поскольку люди склонны выбирать их в качестве парольных элементов.

Монохромные изображения оказалась достаточно спорной категорией, так как для исследования были взяты по одному образцу из других категорий, но черно-белой цветности.

#### **Список используемых источников**

1. **Multimedia Communications Research Laboratory University of Ottawa / Fawaz A Alsulaiman, Abdulmotaleb El Saddik.** – Ottawa, Canada, 2006.
2. **Department of Computer Science and Engineering / Ashwini Fulkar, Suchita Salwa, Zubin Khan and Sarang Solanki // J.D.I.E.T., Yavatmal, MS, India, May 2012.**
3. **Graphical Password / Greg E. Blonder // United State Patent 5559961, September 1996.**
4. **Eye, Brain and vision / David H. Hubel.** – New York, 1990. – 256 p.
5. **Fundamentals of digital image processing / Chris Solomon, Toby Breckon.** – UK, 2011. – 355 p.
6. **Зрение: Информационный подход к изучению представления и обработки зрительных образов / Д. Марр.** – М. : Радио и связь, 1987. – 400 с.

*Статья представлена научным руководителем д-ром техн. наук, профессором В. А. Яковлевым.*

УДК 621

**Л. В. Фролова (студентка группы СП-92 СПбГУТ)**

## **МАТЕМАТИЧЕСКАЯ И ПРОГРАММНАЯ МОДЕЛЬ ПОСТРОЕНИЯ ПОЛЯ ОСОБЫХ ТОЧЕК НА ОСНОВЕ УРАВНЕНИЯ ЛЯМЕ**

### *Введение*

Одним из наиболее универсальных математических методов познания является метод математических моделей (математическое моделирование). Математическая модель – это описание какого-либо класса явлений на языке математики. Метод моделирования дает возможность применять математический аппарат к решению многих практических задач.

Построение математической модели открывает новый подход к обработке графической информации. Он построен на основе представления изображения в виде скалярного или векторного поля. Такое представление не требует разработки специального формата, и базируется на матрице, в которой каждый элемент определяется пиксели с определенной градацией цветности (например, формат BMP). В этом случае значения градаций цветности каждого пикселя интерпретируются как значение поля в соответствующей точке. Трактовка обычной матрицы цветности в виде полевой структуры дает возможность использовать для обработки изображений методы и приемы математической физики.

### *Общие понятия*

На кафедре «Программная инженерия и вычислительная техника» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича для обработки изображений была разработана полевая модель, для которой характерны следующие понятия [2, 3, 4]:

- особыми точками, т. е. пикселями, в окрестностях которых наблюдаются резкие перепады градаций цветности (в полевой модели они интерпретируются как источники поля, в которых нарушается «сплошность» среды);
- уравнение состояния – уравнение математической физики, которое «порождает» соответствующие функции или матрицы Грина;
- понятие функции Грина, как правило, связано с частным решением уравнений математической физики, которые характеризуются наличием вторых частных производных;
- дивергенция ( $div$ ) – дифференциальный оператор, отображающий векторное поле на скалярное, который определяет насколько расходится входящее и исходящее из малой окрестности данной точки поле;

- градиент (*grad*) – вектор, своим направлением указывающий направление наискорейшего возрастания некоторой величины, значение которой меняется от одной точки пространства к другой, а по величине равный быстроте роста этой величины в этом направлении;
- ротор или вихрь (*rot*) – векторный дифференциальный оператор над векторным полем.

### *Функция Грина в контексте обработки визуальной информации*

Для решения задач, связанных с обработкой изображения достаточно ограничиться рассмотрением линейных дифференциальных уравнений в частных производных с соответствующими источниками в правой части. Примером таких уравнений могут являться: скалярные уравнения Пуассона и Гельмгольца и векторное уравнение Ляме [4].

Источники, в которых нарушается «сплошность» среды, представляют собой обобщенные функции с локальными носителями. С представлением этих функций удобно использовать символическую дельта-функцию Дирака. В силу линейности используемых уравнений источники (особые точки) общего вида можно представить, как суперпозицию точечных источников. Источники можно разделить на три основных типа: монополи, диполи и квадруполи.

В случае построения поля на основе уравнения Ляме источники будут типа квадруполи, т. к. поле определяется более высокими производными от функции Дирака. Квадруполь можно рассматривать как совокупность двух одинаковых диполей с равными по величине и противоположными по направлению дипольными моментами, расположенных на некотором расстоянии друг от друга. Диполь общего вида можно разложить на диполь с осью вдоль оси  $x$  и на диполь с осью вдоль оси  $y$  (рис. 1). Поле диполя в месте нахождения источников претерпевает разрыв вместе со всеми производными. В остальных точках поле диполя является непрерывным. Очевидно диполи или совокупности диполей (квадруполь) идеально подходят для моделирования точек, в окрестностях которых имеют место резкие перепады градации цветности. Чтобы выразить поле диполя (квадруполя) достаточно взять от функции Грина адекватную производную.

В реальных изображениях, источники образуют линии разреза, разделяющие цветовые зоны. Совокупность этих линий образует абрис рисунка. Суммарное поле источников представляет собой изображение.

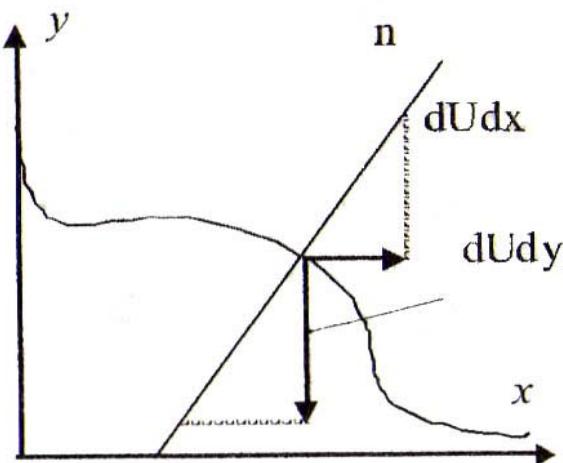


Рис. 1. Разложение диполя с произвольной ориентацией на два диполя, один из которых ориентирован вдоль оси  $x$ , а другой – вдоль оси  $y$

### *Методика выделения особых точек из изображения*

Рассмотрим на поле размером  $N \times M$  изображение, которое пусть определяется для определенности тремя цветовыми плоскостями, например  $R, G, B$ . Пусть в каждой цветовой плоскости во всех пикселях значение градации цвета задается значением от 0 до 255 (обычный BMP формат).

Будем рассматривать эти значения как три скалярных функции, определенные в прямоугольнике  $N \times M$ :

$$U_i(x, y), \text{ где } 0 < x < N, 0 < y < M, i = 1, 2, 3, \dots$$

$U_i(x, y)$  – непрерывные функции кроме конечного числа особых точек, в которых имеют место скачки градаций цветности. Принадлежность пикселя к особой точке определяется по превышению перепада градаций цветности в его окрестности некоторого выбранного порога.

В качестве уравнений состояния можно выбирать уравнения математической физики, характеризуемые вторыми производными (такие скачки могут генерировать источники типа диполь) или третьими производными (источники типа квадруполь).

$$L_i(U_i(x, y)) = f_i(x, y),$$

где  $f_i(x, y)$  – функция распределения источников типа диполей (квадрупольей);  $L_i$  – дифференциальные соотношения, соответствующие выбранному уравнению состояния.

Используя функцию Грина, поле особых точек (частное решение) можно найти по следующей формуле:

$$u(\vec{x}) = \int_{\Omega} G'(\vec{x}, \vec{x}_0) \cdot f(\vec{x}_0) d\vec{x}_0,$$

где  $G'(\vec{x}, \vec{x}_0)$  – производная от функции Грина по нормали к контуру,  $\vec{x}$  – вектор, определяющий текущие координаты в плоскости изображения,  $\vec{x}_0$  – вектор определяющий координаты особых точек (источников);  $f(\vec{x}_0)$  – функция распределения производных по  $x$  и  $y$  в особых точках.

### *Полевая модель на основе уравнения Ляме*

Уравнение Ляме описывает распространение продольных и сдвиговых волн в упругой изотропной среде. Уравнение является векторным и в двухмерном случае имеет следующий вид:

$$\mu \Delta \vec{u} + (\lambda + \mu) \operatorname{grad}(\operatorname{div} \vec{u}) - \rho \frac{d^2 \vec{u}}{dt^2} = 0, \quad (1)$$

где  $\mu$  и  $\lambda$  – коэффициенты Ляме,  $\rho$  – плотность среды,  $\vec{u} = \vec{u}(x, y, t)$  – вектор смещения среды.

Вектор смещения среды без нарушения общности можно представить, как

$$\vec{u} = \vec{U}(x, y) \exp(j\omega t).$$

Уравнение (1) после подстановки этого выражения примет вид:

$$\mu \Delta \vec{U} + (\mu + \lambda) \operatorname{grad}(\operatorname{div} \vec{U}) + \omega^2 \rho \vec{U} = 0. \quad (2)$$

Согласно теореме разложения Гельмгольца [1], если в каждой точке векторного поля определены ротор и дивергенция (т. е. являются непрерывными), то данное векторное поле можно представить в виде суммы безвихревого поля (ротор равен нулю) и вихревого (соленоидального) поля (дивергенция равна нулю). Решение однородного уравнения Ляме для неограниченного пространства, безусловно, имеет в каждой точке вектор и дивергенцию и поэтому может быть разложено на указанные поля. При этом роль безвихревого поля играет поле, образованное совокупностью продольных волн  $\vec{U}_l$  ( $\operatorname{rot} \vec{U}_l = 0$ ), а роль соленоидального поля – совокупность сдвиговых волн  $\vec{U}_t$  ( $\operatorname{div} \vec{U}_t = 0$ ):  $\vec{U} = \vec{U}_l + \vec{U}_t$ .

Подставляя в (2) сумму  $\vec{U}_l + \vec{U}_t$  и учитывая, что  $\operatorname{grad}(\operatorname{div} \vec{v}) = \Delta \vec{v} + \operatorname{rot}(\operatorname{rot} \vec{v})$ , получаем

$$(2\mu + \lambda) \Delta \vec{U}_l + \mu \Delta \vec{U}_t + \omega^2 \rho \vec{U}_l + \omega^2 \rho \vec{U}_t = 0.$$

Разделив левую часть последнего выражения на переменную  $c_t^2$  получим

$$\frac{c_l^2}{c_t^2} \Delta \vec{U}_l + \Delta \vec{U}_t + k_t^2 \vec{U}_l + k_t^2 \vec{U}_t = 0, \quad (3)$$

где  $k_t = \frac{\omega}{c_t^2}$  – волновое число для сдвиговых волн,  $c_t^2 = \frac{(2\mu + \lambda)}{\rho}$  – скорость распространения продольных волн,  $c_t^2 = \frac{\mu}{\rho}$  – скорость распространения сдвиговых волн.

Применяя к обеим частям последнего равенства сначала операцию  $\text{rot}$ , а затем  $\text{div}$ , несложно получить два уравнения Гельмгольца (первое относительно продольных волн, второе относительно сдвиговых):

$$\Delta \vec{U}_l + k_l^2 \vec{U}_l = 0, \quad \Delta \vec{U}_t + k_t^2 \vec{U}_t = 0.$$

В первом уравнении учтено, что  $k_l^2 = \frac{\omega^2}{c_l^2} = \frac{k_t^2 c_t^2}{c_l^2}$ .

Говоря другими словами, уравнение Ляме можно свести к двум векторным уравнениям Гельмгольца, на решения которых накладываются дополнительные условия: в виде равенства нулю соответственно ротора и дивергенции.

### *Разделение на безвихревое и соленоидальное поле*

Введём в правую часть векторного уравнения (4) два элементарных источника типа диполя, соответственно ориентированных вдоль оси  $x$  и вдоль оси  $y$ :

$$\frac{c_l^2}{c_t^2} \Delta \vec{U}_l + \vec{U}_t + k_t^2 \vec{U}_l + k_t^2 \vec{U}_t = \vec{i} A_x k_t^2 \delta'(x - x_0) \delta(y - y_0) + \vec{j} A_y k_t^2 \delta(x - x_0) \delta'(y - y_0), \quad (4)$$

где  $\vec{i}$  и  $\vec{j}$  – единичные вектора соответственно вдоль оси  $x$  и  $y$ ,  $x_0$  и  $y_0$  – координаты особой точки,  $A_x$  и  $A_y$  – коэффициенты, пропорциональные перепадам градаций цветности соответственно по  $x$  и  $y$ .

Наличие в правой части обобщенных функций не позволяет в рамках классической теоремы разложения Гельмгольца представить поле в виде суммы безвихревого и соленоидального полей. Физическая трактовка этого факта очевидна: источник, ориентированный, например, вдоль оси  $x$ , возбуждает вдоль нее продольные волны, а вдоль оси  $y$  – сдвиговые волны. Эти типы волн, распространяющиеся с разной скоростью, создают вокруг источника сложное поле.

Расщепим элементарный источник общего вида на два точечных источника, один из которых возбуждает «чистые» продольные волны, а другой – «чистые» сдвиговые волны. В этом случае частное решение уравне-

ния Ляме можно будет представить в виде суммы продольных и сдвиговых волн, независимо распространяющихся в неограниченном пространстве.

Поле двух диполей, один из которых ориентирован вдоль оси  $x$ , а другой – вдоль оси  $y$ , можно представить в виде:

$$U_j(x - x_0, y - y_0) = A_i(x_0, y_0)(G'_{ji}(x - x_0, y - y_0) + G'_{ij}(x - x_0, y - y_0)),$$

где

$$G'_{ij}(x - x_0, y - y_0) = \frac{i}{4\pi} \begin{bmatrix} k_t^2 \frac{\partial H_0^{(1)}(k_t r)}{\partial x} + \frac{\partial^3 H_0^{(1)}(k_t r)}{\partial x^3} & \frac{\partial^3 H_0^{(1)}(k_t r)}{\partial y^2 \partial x} \\ \frac{\partial^3 H_0^{(1)}(k_t r)}{\partial x^2 \partial y} & k_t^2 \frac{\partial H_0^{(1)}(k_t r)}{\partial y} + \frac{\partial^3 H_0^{(1)}(k_t r)}{\partial y^3} \end{bmatrix} - \quad (5)$$

решение первого векторного уравнения;  $r = \sqrt{(x - x_0)^2 + (y - y_0)^2}$ ,  $H_0^{(1)}(kr)$  – функция Ханкеля первого рода нулевого порядка,

$$G'_{ij}(x - x_0, y - y_0) = -\frac{i}{4\pi} \frac{c_t^2}{c_l^2} \begin{bmatrix} \frac{\partial^3 H_0^{(1)}(k_l r)}{\partial x^3} & \frac{\partial^3 H_0^{(1)}(k_l r)}{\partial y^2 \partial x} \\ \frac{\partial^3 H_0^{(1)}(k_l r)}{\partial x^2 \partial y} & \frac{\partial^3 H_0^{(1)}(k_l r)}{\partial y^3} \end{bmatrix} - \quad (6)$$

решение второго векторного уравнения,  $i$  и  $j$  пробегают значения 1, 2.

Функция Ханкеля  $H_0^{(1)}(kr)$  является функцией Грина для уравнения Гельмгольца. Поэтому ее подстановка в (8) обращает это соотношение в нуль во всей плоскости кроме особой точки.

Данный факт позволяет упростить выражения для диагональных компонент матрицы  $G'_{ij}(x - x_0, y - y_0)$ .

В результате эта матрица принимает следующий вид:

$$G'_{ij}(x - x_0, y - y_0) = \frac{i}{4\pi} \begin{bmatrix} -\frac{\partial^3 H_0^{(1)}(k_t r)}{\partial x \partial y^2} & \frac{\partial^3 H_0^{(1)}(k_t r)}{\partial y^2 \partial x} \\ \frac{\partial^3 H_0^{(1)}(k_t r)}{\partial x^2 \partial y} & -\frac{\partial^3 H_0^{(1)}(k_t r)}{\partial y \partial x^2} \end{bmatrix}. \quad (7)$$

Выражения (5), (6), (7) представляют собой полевую модель на основе векторного уравнения Ляме. Для соленоидального (9) поля все компоненты выражаются через смешанные производные. В этом случае, если одна производная (перепад градации цветности) существенно больше другой, то значение вихревой компоненты будет давать значительно меньший вклад в поле, чем безвихревая компонента. Например, если граница между двумя областями цветности идет по вертикали (горизонтали), то производная по  $y(x)$  равна нулю. С другой стороны, если производные по  $x$  и  $y$  имеют приближенно равные значения, то, как видно из (9), компонента соленоидального поля также стремится к нулю. Другие комбинации соотношений пе-

репадов цветности в контексте дискретной полевой модели не просматривается. Поэтому полевую векторную модель можно упростить, отбросив вихревую часть модели.

### Выходы

Модель Ляме по сравнению, например, с моделью Пуассона обладает двумя преимуществами:

- усложнение математической модели привело к упрощению структуры физического поля, т. к. в отличие от модели на основе уравнения Пуассона здесь отсутствует вихревая составляющая;

- поле удовлетворяет во всех точках соотношению  $\text{rot} = 0$ .

Полевая модель Ляме является перспективной моделью и может быть использована в обработке изображений для достижения нового качества обработки.

### Результаты построения поля особых точек на основе уравнения

0,00	0,00	0,00	0,00	-0,00	-0,00	-0,00	-0,00	-0,00
0,00	0,01	0,01	0,01	-0,02	-0,01	-0,01	-0,01	-0,00
-0,00	-0,01	-0,01	-0,01	0,01	0,01	0,01	0,01	0,00
-0,00	-0,00	-0,00	0,00	-0,01	-0,00	0,00	0,00	0,00
-0,00	-0,00	-0,01	-0,02	-0,09	0,02	0,01	0,00	0,00
0,00	0,00	0,01	0,02	0,09	-0,02	-0,01	-0,00	-0,00
0,00	0,00	0,00	-0,00	0,01	0,00	-0,00	-0,00	-0,00
0,00	0,01	0,01	0,01	-0,01	-0,01	-0,01	-0,01	-0,00
-0,00	-0,01	-0,01	-0,01	0,02	0,01	0,01	0,01	0,00
-0,00	-0,00	-0,00	-0,00	0,00	0,00	0,00	0,00	0,00

Рис. 2. Поле диполя в матричном виде (с осью вдоль оси у при  $Win = 5$ )

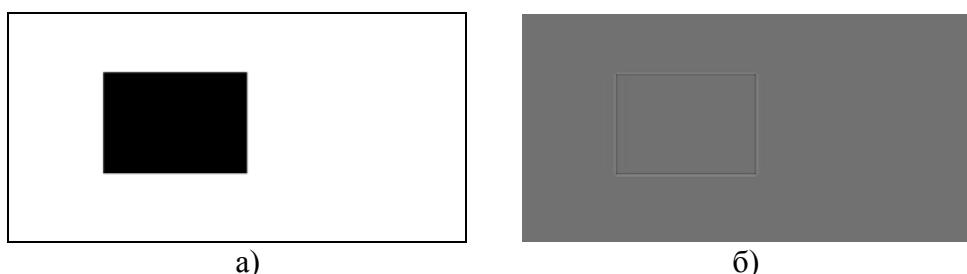


Рис. 3. Результаты построения поля особых точек для цветного полутонового изображения (объем 628 кб) под кодовым названием квадрат.bmp: исходное изображение (а); поле особых точек, порог = 1,  $Win = 16$  (б)

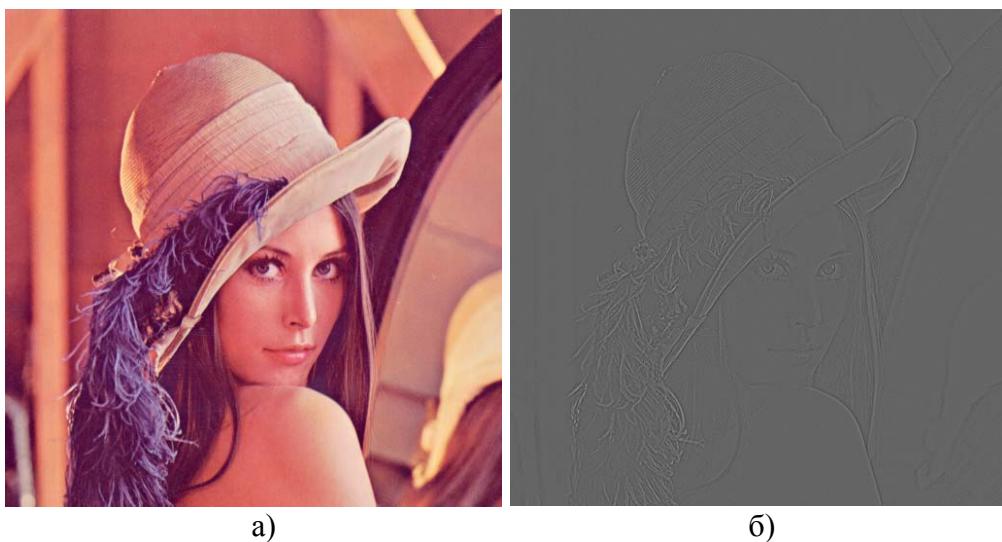


Рис. 4. Результаты построения поля особых точек для эталонного цветного полутонового изображения (объем 768 кб) под кодовым названием lena.bmp: исходное изображение (а); поле особых точек, порог = 1,  $Win = 16$  (б)

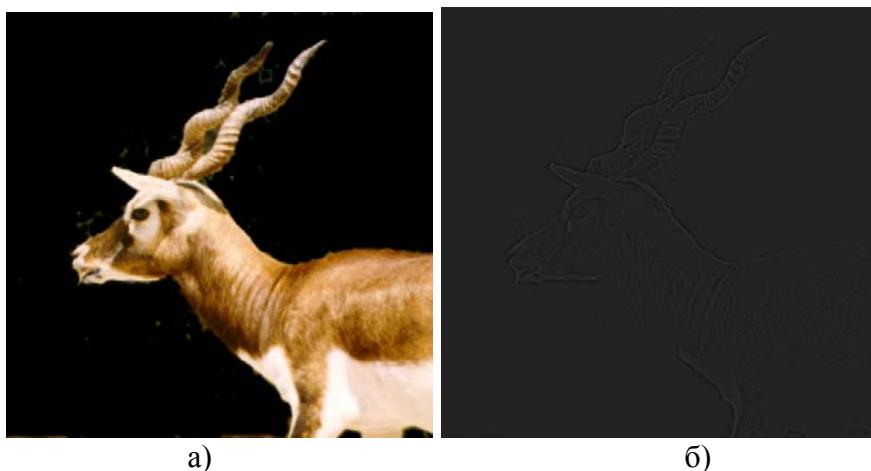


Рис. 5. Результаты построения поля особых точек для цветного полутонового изображения (объем 768 кб) под кодовым названием blackbuck.bmp: исходное изображение (а); поле особых точек, порог = 1,  $Win = 16$  (б)

### Список используемых источников

1. Теоретическая Физика. Т. 8. Теория упругости / Л. Д. Ландау, Е. М. Лифшиц. – М. : Наука, 1967. – 248 с.
2. Выделение контуров изображений на основе функции Грина / Ю. Ф. Болтов // Телекоммуникации. – 2009. – № 5. – С. 27–32.
3. Условия бездисперсионного распространения волн упругих деформаций в твердом волноводе с прямоугольным сечением / Ю. Ф. Болтов, И. Н. Григорьев // Акустический журнал. – 1978. – Т. XXIV. Вып. 3. – С. 413–415.

4. Обработка визуальной информации на основе ее представления в виде скалярных или векторных полей: концепция, математические модели и алгоритмы: монография / Ю. Ф. Болтов. – СПб. : СПбГУТ, 2010. – 183 с.

*Статья представлена научным руководителем канд. техн. наук, доцентом Ю. Ф. Болтовым.*

**УДК 621.315.2**

**П. А. Чаймарданов (студент группы МТ-03 СПбГУТ)**

## **ТЕОРЕТИЧЕСКОЕ ИССЛЕДОВАНИЕ КАБЕЛЬНЫХ ЦЕПЕЙ С БИМЕТАЛЛИЧЕСКИМИ ПРОВОДНИКАМИ**

Основным элементом электрического кабеля связи являются проводящие жилы, которые традиционно изготавливаются из меди или алюминия. По электрической проводимости медь превосходит все другие материалы, за исключением серебра, что позволяет обеспечивать минимальные габаритные размеры кабелей и проводов. Однако в кабельной промышленности используются и биметаллические проводники. Наиболее распространены проводники с сердечником из алюминия или стали и оболочкой из меди, получаемые с использованием технологии плакирования. Известны также биметаллические проводники с медным сердечником и оболочкой из никеля или серебра.

Одно из основных применений биметаллического проводника – высокочастотные кабельные изделия. За счет поверхностного эффекта высокочастотный сигнал передается по внешней оболочке проводника, а повышенное электрическое сопротивление внутренней жилы не имеет принципиального значения.

В последние годы на рынке появились относительно дешевые LAN кабели категории 5е с биметаллическими проводниками из алюминия или стали, покрытыми медью. Относительно соответствия параметров этих изделий международным стандартам у специалистов нет единого мнения [1]. Поэтому актуальной задачей является анализ параметров этих кабелей, который позволит подтвердить возможность их использования в сетях Ethernet.

В данной работе получены выражения для расчета распределения электромагнитного поля пары биметаллических проводников ([рис. 1](#)) и полного сопротивления одного проводника с учетом поверхностного эффекта и эффекта близости. Предположим, что сердечник проводника изготовлен из материала с удельным сопротивлением  $\rho_1$  и магнитной проница-

емостью  $\mu_1$ , а оболочка – из материала с удельным сопротивлением  $\rho_2$  и магнитной проницаемостью  $\mu_2$ .

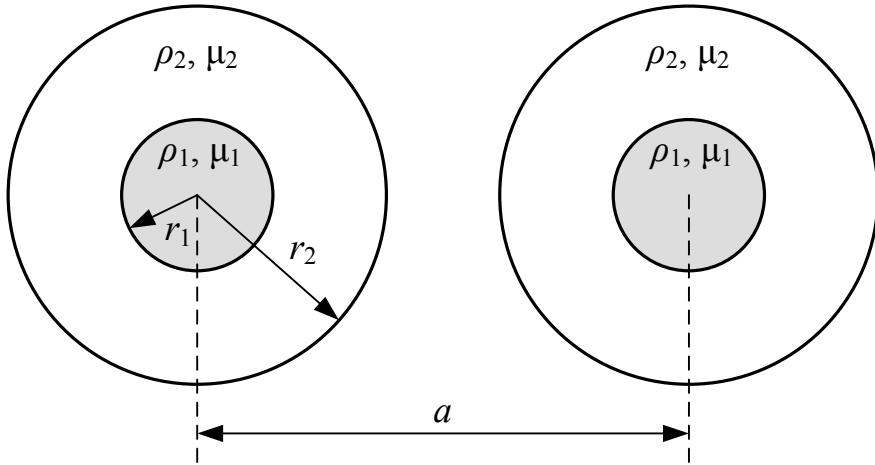


Рис. 1. Пара биметаллических проводников

Поскольку каждый из рассматриваемых проводников обладает осевой симметрией, будем пользоваться цилиндрической системой координат. Учитывая, что ток в проводнике протекает только вдоль его оси (оси z) можно утверждать, что не равными нулю составляющими электромагнитного поля будут  $E_z$ ,  $H_r$  и  $H_\phi$ .

Уравнения Максвелла в цилиндрических координатах для биметаллического проводника имеют вид [2]:

$$\begin{aligned} H_r &= -\frac{1}{i\omega\mu r} \frac{\partial E_z}{\partial\varphi}, & H_\phi &= \frac{1}{i\omega\mu} \frac{\partial E_z}{\partial r}, \\ \frac{\partial H_\phi}{\partial r} + \frac{H_\phi}{r} - \frac{1}{r} \frac{\partial H_r}{\partial\varphi} &= \frac{E_z}{\rho}, \end{aligned} \quad (1)$$

где,  $\omega$  – круговая частота,  $i$  – мнимая единица,  $\mu$  и  $\rho$  – относительная магнитная проницаемость и удельное электрическое сопротивление среды, определяемые следующим образом:

$$\mu = \begin{cases} \mu_1, & 0 < r \leq r_1 \\ \mu_2, & r_1 \leq r \leq r_2 \end{cases}, \quad \rho = \begin{cases} \rho_1, & 0 < r \leq r_1 \\ \rho_2, & r_1 \leq r \leq r_2 \end{cases}. \quad (2)$$

Из (1)–(2) можно получить следующее уравнение для  $E_z(r)$ :

$$\frac{\partial^2 E_z}{\partial r^2} + \frac{1}{r} \frac{\partial E_z}{\partial r} + \frac{1}{r^2} \frac{\partial^2 E_z}{\partial\varphi^2} - ik^2 E_z = 0. \quad (3)$$

$$\text{где } k = \begin{cases} \sqrt{\omega\mu_1/\rho_1}, & 0 < r \leq r_1 \\ \sqrt{\omega\mu_2/\rho_2}, & r_1 \leq r \leq r_2 \end{cases}.$$

Поле в окружающем проводники диэлектрике также можно описать уравнением (3), считая, что  $k = 0$ . Решение (3) имеет вид [3]:

$$E_z(r) = \begin{cases} \sum_{n=0}^{\infty} A_{1,n} I_n(m_1 r) \cos n\varphi, & 0 < r \leq r_1 \\ \sum_{n=0}^{\infty} (A_{2,n} I_n(m_2 r) + B_{2,n} K_n(m_2 r)) \cos n\varphi, & r_1 \leq r \leq r_2 \\ F_0 \ln(r) + C_0 + \sum_{n=1}^{\infty} (F_n r^n + C_n r^{-n}) \cos n\varphi, & r > r_2 \end{cases} \quad (4)$$

Из (4) и (1) получаем для  $H_\varphi(r)$ :

при  $0 < r \leq r_1$

$$H_\varphi(r) = \frac{1}{m_1 \rho_1} \left[ A_{1,0} I_1(m_1 r) + \frac{1}{2} \sum_{n=1}^{\infty} A_{1,n} (I_{n-1}(m_1 r) + I_{n+1}(m_1 r)) \cos n\varphi \right],$$

при  $r_1 < r \leq r_2$

$$H_\varphi(r) = \frac{1}{m_2 \rho_2} \left[ A_{2,0} I_1(m_2 r) - B_{2,0} K_1(m_2 r) + \frac{1}{2} \sum_{n=1}^{\infty} [A_{2,n} (I_{n-1}(m_2 r) + I_{n+1}(m_2 r)) - B_{2,n} (K_{n-1}(m_2 r) + K_{n+1}(m_2 r))] \cos n\varphi \right],$$

при  $r > r_2$

$$H_\varphi(r) = \frac{F_0}{i\omega\mu_d r} + \frac{1}{i\omega\mu_d} \sum_{n=1}^{\infty} [n(F_n r^{n-1} - C_n r^{-n-1}) \cos n\varphi]. \quad (5)$$

В (4) и (5)  $A_{1,n}$ ,  $A_{2,n}$ ,  $B_{2,n}$ ,  $C_n$ ,  $F_n$  – постоянные интегрирования,  $I_n$  – модифицированная функция Бесселя первого рода  $n$ -го порядка,  $K_n$  – модифицированная функция Бесселя второго рода  $n$ -го порядка,  $m_1 = \sqrt{i}k_1$ ,  $m_2 = \sqrt{i}k_2$ ,  $k_1 = \sqrt{\omega\mu_1/\rho_1}$ ,  $k_2 = \sqrt{\omega\mu_2/\rho_2}$ ,  $\mu_d$  – относительная магнитная проницаемость изоляции.

Для определения постоянных интегрирования воспользуемся граничными условиями, заключающимися в непрерывности  $E_z(r)$  и  $H_\varphi(r)$  при  $r = r_1$  и  $r = r_2$ :

$$\begin{aligned} A_{1,n} &= \frac{i2nF_n r_2^n}{-z_n \omega \mu_d r_2 + i n h_n}, & C_n &= -F_n r_2^{2n} \left( \frac{z_n \omega \mu_d r_2 + i n h_n}{z_n \omega \mu_d r_2 - i n h_n} \right) \\ A_{2,n} &= A_{1,n} \frac{m_1 p_1 I_n(m_1 r_1) (K_{n+1}(m_2 r_1) + K_{n-1}(m_2 r_1)) + m_2 p_2 K_n(m_2 r_1) (I_{n+1}(m_1 r_1) + I_{n-1}(m_1 r_1))}{m_1 p_1 (K_n(m_2 r_1) (I_{n+1}(m_2 r_1) + I_{n-1}(m_2 r_1)) + (K_{n+1}(m_2 r_1) + K_{n-1}(m_2 r_1)) I_n(m_2 r_1))}, \\ B_{2,n} &= -A_{1,n} \frac{m_2 p_2 I_n(m_2 r_1) (I_{n+1}(m_1 r_1) + I_{n-1}(m_1 r_1)) - m_1 p_1 I_n(m_1 r_1) (I_{n+1}(m_2 r_1) + I_{n-1}(m_2 r_1))}{m_1 p_1 (K_n(m_2 r_1) (I_{n+1}(m_2 r_1) + I_{n-1}(m_2 r_1)) + (K_{n+1}(m_2 r_1) + K_{n-1}(m_2 r_1)) I_n(m_2 r_1))}. \end{aligned} \quad (6)$$

В выражениях (6) использованы обозначения  $h_n = \frac{A_{2,n} I_n(m_2 r_2) + B_{2,n} K_n(m_2 r_2)}{A_{1,n}}$ ,  
 $z_n = \frac{1}{2m_2 p_2} \frac{(A_{2,n} (I_{n+1}(m_2 r_2) + I_{n-1}(m_2 r_2)) - B_{2,n} (K_{n+1}(m_2 r_2) + K_{n-1}(m_2 r_2)))}{A_{1,n}}$ .

Выражение (6) позволяет рассчитать постоянные интегрирования  $A_{1,n}$ ,  $A_{2,n}$ ,  $B_{2,n}$ ,  $C_n$ , если известны постоянные интегрирования  $F_n$ . Найдем их. Запишем выражение (5) для напряженности магнитного поля в диэлектрике (при  $r \geq r_2$ ) с учетом (6) и закона полного тока:

$$H_\varphi(r) = \frac{I}{2\pi r} + \frac{1}{i\omega\mu_d} \sum_{n=1}^{\infty} \left[ nF_n r^{n-1} \left( 1 + \left(\frac{r_2}{r}\right)^{2n} \chi_n \right) \cos n\varphi \right], \quad (7)$$

где  $\chi_n = \frac{z_n \omega \mu_d r_2 + i n h_n}{z_n \omega \mu_d r_2 - i n h_n}$ .

Сравнивая (7) и (5) получим:

$$F_0 = \frac{i\omega\mu_d I}{2\pi}. \quad (8)$$

Напряженность магнитного поля (7) можно разложить на две составляющие –  $H_{\varphi 1}$ , обусловленную протеканием тока в 1-м проводнике пары,  $H_{\varphi 2}$ , обусловленную протеканием тока во 2-м проводнике пары:

$$H_{\varphi 1}(r) = \frac{I}{2\pi r} + \sum_{n=1}^{\infty} \frac{nF_n r_2^{2n} \chi_n}{i\omega\mu_d r^{n-1}} \cos n\varphi, \quad H_{\varphi 2}(r) = \sum_{n=1}^{\infty} \frac{nF_n r^{n-1}}{i\omega\mu_d} \cos n\varphi. \quad (9)$$

Так как проводники идентичны, при  $\varphi = 0$  должно выполняться условие:  $H_{\varphi 1}(r - a) = H_{\varphi 2}(r)$ , где  $a$  – расстояние между проводниками пары.

$$\sum_{n=1}^{\infty} nF_n r^{n-1} = \frac{iIw\mu}{2\pi a \left(1 - \frac{r}{a}\right)} + \sum_{n=1}^{\infty} \frac{nF_n r_2^{2n} \chi_n}{\left(1 - \frac{r}{a}\right)^{n+1} a^{n+1}}. \quad (10)$$

Разлагая (15) по степеням  $r$  и приравнивая коэффициенты при одинаковых степенях, получим:

$$nF_n r^n \cong \frac{iIw\mu}{2\pi} \varepsilon^n + \sum_{j=1}^{\infty} \frac{jF_j r_2^{2j} \chi_j \varepsilon^n}{a^j} \frac{(j+n-1)!}{j!(n-1)!}. \quad (11)$$

Выражение (11) представляет собой систему уравнений, решение которой позволяет определить все переменные интегрирования  $F_n$ . Трудность заключается в том, что и уравнений и неизвестных бесконечно много, поэтому при проведении расчетов их число придется ограничить. Минимально необходимое число определяемых переменных интегрирования  $F_n$  выбирается, исходя из заданной точности расчета.

Для определения полного сопротивления  $Z$  биметаллического проводника воспользуемся теоремой Умова-Пойтинга:

$$I^2 Z = \int_0^{2\pi} E_z(r_2) H_\varphi^*(r_2) r_2 d\varphi, \quad (12)$$

где  $I$  – ток в проводнике. С учетом (4) и (5) из (12) получим:

$$I^2 Z = \frac{i2\pi F_0 F_0^* \chi_0}{w\mu} + \frac{i\pi}{w\mu} \sum_{n=1}^{\infty} nF_n F_n^* r_2^{2n} (1 - \chi_n)(1 + \chi_n^*). \quad (14)$$

Из (14) можно получить:

$$R = Re(Z) = -\mu f Im(\chi_0) + \frac{\pi}{I^2 w^2 \mu} \sum_{n=1}^{\infty} 2nF_n F_n^* r_2^{2n} Im(\chi_n), \quad (15)$$

$$L = Im(Z) = \frac{\mu}{2\pi} Re(\chi_0) + \frac{\pi}{I^2 w^2 \mu} \sum_{n=1}^{\infty} nF_n F_n^* r_2^{2n} (1 - Re(\chi_n)^2 - Im(\chi_n)^2). \quad (16)$$

На рисунке 2 представлены результаты расчета зависимостей от частоты погонного сопротивления и погонной индуктивности алюмомедного цилиндрического проводника симметричной пары. Расчет проведен по выражениям (15) и (16) с учетом (6) и (11) при следующих параметрах  $r_2 = 0,2555$  мм, толщина медного слоя 0,05 мм,  $a = 1,022$  мм. Для сравнения на графиках приведены аналогичные зависимости для симметричных пар из медных и алюминиевых проводников радиуса 0,2555 мм при расстоянии между ними, равном 1,022 мм.

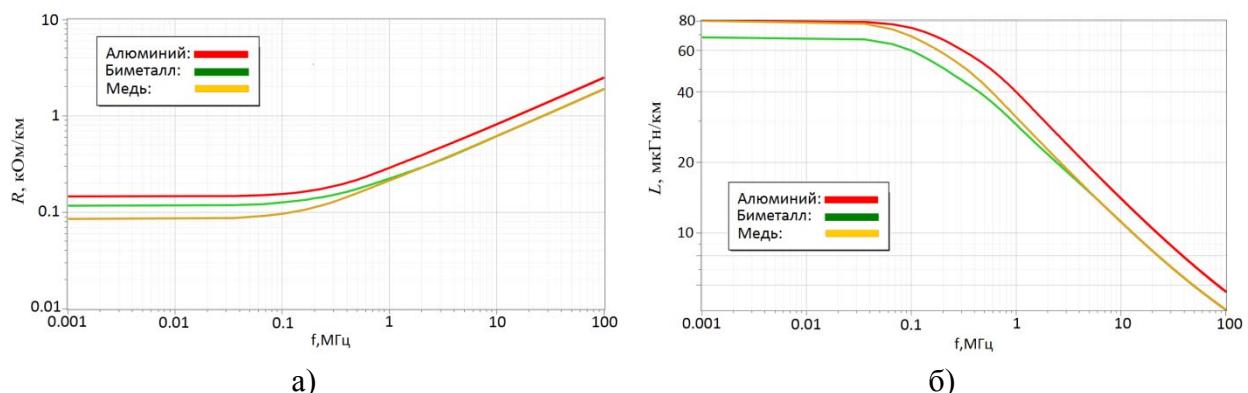


Рис. 2. Погонные сопротивление (а) и индуктивность (б) биметаллического (алюмомедного), медного и алюминиевого проводников

Полученные в работе соотношения являются частью математической модели, разработанной для новой виртуальной лабораторной установки по исследованию первичных и вторичных параметров двухпроводной кабельной цепи.

#### Список использованных источников

1. Цена не аргумент [Электронный ресурс] / О. А. Лучак // Сети и телекоммуникации – 2007. – № 10. – Режим доступа: <http://daily.sec.ru/2008/10/14/O-Luchak-TSene-ne-argument.html> (Дата обращения 20.05.2014).
2. Теория кабелей связи / В. Н. Кулешов. – М. : Связьиздат, 1950. – 420 с.
3. К вопросу о расчете распределения электромагнитного поля и полного сопротивления биметаллического проводника [Электронный ресурс] / М. С. Былина, П. А. Чаймарданов // III Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сб. науч. ст. – СПб. СПбГУТ, 2014. – Режим доступа: <http://itt.sut.ru/index.php/confsut2014> (Дата обращения 20.05.2014).

*Статья представлена научным руководителем канд. техн. наук, доцентом М. С. Былиной.*

УДК 004.056.57

**И. Р. Шалин (студент группы СП-91 СПбГУТ)**

**РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ  
ДЛЯ ПРОВЕРКИ РЕШЕНИЙ ЗАДАЧ  
ПО ПРОГРАММИРОВАНИЮ**

При проведении практических занятий по программированию в ВУЗе перед преподавателем стоит очень трудоемкая задача – проверить работу программ каждого студента. При этом оценка программы состоит из синтаксического анализа исходных текстов программы, стиля написания программы, корректности выполнения задачи и предостережение от потенциально возможных ошибок. Большую часть этих задач можно автоматизировать. Именно данной теме посвящена эта статья.

*Преимущества автоматизации проверки программ*

- Оптимизация времени проверки программы. Проверка программного кода одного студента или программ целой группы будет занимать примерно одно время.
- У преподавателя остается больше времени на работу со студентами и передачу опыта. Это достигается за счет перекладывания рутинной работы на программу, что экономит большое количество времени.
- Повышение качества проверки программы. Это достигается путем многокритериальной оценки, итогом которой является полный отчет о результате работы программы. Отчет содержит данные о времени выполнения, потреблении памяти, корректности решения задачи и т. д.
- Сбор статистики. К результатам выполнения студенческих программ можно вернуться через длительное время. Это создает огромный потенциал по двум направлениям: улучшение качества существующих задач и оценке вероятность копирования программ студентами друг у друга. Так как коды программ хранятся в системе проверки, мы всегда можем сравнить программы студентов и выявить недобросовестных.

Перед началом разработки собственного решения были проанализированы уже существующие решения в данной области:

1. МФТИ, МГУ – система проверки задач eJudge для проведения олимпиад.
2. Саратовский государственный университет – проект Codeforces.
3. Университет Гарварда – система онлайн обучения Harvard Extension School.

После оценки существующего программного обеспечения было принято решение писать свою систему проверки программ на основе веб-приложения. Это дает ряд преимуществ, а именно:

1. Веб-приложение доступно из любой точки мира в любой момент времени при наличии сети интернет.

2. Достигается большая гибкость в настройке системы проверки в зависимости от потребностей преподавателей.

3. Мы можем анализировать синтаксическую корректность кода, наличие потенциальных проблем в коде, соответствие кода общепринятым стандартам написания кода на определенном языке.

4. Ведение собственной базы задач и статистики.

Приложение состоит из трех логических частей:

1. Сервер приложения

2. Система проверки задач.

3. База данных.

Это позволит в будущем легко масштабировать систему и гибко ее настраивать в зависимости от нагрузки и требованиям к производительности и отказоустойчивости.

Сервер приложения является связующим звеном между пользователем, базой данных и системой проверки. По этой причине на эту часть системы возлагается наибольшая ответственность и требования по функциональности и производительности. Исходя из высоких требований к системе, было принято решение реализовать сервер приложения на фреймворке Node.js [1], что имеет несколько весомых преимуществ перед PHP:

1. Node.js позволяет писать серверную часть на языке программирования JavaScript. Это значит, что все приложение можно написать используя только один язык программирования – JavaScript.

2. Асинхронность. Операции ввода/вывода в Node.js основаны на библиотеке libevent, что делает эти операции асинхронными и неблокирующими и как следствие – быстрыми.

3. Node.js позволяет написать совместимый с ней модуль на языке C++, и работать с ним будто он написан на JavaScript. Это позволяет оптимизировать узкие места в приложении, переписав небольшую часть кода на более производительный язык.

4. Node.js производительнее PHP за счет того, что PHP – это скриптовый язык. При каждом запросе скрипт интерпретируется и компилируется заново. Node.js же создает приложение, которое однажды компилируется, запускается и работает.

В качестве базы данных использована документно-ориентированная база данных MongoDB [2]. Это позволило получать данные из базы без преобразований, а также писать запросы в родном для JavaScript формате – в формате JSON.

Система проверки выполняет непосредственно компиляцию и запуск кода в изолированной от основной системы среде. Безопасность достигается за счет четкого разграничения прав и встроенного инструмента в Linux – chroot. Благодаря этому, программа студента полностью контролируется родительской системой, и пресекаются попытки израсходовать ресурсы компьютера или вывести из строя систему.

При разработке системы тестирования возникли технические трудности. Дело в том, что в единицу времени система должна тестировать только одну программу пользователя. Но ввиду асинхронной архитектуры приложения была возможность отправить на проверку больше одной задачи, и тогда между проверяемыми задачами начиналась борьба за ресурсы. Это приводило к искажению результатов отчета о производительности и выполнении программ.

Решение было найдено в реализации синхронной очереди, которая получала асинхронно присылаемый от пользователей код и синхронно передавала его системе проверки задач.

Так же следует отметить, что система была написана при помощи IDE WebStorm. Этот инструмент позволяет контролировать соответствие кода общепринятым нормам, проводит синтаксический анализ кода на лету и является одним из многих инструментов, корректно работающих с JavaScript.

Сама система была развернута на виртуальной машине в ЦОД. Во время проведения конкурса по программированию для отказоустойчивости система была развернута на трех виртуальных машинах. Система легко горизонтально масштабируется.

В будущем планируется реализовать следующие улучшения:

- Увеличение количества поддерживаемых языков.
- Личный кабинет пользователя для просмотра статистики решенных задач.
- Разработка интеллектуальной системы подбора задач для онлайн обучения языкам программирования.

#### **Список используемых источников**

1. Node.js docs. – URL: <http://nodejs.org/api/> (Дата обращения 26.05.2014).
2. MongoDB docs. – URL: <http://docs.mongodb.org/manual/> (Дата обращения 26.05.2014).

*Статья представлена научным руководителем, доцентом О. Б. Петровой.*

УДК 681.3.07

**Д. А. Шаньгина (студентка группы СП-02 СПбГУТ)**

## **РАЦИОНАЛЬНЫЙ АГЕНТ, РЕШАЮЩИЙ ЗАДАЧУ ПОИСКА В ТЕРМИНАХ ЗАДАННЫХ МЕСТОПОЛОЖЕНИЙ И ПЕРЕХОДОВ ПО СВЯЗЯМ МЕЖДУ НИМИ**

### *Введение*

В настоящее время концепция рациональности применяется все чаще к самым разным агентам, действующим практически в любой среде. В статье показано, как можно реализовать агента, работающего на основе цели. Агент формулирует цель и задачу, затем ищет последовательность действий, приводящих к решению этой задачи, и, наконец, выполняет эту последовательность действий. В данном случае задачей агента является поиск маршрута.

### *Общие понятия*

Агент – это всё, что может воспринимать окружающую среду через датчики и реагировать на события эффекторами/исполнительными устройствами. Для каждой возможной последовательности результатов рациональный агент должен выбрать действие, которое предполагает максимизацию эффективности. Вывод делается на основе накопленной истории восприятий, а также встроенной базы знаний, если таковая имеется. В данной статье для наглядности речь пойдёт о простейших агентах [1].

Для реального агента архитектура ПО может иметь различные уровни:

- реактивный («восприятие-действие»);
- исполнительный (посредник);
- алгоритмический (вырабатывает решение сложных задач с использованием различных методов планирования).

Для принятия решения используются различные модели. Они либо заранее подготовлены, либо формируются в процессе обучения и самообучения агента на основе имеющихся данных и хранения истории.

Архитектура рационального агента представлена на [рисунке 1](#).

Как видно, информация воспринимается агентом из окружающей среды с помощью сенсоров (датчиков) и анализируется в соответствии сложенными в программу критериями. Когда агент определил состояние среды, он обращается к базе правил, чётко описывающих действия агента в той или иной ситуации. В результате сопоставления правил и информации извне производится выбор действия и отправка сигнала эффекторам (манипуляторам, исполнительным устройствам).

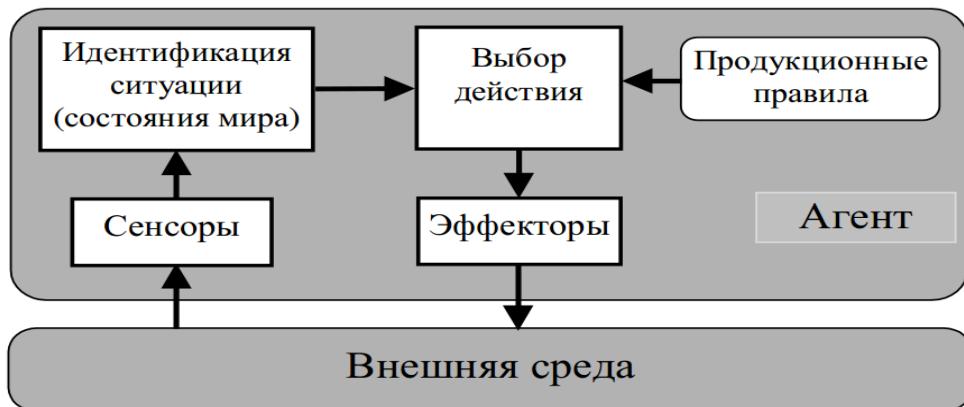


Рис. 1. Архитектура простейшего рационального агента

Рассмотрим агента, который решает поставленную задачу на основании стоящей перед ним цели. Для решения задачи агент должен определить последовательность действий, которые ведут его к желаемому состоянию. При этом агент должен обладать способностью максимизировать свои показатели производительности. Поэтому важным первым шагом является четкая формулировка цели с учетом текущей ситуации и показателями производительности агента.

Для данного случая цель представляет собой пространство состояний, в которых достигается такая цель. Это и есть формализованная структура для представления проблемы.

Пространство состояний можно представить как ориентированный граф, узлы графа – проблемные ситуации, дуги – возможные действия. Известен начальный узел и целевое состояние. Задачу оптимизации можно смоделировать, назначая дугам определенные стоимости.

Задача агента – это процесс определения того, какие действия и состояния следует рассматривать с учетом поставленной цели. Допустим, агент хочет добраться из пункта А в пункт Б. Если в пункт Б ведёт не одна дорога, агент должен выбрать оптимальную (по стоимости).

### *Решение проблемы посредством поиска*

Есть много алгоритмов выбора пути. В данной статье рассматривается «поиск в глубину».

Агент приступает к работе в начальном состоянии. Необходимо иметь описание доступных действий агента из начального состояния. Обычно это называется функцией определения преемника. Начальное состояние и функция определения преемника, вместе взятые, неявно задают пространство состояний. Проверка цели позволяет определить, является ли данное конкретное состояние целевым состоянием.

Решением задачи является путь от начального состояния до целевого состояния. При этом для того, чтобы агент считался рациональным, реше-

ние должно быть оптимальным в соответствии с выбранным критерием. Для данного случая – это кратчайший путь.

### Поиск решения

Как уже было сказано, будет использоваться «поиск в глубину». В качестве языка программирования при моделировании на компьютере выбран язык логического программирования Пролог.

Идея состоит в том, чтобы найти решающий путь  $Res$  из заданной вершины  $B$  в некоторую целевую вершину, для этого необходимо:

- если  $B$  – это целевая вершина, то положить  $Res = [B]$ , или
- если для исходной вершины  $B$  существует вершина-преемник  $B1$ , такая, что можно провести путь  $Res1$  из  $B1$  в целевую вершину, то положить  $Res = [B | Res1]$ .

```
solve(B, [B]):-
    goal(B).
solve(B, [B | Res1]):-
    s(B, B1),
    solve(B1, Res1).
```

Эта программа и есть реализация «поиска в глубину». Каждый раз, когда алгоритму придется выбирать, какую вершину просмотреть, он будет обращаться к той вершине, которая находится дальше всех от исходной.

$s(X, Y)$  – пространство состояний, которое принимает истинное значение, если в данном пространстве состояний имеется допустимый переход из узла  $X$  в узел  $Y$ .

«Поиск в глубину» хорошо согласуется с рекурсивным стилем программирования, принятым в Прологе. Причина этого состоит в том, что, обрабатывая цели, пролог-система сама просматривает альтернативы именно в глубину [2].

«Поиск в глубину» часто работает хорошо, однако процедура  $solve$  может попасть в затруднительное положение. Для этого достаточно добавить дугу, ведущую из  $h$  в  $d$ , чтобы получился цикл (рис. 2). Очевидное усовершенствование программы поиска в глубину – добавление к ней механизма обнаружения циклов.

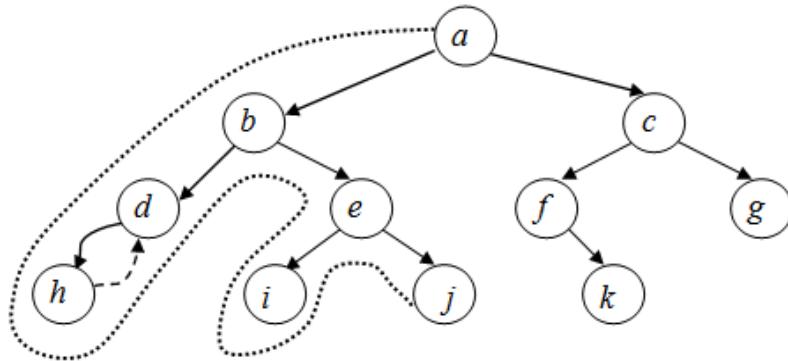


Рис. 2. «Поиск в глубину»

Добавим программу «поиска в глубину», позволяющую предотвратить возникновения циклов:

```

solve(B, Res) :-
    dpth([ ], B, Res).
dpth(Res1, B, [B | Res1]) :-
    goal(B).
dpth(Res1, B, Res) :-
    s(B, B1),
    not member(B1, Res1),
    dpth([B | Res1], B1, Res).

```

Эта программа может потерпеть неудачу, только если пространство состояний окажется бесконечным. Чтобы этого не случилось, глубина поиска ограничивается некоторым максимальным значением, которое выставляем заранее.

### Выводы

Проанализирован и промоделирован на компьютере метод решения задачи с помощью алгоритма «поиска в глубину», в котором выбирается самый глубокий неразвернутый узел в дереве поиска. Временная сложность  $O(b^m)$  и пространственная сложность  $O(bm)$ , где  $m$  — максимальная глубина любого пути в пространстве состояний. Предел глубины ограничен.

Дальнейшее направление работы заключается в том, чтобы физически реализовать рационального агента. Для этого агент должен иметь информацию о местонахождении пунктов, к которым он должен добраться. Карта расположения этих пунктов (карта среды) должна быть помещена в БЗ. Кроме того, он должен иметь информацию о своем собственном местонахождении, чтобы проложить путь к нужным ему пунктам. При моделировании эти данные вводились с клавиатуры. При физической реализации агента потребуются датчики. Датчики — это интерфейс между агентом и

средой, в которой они действуют. Чтобы этот агент мог передвигаться, нужны исполнительные механизмы. В распоряжении на данный момент есть плата разработчика, есть контроллер на базе Cortex M3, ультразвуковой датчик измерения расстояния DYP-ME007, мини-мотор-редуктор Mini Motor Multi Ratio Gearbox 12-Speed (TAM70190) и некоторое другое аппаратное обеспечение агентов. Аппаратное обеспечение постепенно пополняется. Следующим результатом работы будет низкоуровневое управление агентом. Результатом тестирования ожидается проверка восприятие-действие. Это очень важная и сложная задача, потому что создание низкоуровневых систем есть основа, на которой будут строиться высокоуровневые компоненты, позволяющие формировать рассуждения и осуществлять планирование деятельности рационального агента.

#### **Список используемых источников**

1. **Artificial Intelligence** / P. H. Winston. – Addison-Wesley Publishing company, 2003. – 776 р.
2. **Алгоритмы** искусственного интеллекта на языке Prolog : 3-е издание / И. Братко; пер. с англ. – М. : Вильямс, 2004. – 640 с.

*Статья представлена научным руководителем, доцентом Т. В. Губановой.*

# ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 551.46.06

**Е. Е. Андрианова (старший преподаватель кафедры БИС СПбГУТ)**

## ТЕХНОЛОГИИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ ПРИ ПОДГОТОВКЕ *IT*-СПЕЦИАЛИСТОВ

Принятие решений – это особый вид человеческой деятельности, направленный на выбор способа достижения поставленной цели. В повседневной жизни человек все время стоит перед выбором и принимает решение: перейти дорогу по зеленому сигналу светофора или перебежать по красному, двигаться на автомобиле дальше или заправиться, глядя на панель приборов и используя адекватную информацию о его состоянии. Иногда приборов и данных столь много, что такое количество информации человек не в состоянии проанализировать и решение принимается интуитивно.

В качестве вспомогательного средства для обеспечения принятия решений используются системы поддержки принятия решений (СППР) [1]. СППР относят к информационным системам интеллектуальной поддержки процессов разработки и реализации решений. Они являются инструментом, призванным оказать помощь лицам, принимающим решений, особенно при решении неструктурированных и слабоструктурированных задач, в том числе и многокритериальных.

Роль СППР не в том, чтобы заменить ЛПР, а в том, чтобы повысить эффективность его деятельности. Цель СППР заключается не в автоматизации процесса принятия решения, а в осуществлении кооперации, взаимодействия между системой и человеком в процессе принятия решений.

Системы поддержки принятия решений в общем случае можно охарактеризовать следующими четырьмя основными характеристиками. Они:

- используют и данные, и модели;
- предназначены для решений слабоструктурированных и неструктурированных задач;
- поддерживают, а не заменяют, выработку решений пользователями;
- способствуют повышению эффективности принимаемых решений.

СППР имеют большую аналитическую мощность: используют разнообразные модели и численные методы, чтобы анализировать данные. Они помогают находить ответы на следующие типичные вопросы.

Анализ случаев (*case analysis*) – оценка значений выходных величин для заданного набора значений входных переменных.

Параметрический анализ {«Что, если... ?»} – оценка поведения выходных величин при изменении значений входных переменных.

Анализ чувствительности – исследование поведения результирующих переменных в зависимости от изменения значений одной или нескольких входных переменных.

Анализ возможностей («поиск целевых решений», «анализ значений целей», «управление по целям») – нахождение значений входной переменной, которые обеспечивают желаемый результат

Анализ данных – прямой ввод в модель ранее имевшихся данных и манипулирование ими при прогнозировании.

Сравнение и агрегирование – сравнение результатов двух или более прогнозов, сделанных при различных входных предположениях, или сравнение предсказанных результатов с действительными, или объединение результатов, полученных при различных прогнозах или для разных моделей.

Анализ риска – оценка изменения выходных переменных при случайных изменениях входных величин.

Оптимизация – поиск значений управляемых входных переменных, обеспечивающих наилучшее значение одной или нескольких результирующих переменных.

Системы поддержки принятия решений в отличие от традиционных информационных систем аналогичного назначения ориентированы на конкретного пользователя, на его знания, опыт и интуицию. Процесс принятия решений носит субъективный характер, и СППР помогает пользователю найти решения, которые именно ему представляются наилучшими, но которые без ее помощи было бы трудно, или даже невозможно отыскать из-за очень большой сложности решаемой задачи.

Выработка решения происходит в результате итерационного процесса. Участвуют в этом процессе СППР и человек. Система поддержки принятия решений выступает как вычислительное звено и объект управления, а человек задает входные данные, получает и оценивает результат вычислений на компьютере с помощью СППР.

В состав системы поддержки принятия решений входят следующие основные компоненты [1]:

- база данных и система управления базой данных (СУБД);
- база моделей и система управления базой моделей (СУБМ);
- система управления интерфейсом между пользователем и компьютером.

Эти компоненты системы отражают функциональный подход к рассмотрению СППР, то есть на первый план выступает вопрос о том, что бу-

дет делать данная СППР. Так управление данными предполагает наличие базы данных.

Базы данных СППР содержат как количественную, так и качественную информацию, поступающую из различных источников, а база моделей содержит разнообразные статистические, финансовые и управленческие модели, которые важны для решения встречающихся в данной предметной области проблем [2].

Эффективность и гибкость информационной технологии поддержки принятия решений во многом зависят от характеристик интерфейса СППР. Общая цель создания пользовательского интерфейса заключается в том, чтобы сделать систему как можно проще, чтобы позволить пользователям наиболее полно использовать программное обеспечение системы. Интерфейс должен обеспечивать как опытных, так и неопытных пользователей, предоставляя необходимую помощь в части применения специфических методов и моделей.

Сегодня СППР может быть найдена в персональном компьютере руководителя, как часть программы Microsoft Access. Бухгалтерские и финансовые модели могут создаваться как настольные СППР в программе Microsoft Excel и как программные компоненты, и в корпоративной СППР. Пакеты программного обеспечения оптимизационных расчетов, как составные части СППР, обычно рассчитаны на отдельного пользователя и применяются в виде компьютерных настольных пакетов. Однако в некоторых случаях в оптимизационных моделях специфических СППР могут использоваться для вычислений данных, получаемых в реальном масштабе времени из местных или информационных сетей, которые распространяются на другие территории.

Учебный план ИТ-специалиста в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича содержит курсы по отдельным компонентам СППР. Это такие курсы, как Информационные технологии, Управление данными, Интеллектуальные системы и технологии, Технологии обработки информации, Высокопроизводительные информационные технологии компьютерных сетях, Технологии распределенных управляемых систем, Сети хранения данных.

Уже при изучении курса «Информационные технологии» студенты знакомятся с отдельными возможностями СППР в рамках лабораторных работ. Например, одна из работ связана с исследованием задач оптимизации с помощью табличного процессора Excel. При выполнении данной работы студенты знакомятся с такими инструментами Excel, как «подбор параметра» и «поиск решения», которые являются инструментами анализа «Что, если ...». Используя эти инструменты и различные наборы значений данных в одной или нескольких формулах, студенты получают несколько вариантов решений и должны оценить их и выбрать наилучшее. В работе

«Анализ данных. Статистические расчеты» студенты знакомятся основами построения простейших статистических моделей средствами Excel.

Первичное ознакомление с основными компонентами СППР и их возможностями студенты знакомятся уже на втором курсе в рамках предмета «Информационные технологии», а на последующих курсах в рамках других дисциплин углубляя эти знания и повышая их профессиональную компетентность.

#### **Список используемых источников**

1. **Информационные** технологии. Поддержка принятия решения. Обработка данных: учеб. пособие / И.А. Липанова, О.Ю. Ильяшенко, Е.Е. Андрианова. – СПб. : СПбГУТ, 2013. – 53 с.
2. **Проблемы** моделирования данных и пути их решения на примере единой системы информации об обстановке в мировом океане / Е. Е. Андрианова, И. А. Липанова // VII Международная науч.-практ. конференция «Международная среда ВУЗа XXI века» : материалы конференции. – Петрозаводск, 2013 – 288 с.

*Статья представлена научным руководителем канд. техн. наук, доцентом И. А. Липановой.*

**УДК 004.041**

**Е. А. Бубнова (студентка группы ТСС-31м СПбГУТ)**

#### **АВТОМАТИЗАЦИЯ ПРОЦЕССА СБОРА И ОБРАБОТКИ ДАННЫХ С ДАТЧИКОВ ФИЗИЧЕСКИХ ВЕЛИЧИН С ПОМОЩЬЮ СРЕДСТВ ВИЗУАЛЬНОГО ПРОГРАММИРОВАНИЯ**

Беспроводная сенсорная сеть представляет собой распределенную, самоорганизующуюся сеть множества датчиков (сенсоров), обеспечивающих сбор, обработку и передачу информации. Сенсорные узлы имеют беспроводной интерфейс и автономный источник питания. Набор датчиков является специфичным для конкретного случая применения [1].

Одним из важных достоинств сенсорных сетей является их всепроникающая самоорганизующаяся структура, выполненная на основе кластеризации и состоящая из огромного количества сенсорных узлов. К самоорганизации относится быстрая адаптация к численному составу устройств в сети, способности подключения новых устройств автоматический выбор маршрутов для передачи данных, а главное возможность ретрансляции сообщений от одного элемента сети к другому.

Беспроводной сенсор сети представляет собой плату (рис. 1), на которой располагаются микро-процессор, оперативная и флэш память, цифровые и аналого-цифровые преобразователи, радиочастотный приемопередатчик, источник электропитания, а так же сам датчик. Питание сенсора осуществляется от батареи, мощностью в несколько вольт.

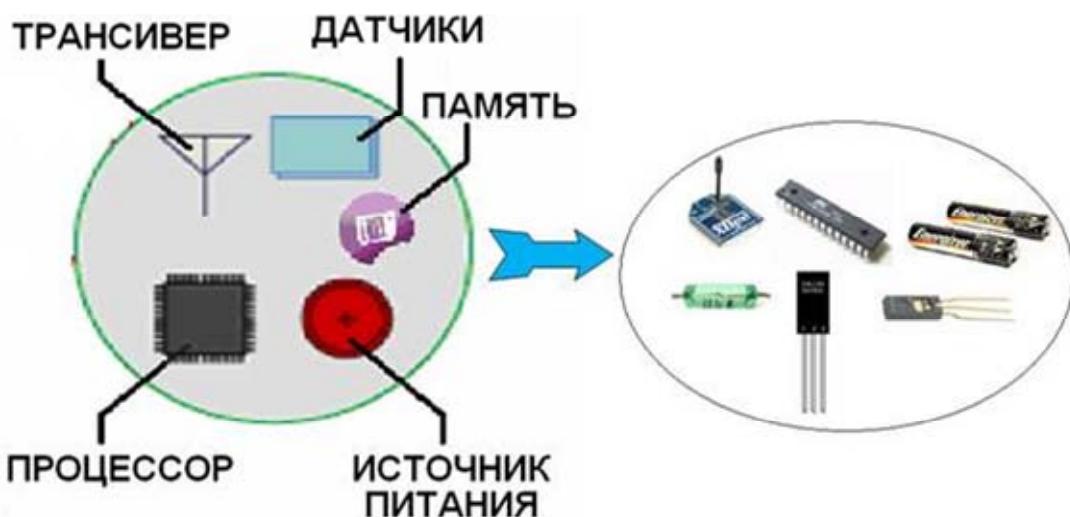


Рис. 1. Модель сенсора и его аппаратные составляющие

Типы датчиков используемых для сенсорных сетей:

- датчик вибрации;
- датчик температуры;
- датчик давления;
- датчик тока, напряжения в электросетях;
- датчик движения.

Электронные счетчики расхода газа, воды, тепловой или электрической энергии, а также любых других типов датчиков.

Основная обработка данных полученных сенсором производится узлом, или шлюзом, который представляет собой мощный компьютер. Передача данных по сети осуществляется посредством радиоканала. Наличие контроллера в узлах сети позволяет реализовать самоорганизующуюся сенсорную сеть и функции ретрансляции. Такой подход обеспечивает качественное покрытие радиосигналом всех необходимых зон, независимо от таких препятствий как железобетонные конструкции или большие расстояния. Данные, передаваемые сенсорами, включают в себя не только информацию, снятую с датчика, но также информацию о состоянии сенсоров и результатах процесса передачи данных. Сообщения передаются от одних сенсоров к другим, образуя цепь, в итоге все переданные данные собираются в ближайших к шлюзу сенсорах. Таким образом, если некоторые сенсоры выходят из строя, то работа всей сенсорной сети, после необходимой реорганизации, произведенной автоматически – продолжается [2].

Современные научные достижения позволяют создавать миниатюрные и интеллектуальные сенсоры. Миниатюризация позволяет расширять возможности применения и интеграции беспроводных сенсорных сетей. Таким образом, сенсорные сети могут дислоцироваться в любую целевую область для осуществления мониторинга и контроля (рис. 2).

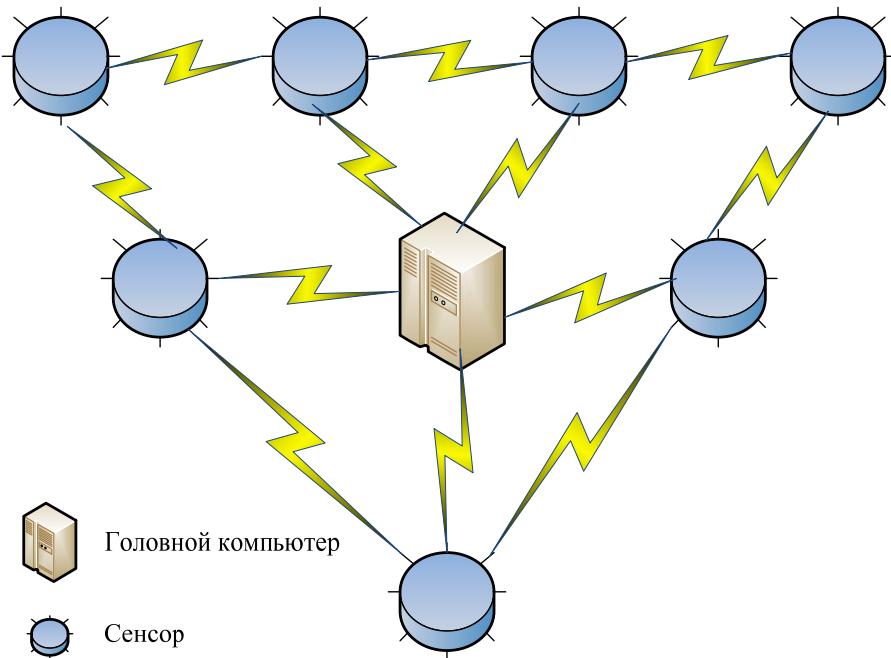


Рис. 2. Схема сенсорной сети

В работе были изучены такие стандарты организации сенсорных сетей как:

- ZigBee;
- IEEE 802.15.4;
- 6loWPAN;
- One-Net.

Было приведено их сравнение, с учетом вопросов лицензирования использования частотного диапазона.

Оборудование, используемое для беспроводных сенсорных сетей, не имеет четкой стандартизации, поэтому существует несколько различных платформ. Каждая из которых отвечает основным базовым требованиям к сенсорным сетям: небольшая мощность потребления, как можно более длительное время работы, маломощные приемопередатчики, наличие различных сенсоров. К таким платформам можно отнести MicaZ, TelosB, Intel Mote 2.

Далее было изучено программное обеспечение, используемое в сенсорных сетях. Существует несколько сотен различных протоколов обработки и передачи данных, а также систем управления узлами. Наиболее распространенной операционной системой является система с открытым кодом – TinyOs, визуализатор TinyViz, эмулятор системы TOSSIM [3, 4].

Одним из направления работы было изучение областей применения проектов на базе сенсорных сетей таких как:

- сельское хозяйство;
- медицина;
- системы безопасности;
- окружающая среда;
- сейсмоопасные районы;
- транспорт и иные объекты.

Такое количество областей применения, показывает огромный потенциал, который нуждается в защите. В настоящее время применение сенсорных сетей связано с определенным риском. Он заключается в огромном количестве угроз, связанных с обеспечением безопасности работоспособности и надежности работы сенсорных сетей. В работе выявлены основные направления обеспечения безопасности в сенсорных сетях. Так как в сеть включено большое количество узлов, важнейшей составляющей сенсорной сети является энергосистема. Возможность максимально уменьшить расход электропитания в сети, а таким образом увеличить жизненный цикл сенсоров, является одной из приоритетных задач при разработке беспроводных сенсорных сетей. Таким образом, существует целый ряд особенностей обеспечения безопасности в сенсорных сетях.

#### **Список используемых источников**

1. **Беспроводные** сенсорные сети: вопросы и ответы / С. С. Баскаков // Автоматизация в промышленности. – 2008. – № 4. – С. 34–35.
2. ГОСТ Р ГСИ 8.673–2009. ГСИ. Датчики интеллектуальные и системы измерительные интеллектуальные. Термины и определения. – Введ. 2010-01-12. – М. : Изд-во стандартов, 2010.
3. **Беспроводные** сенсорные сети [Электронный ресурс] / М. Сергиевский // Компьютер Пресс. – 2008. – № 4. Часть 2. – Режим доступа: <http://www.compress.ru/Article.aspx?id=18943> (Дата обращения 20.05.2014).
4. **Беспроводные** сети. Первый шаг : пер. с англ. – М. : Вильяме, 2005. – 192 с. : ил. – Парал. тит. англ.

*Статья представлена научным руководителем д-ром. техн. наук, профессором Г. В. Верховой.*

УДК 004.93

**И. А. Васильев (старший преподаватель кафедры ИКД СПбГУТ)**

## **ПРИМЕНЕНИЕ НЕЧЕТКОЙ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ В ЗАДАЧЕ РАСПОЗНАВАНИЯ ЭМОЦИЙ**

Эмоции являются ключевым свойством человека и важным звеном в цепи саморегуляции его организма. Они оказывают непосредственное влияние на все сферы человеческой деятельности – перцептивную, когнитивную, мотивационную, целевую. Технологический прогресс не может исключить влияние человеческого фактора, а значит важно четко понимать влияние эмоций человека на риски, возникающие в процессе управления сложной техникой. Для обеспечения должного уровня безопасности на местах повышенного риска информационная среда должна быть адаптирована к возможным эмоциональным сдвигам. В этом ключе актуально построение систем распознавания эмоций, для обеспечения надежности и достоверности вывода относительно эмоционального состояния пользователя. Наибольший интерес в области систем распознавания представляют оптические системы, поскольку они позволяют анализировать действия пользователя не прибегая непосредственно к физическому контакту.

Современные системы распознавания эмоциональных реакций используют ограниченный набор классов эмоций, который строится на формальных классификационных моделях, принятых в психологии. Стоит отметить, что в настоящее время ни одна из предлагаемых классификаций не является в достаточной мере полной и обоснованной, чтобы быть универсальной. Сложность построения классификационной модели связана с обилием способов выражения и представления эмоций. Зачастую эмоция связана непосредственно с неким образом действий, с событиями в результате которых человек получил эмоциональный отклик. Описание эмоции, в этом случае, превращается в целостный рассказ, подкрепленный жестами, мимикой, что позволяет собеседнику в полной мере прочувствовать события и воспринять их. Описание эмоций на естественном языке не позволяет на должном уровне выделить сущностные черты эмоций и провести обобщение. Существующие модели эмоций различаются количеством, обозначением и целевой компонентой, которая ставит эмоции в соответствие некоторое формальное пространство признаков. Например, определяя эмоции как положительные и отрицательные, стенические и астенические. В действительности, в процессе распознавания, однозначно можно утвердить лишь положение о том, что эмоция – это некий пространственно-временной процесс. Пространственная компонента отражается в конфигурации и интенсивности сокращения мимических мышц в конкретный момент времени. В пантомимике может выражаться через позу. Временная

компонента учитывает динамику перехода от одной мимической реакции(позы) к другой.

Реализация системы распознавания эмоций предполагает решение двух важных задач: определение характеристических компонент эмоционального процесса и выбор метода отображения найденных компонент на модель эмоций. Среди множества моделей, применяемых в системах распознавания эмоции популярна модель предложенная Полом Экманом и Уоллесом Фризеном [1]. Она базируется на представлении о существовании базовых, врожденных эмоций: удивление, гнев, радость, печаль, отвращение, презрение. Популярность теории Экмана обеспечивается не только лаконичным набором эмоциональных классов и апробированными положениями, но и разработанной на ее основе системы кодирования мимических реакций (СКЛиД), которая ставит в соответствие положению мимических мышц класс эмоций. Обучение экспертов проводится на наборе статических изображений. Таким образом распознавание эмоций по мимике учитывает исключительно их пространственную характеристику, в предположении, что эксперт способен самостоятельно справиться с опознаванием временных зависимостей. Если мы предполагаем в качестве эксперта человека, то его жизненный опыт способен помочь решить эту задачу. Для систем компьютерного зрения эффективного способа решения этой проблемы не найдено. Большинство современных систем используют исключительно пространственные компоненты, которые не способны адекватно представить развитие эмоционального процесса.

Эмоции могут иметь различные внешние проявления: мимические реакции, частотные характеристики движения, пространственные отношения и т. д. Введем понятие *дескриптор эмоциональной реакции*, которое поможет обобщить различные проявления эмоциональных реакций. Дескриптор эмоциональной реакции (ДЭР) – форма проявления эмоций, выраженная в виде нечеткого правила и отражающая единство эмоционального процесса в различных проявлениях (1).

$$D = \{< x, \mu_D(x) > | x \in U\}. \quad (1)$$

### *Нечеткая модель распознавания эмоций*

Непостоянство признаков эмоций, как следствие культурных различий в выражении и восприятии эмоциональных характеристик, отсутствие однозначной модели представления эмоций и классификации диктует необходимости использовать нечеткие экспертные системы [1], которые используют логико-лингвистические методы описания модели. Базовая модель процесса распознавания эмоций в нечеткой системе представлена на рисунке 1.



Рис. 1. Базовая модель нечеткой системы распознавания эмоций

Архитектура модели нечеткого вывода дает возможность комбинировать ее с нейронными сетями, обеспечив возможность автоматической подстройки параметров функций принадлежности. В качестве нечеткой нейронной сети предлагается использовать структуру TSK [2, 120]. В TSK выделяют 5 слоев:

1. Первый слой обеспечивает фаззификацию каждой переменной. На этом этапе определяются функции принадлежности  $\mu_{D_1}$ . Параметры уравнения (2)  $\sigma_i, a_i, b_i$  подлежат адаптации в процессе обучения сети.

2. Слой агрегирования, определяющий результирующее значение коэффициента принадлежности.

3. Генератор функции TSK, представлен  $y_k(x) = p_{k0} + \sum_{j=1}^N p_{kj} x_j$ . В этом

слое умножение функции  $y_k(x)$  на  $w_k$ , сформированных на предыдущем с. Это параметрический слой, в котором адаптации подлежат линейные веса  $p_{kj}$ .

4. Четвертый слой представлен двумя нейронами, один из которых рассчитывает взвешенную сумму сигнала  $y_k(x)$ , а другой сумму весов  $\omega_k$ .

5. Пятый слой состоит из одного нейрона. В нем происходит нормализация весов и вычисляется выходной сигнал  $y(x)$ .

Одним из основных моментов в проектировании нечеткой нейронной сети является выбор входных параметров и метода обучения.

### *Входные параметры*

Пространство дескрипторов разбито на несколько уровней. Первый уровень представляет собой ответ на выходе четкой многослойной нейронной сети, обученной на множестве базовых эмоций. В качестве Терма первого уровня используется набор соответствующих классов базовых эмоций (1).

$$D_1 = \{ \text{удивление, гнев, радость, печаль, отвращение, презрение}\}.$$

Функция принадлежности определяется следующим уравнение(2)

$$\mu_{D_1} = \frac{1}{1 + (\frac{x_i - a_i}{\sigma_i})^{2b_i}}, \quad (2)$$

где  $\sigma_i, a_i, b_i$  – параметры подлежащие адаптации в процессе обучения.

Второй уровень определяет активность некоторых мимических мышц, что позволяет уточнить достоверность вывода. Терм второго уровня представлен в следующем виде:

$$D_2^{(k)} = \{\text{Слабо Различимое, Ярко выраженное, Сильное, Предельное}\},$$

где  $k$  – идентификатор мышцы по СКЛиД.

Второй класс дескрипторов использует межкадровую разницу изображений на текущем и предыдущем кадрах, пропущенных через фильтр Габора в зоне мимической активности (3):

$$x_i(t) = \sum(G(I(t+1)) - G(I(t))), \quad (3)$$

где  $D_2^{(k)}$  – дескриптор эмоциональной реакции,  $k$  – идентификатор определяет зону лица по СКЛиД Экмана.

$$G(I(x, y), u, v, \theta, \lambda, \phi, \sigma, \gamma) = e^{-\frac{u'^2}{2\sigma^2}} \cos\left(2\pi\frac{u'}{\lambda} + \phi\right), \quad (4)$$

$$u' = u\cos(\theta) + v\sin(\theta),$$

$$v' = -u\cos(\theta) + v\sin(\theta),$$

где  $G(I(x, y), \theta, \lambda, \phi, \sigma, \gamma)$  – фильтр Габора;  $\theta$  – определяет ориентацию фильтра,  $\lambda$  – длина волны,  $\phi$  – фаза,  $\sigma$  – радиус гауссиана,  $\gamma$  – определяет отношение сторон для гауссиана. Параметры фильтра  $\theta$  определяются через угол наклона головы,  $\gamma$  зависит от расстояния камеры до пользователя.

Третий класс дескрипторов описывает интенсивность движения пользователя в кадре. Термы, описывающие интенсивность движения:

$$D_3 = \{\text{активность, норма, пассивность}\}.$$

Решающие правила составляет эксперт в момент просмотра заранее заготовленных видеофайлов. Отвечая на вопросы системы, о наличии того или иного дескриптора, и определяя название эмоции. Пример решющего правила для эмоции “сильный гнев” представлен в следующем виде:

$$R_{\text{сильный гнев}}: (D \wedge D^{(4)} \wedge D^{(5)} \wedge D^{(7)} \wedge D^{(24)}) \rightarrow y_{\text{сильный гнев}}, \text{ где } y \in Y,$$

где  $R_{\text{сильный гнев}}$  – правило для нечеткого вывода эмоции сильный гнев.  $Y$  – множество выходных термов.

### Заключение

В настоящее время накоплен опыт работы множества экспертов в области распознавания эмоций, назрела необходимость обобщения этого

опыта в рамках определенной системы. Создаваться такая система может на основе нечеткой нейронной сети TSK. Обучение нейронной сети предполагается проводить в процессе анкетирования эксперта предъявляя ему набор, заранее подготовленный видеофайлов, полученных при съемке людей, в момент переживания ими экспрессивной реакции. Они должны ответить на вопросы о наличии тех или иных параметров эмоций. Нейронная сеть автоматически адаптируется к решению эксперта. В настоящее время осуществляется сбор данных для обучающей выборки.

### **Список используемых источников**

1. **Facial Action Coding System Investigator's Guide** / P. Ekman, W. V. Friesen, J. C. Hager. – Research Nexus, 2002. – 197 p. – ISBN 0-931835-01-1.
2. **Нечеткие модели и методы в интеллектуальных системах: учебн. пособие для ВУЗов / Ю. П. Зайченко.** – Киев : Слово, 2008. – 344 с. – ISBN 978-966-8407-79-6.

*Статья представлена заведующим кафедрой, д-ром техн. наук, профессором Д. В. Волошиновым.*

**УДК 004.415**

**Н. В. Воинов (доцент кафедры ИУС СПбГПУ)**  
**П. Д. Дробинцев (доцент кафедры ИУС СПбГПУ)**  
**В. П. Котляров (профессор кафедры ИУС СПбГПУ)**  
**И. В. Никифоров (ассистент кафедры ИУС СПбГПУ)**

## **ИНТЕГРИРОВАННАЯ ТЕХНОЛОГИЯ ФОРМАЛИЗАЦИИ ТРЕБОВАНИЙ НА ПРОГРАММНЫЙ ПРОДУКТ НА ОСНОВЕ СОВМЕСТНОГО ИСПОЛЬЗОВАНИЯ ДВУХ ФОРМАЛЬНЫХ ЯЗЫКОВ**

Одной из основных проблем разработчиков программного продукта является проблема проверки корректности функционирования создаваемой системы. Стоимость исправления ошибок в пределах жизненного цикла продукта растет экспоненциально в соответствии с фазой разработки. Предотвращение ошибок в требованиях и обнаружение их на ранних этапах проекта сильно уменьшает общий объём корректировок продукта и таким образом сокращает конечную стоимость разработки системы. Отсюда возникает целевая установка: концентрироваться на поиске ошибок на самых ранних фазах жизненного цикла, не дожидаясь их обнаружения в процессе тестирования готовой реализации. Отвечая этой установке, в послед-

нее время активно развиваются методы и инструменты верификации и тестирования на основе формальных моделей [1].

Формальные модели позволяют применить математический аппарат верификации, получить спектр моделей различной детальности в процессе уточнений, а также предоставляют возможность автоматической генерации исполняемого кода и тестовых сценариев по модели. Верификация позволяет осуществить проверку корректности, полноты и непротиворечивости требований до этапа автоматической кодогенерации, что существенно снижает стоимость создания корректной исполнимой модели проектируемой системы.

Однако создание формального описания систем сразу на языках, воспринимаемых средствами верификации, – весьма трудоемкий процесс. Во-первых, свойственная на ранних стадиях проекта неполнота и изменчивость исходных требований затрудняет построение модели, требует перманентной коррекции формализации и, как следствие, привносит значительные временные затраты в выполнение проекта. Во-вторых, высокий уровень необходимых знаний в области математической логики, предъявляемый исполнителям, является дополнительным ограничивающим фактором, усложняющим внедрение формальных методов в процесс индустриальной разработки продукта.

Решением описанных проблем является совместное использование двух высокоуровневых формальных языков спецификаций на протяжении всего процесса работы с требованиями. Один из языков должен быть интуитивно понятен как инженеру, так и заказчику, что позволяет описывать требования и общий дизайн системы на ранних стадиях разработки продукта. Второй язык должен обладать возможностью представлять модель в математических терминах, с которыми непосредственно работает инструментарий верификации и тестирования. Таким образом, первый язык является промежуточным звеном между неформально сформулированными требованиями и формальными моделями, с которыми работают доказательные средства верификации.

Данное решение с применением двух формальных языков описания спецификаций позволяет пользователям, не экспертам в области математической логики, создавать спецификации, которые будут использованы для доказательства корректности, верификации и генерации исполнимого кода системы.

Авторами предложен подход, заключающийся в создании высокоуровневой формальной модели, понятной заказчику и им контролируемой, на языке Use Case Maps (UCM) [2], с дальнейшим ее автоматическим преобразованием в эквивалентную модель на языке базовых протоколов, поддерживаемую промышленным инструментом верификации VRS [3]. Также в работе приведены результаты применения разработанного подхода.

## Язык Use Case Maps

Use Case Maps (рус. – «варианты использования») – это описание последовательности действий, которые может производить система в ответ на внешние воздействия пользователей или программных систем (компонентов). Варианты использования отражают функциональность системы с точки зрения описания архитектуры системы. Их применение привносит важные составляющие в процесс разработки программных систем и позволяет:

- заполнить промежуток между словесным, неформальным описанием требований и детальным дизайном системы;
- разработать архитектуру системы на высоком уровне абстракции, а также задать поведение системы, когда архитектура уже определена;
- помочь разработчику предсказывать поведение сложных систем и изображать в модели параллельные структуры, таймеры, точки прерывания;
- использовать аспектное программирование.

Дизайн системы на языке UCM представляет собой набор взаимодействующих между собой диаграмм. В свою очередь каждая из диаграмм сосредоточена на описании взаимодействия компонентов (агентов, процессов системы), объектов, наблюдателей и подсистем. Каждый компонент и подсистема содержит в себе элементы ответственности (*Responsibilities*), соответствующие некоторым событиям в системе, а также строгую последовательность их возникновения. Таким образом, совокупность компонентов и диаграмм дает пользователю наглядное представление о поведении системы и взаимодействии между ее компонентами.

Формально модель на языке UCM можно определить, как ориентированный граф с вершинами из множества элементов диаграммы и дугами, характеризующими процедуры получения одного элемента диаграммы из других. Таким образом, UCM-модель описывается четверкой  $(U, S, E, R)$ , где  $U$  – конечное множество элементов;  $S$  – множество стартовых точек;  $E$  – множество конечных точек;  $R$  – отношение переходов между элементами [4].

Разработка UCM-диаграмм осуществляется с использованием графического редактора UCM Navigator. На рисунке 1 приведен фрагмент UCM-модели для проекта из области телекоммуникаций, на котором описано многопоточное поведение системы на самом высоком уровне абстракции. Сценарии взаимодействия изображаются линиями и различными элементами (например, *Responsibility*, *Stub*, *AndFork* и др.), порядок следования которых определен направленностью линий.

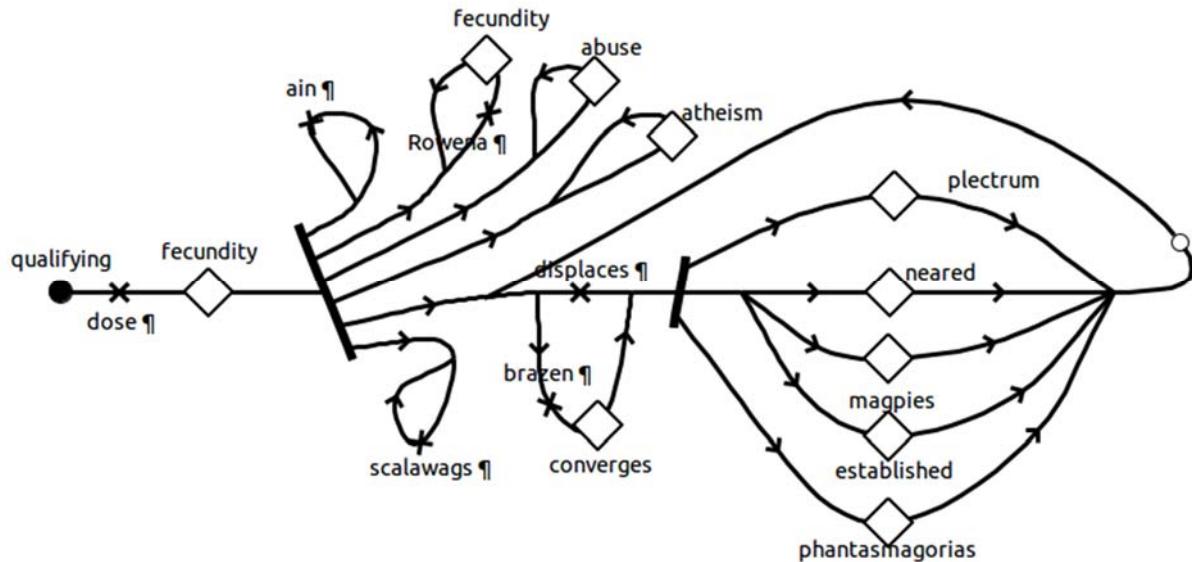


Рис. 1. Пример модели системы на языке UCM

Когда диаграмма, изображающая поведение системы или ее фрагмента, становится сложной для понимания, используется механизм структурирования диаграмм с помощью элементов *Stub* (контейнер) [4]. Верхний уровень UCM-модели рассматривается как корневая диаграмма, которая может содержать контейнеры для поддиаграмм (*plug-ins map*). Элемент *Stub* изображается на диаграмме ромбом, который может иметь несколько входов (линий, входящих в *Stub*) и выходов (линий, выходящих из *Stub*). Таким образом, использование элемента *Stub* – это способ добавления различных уровней абстракции в модели, что позволяет при необходимости изучать систему на высоком уровне абстракции, не вдаваясь в детальное описание ее компонентов.

На [рисунке 2](#) приведена UCM-диаграмма с элементом *Stub* (имя «*voice 2*»), имеющим один вход и два выхода. Также на рисунке 2 изображен элемент *Timer*, задающий временные задержки и изображенный в виде часов.

Таким образом, как видно из приведенного описания, модели на языке *UCM* очевидны, наглядны и содержат широкий спектр графических элементов, которые позволяют моделировать практически любое поведение системы, выраженное в виде последовательности событий.

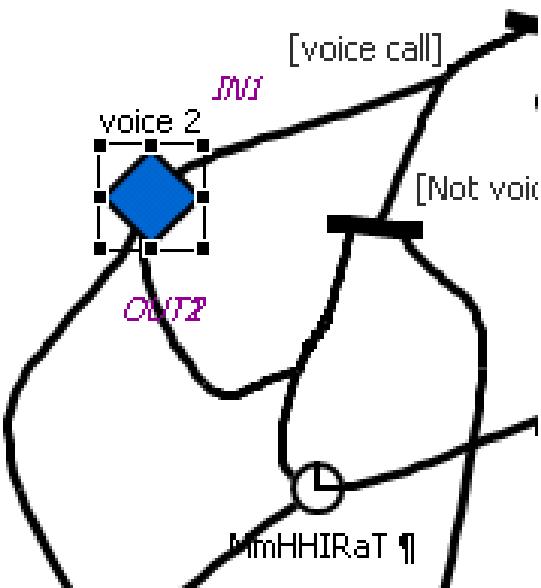


Рис. 2. UCM-диаграмма с элементом Stub

### Язык базовых протоколов

Базовый протокол состоит из предусловия, процессной части и постусловия и описывает набор действий, выполнение которых приводит к изменению состояния модели [3].

Предусловие базового протокола описывает состояние модели до применения протокола. Процессная часть базового протокола описывает набор событий, происходящих в системе после того, как предусловие становится истинным. В результате событий, описанных в процессной части, система переходит в состояние постусловия.

Базовый протокол использует синтаксис MSC-диаграммы, поэтому может представляться в двух формах: текстовой и графической (*MSC/PR* и *MSC/GR*).

Для работы с базовыми протоколами используется VRS технология, позволяющая проводить анализ поведения моделей системы на разных уровнях абстракции [3]. Она проверяет формальные модели, заданные с помощью базовых протоколов, на детерминированность, достижимость определённых состояний, а также на полноту и непротиворечивость.

Для проведения сеанса верификации по требованиям создается эталонный сценарий или список, содержащий имена базовых протоколов, кодирующих определённую последовательность событий (сигналов, действий). VRS проверяет, что анализируемая модель удовлетворяет эталонному сценарию, т. е. содержит пути, куда входят состояния или протоколы в указанном порядке. Нахождение таких путей (трасс) является доказательством корректности поведения модели системы, зафиксированного в требованиях.

Таким образом, трасса – это один из сценариев поведения модели, а поскольку исполняемая программа генерируется из модели, то можно сказать, что трасса – это сценарий поведения самой программы.

### *Преобразование модели на языке UCM в модель на языке базовых протоколов*

Разработанный авторами инструмент преобразования основан на правилах отображения семантических элементов и конструкций языка UCM в эквивалентные конструкции на языке базовых протоколов. В инструменте поддерживается более 40 конструкций UCM, что позволяет полностью автоматизировать преобразование моделей и использовать его в промышленной разработке [5].

Преобразование модели занимает от нескольких секунд до десятков секунд в зависимости от сложности исходной UCM-модели, что существенно упрощает совместное использование двух языков и устраниет риски привнесения дополнительных ошибок, связанных с человеческим фактором при преобразовании моделей: описок, опечаток и других неточностей.

### *Результаты*

Разработанный подход с совместным применением двух формальных языков и автоматическим преобразованием высокогоуровневой UCM-модели в модель базовых протоколов был применен в рамках четырех крупных телекоммуникационных проектов и в среднем на 45 % сократил время на создание формальной модели, ее корректировку и анализ исходных требований на наличие ошибок.

### **Список используемых источников**

1. **Верификация** и автоматизация тестирования UML-проектов / Н. В. Воинов, В. П. Котляров // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2009. – Т.3 – № 80. – С. 220–225.
2. **Международный** стандарт ITU-T Recommendation Z.151. User requirements notation (URN) – Language definition. – ITU-T, 2012. – 216 с.
3. **Basic protocols**, message sequence charts, and the verification of requirements specifications / A. Letichevsky, J. Kapitonova, A. Jr. Letichevsky, V. Volkov, S. Baranov, T. Weigert // Computer Networks: The International Journal of Computer and Telecommunications Networking. – 2005. – Т.49 – № 5. – С. 661–675.
4. **Методика** проектирования тестов сложных программных комплексов на основе структурированных UCM моделей / П. Д. Дробинцев, И. В. Никифоров, В. П. Котляров // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2013. – № 174. – С. 99–104.
5. **Генерация** формальной модели системы по требованиям, заданным в нотации Use Case Map / И. В. Никифоров, А. В. Петров, Ю. В. Юсупов // Научно-технические

ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2010. – Т.4 – № 103. – С. 191–195.

**УДК 004.1**

**И. П. Волынкин (студент группы ТСС-95 СПбГУТ)**

## **РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ АВТОМАТИЗИРОВАННОЙ МАРШРУТИЗАЦИИ ВНУТРИЦЕХОВЫХ МОБИЛЬНЫХ РОБОТОВ**

Автоматизация на производстве способствует сокращению трудоёмкости, времени выполнения задач, увеличению производительности качества труда и внедрению новых технологических методов, реализации научно-технических и технологических решений.

В настоящее время на производствах множество операций осуществляется вручную. Для оптимизации и сокращения расходов на производство многие задачи можно передать механическим автоматизированным и автоматическим системам.

Механический труд имеет ряд преимуществ над ручным трудом:

- меньшая вероятность ошибки;
- меньшая стоимость за время работы;
- выше выносливость, грузоподъемность, реакция и скорость;
- возможность беспрерывной работы 24 часа 7 дней в неделю;
- возможность работать в опасных для человека условиях: загрязнения, высокие или низкие температуры и давление и т. д.;
- недостатки работы автоматизированных систем;
- трудоёмкость при проектировании, создании и внедрении;
- регулярный контроль и обслуживание системы и её объектов.

Простейшие операции по перемещению объектов при производственном процессе намного выгоднее поручать мобильным роботам — автоматизированные устройства, способные перемещаться в пространстве и имеющие манипулятор для погрузки и выгрузки груза.

Чтобы уменьшить участие человека в процессе, необходимо разработать автоматизированную систему управления (АСУ), контролирующую и управляющую перемещающимися объектами.

Для производства важна скорость выполнения работы, поэтому основной задачей для системы управления роботами является сокращение времени перемещения, и, соответственно, увеличение скорости.

Для представления системой пространственного окружения создаётся карта помещения, где будут перемещаться мобильные роботы. Карта может быть, как двухмерная, так и трёхмерная. Проще всего её описать взвешенным ориентированным графом, где вершинами будут точки внутри помещения, а рёбрами – пути между точками. Вес ребра описывает время, которое движущийся объект затрачивает на перемещение из одной точки (вершины) в другую. Граф должен быть ориентированным, так как бывают случаи, когда из одной точки можно попасть в другую, но не наоборот.

Описанная карта заносится в систему. Для контроля системой объектов, обеспечивается обратная связь в виде информирования системы о текущем положении движущегося объекта. Местоположение определяется при помощи системы позиционирования в помещении. Основные используемые для позиционирования группы технологий – это:

- радиочастотные технологии;
- технологии локального позиционирования (инфракрасные и ультразвуковые);
- радиочастотные метки – RFID.

Радиочастотные технологии, в свою очередь, делятся на стандартные технологии передачи данных (*Wi-Fi, Bluetooth, Zigbee*), так или иначе приспособленные для измерения расстояний, и на те, которые, исходя из физических свойств модуляции, наиболее подходят для измерения расстояний (*CSS/ISO24730-5, UWB, ISO24730-2, NFER* и другие) [1].

Чтобы прокладывать маршруты объектам в АСУ закладываются алгоритмы поиска кратчайшего пути во взвешенном графе.

В качестве примеров таких алгоритмов можно отметить:

- алгоритм Беллмана – Форда [2] – алгоритм поиска кратчайшего пути во взвешенном графе. За время  $O(|V| \times |E|)$  алгоритм находит кратчайшие пути от одной вершины графа до всех остальных. В отличие от алгоритма Дейкстры, алгоритм Беллмана – Форда допускает рёбра с отрицательным весом. Предложен независимо Ричардом Беллманом и Лестером Фордом;
- алгоритм Дейкстры [3] – алгоритм, изобретённый нидерландским ученым Э. Дейкстрой в 1959 году. Находит кратчайшее расстояние от одной из вершин графа до всех остальных. Алгоритм работает только для графов без рёбер отрицательного веса.

Для унификации системы, необходимо абстрагироваться от конечного алгоритма и предусмотреть возможность использования любого алгоритма.

Так как перемещающихся объектов будет несколько, АСУ придётся рассчитывать маршруты с учётом того, что траектории разных объектов могут пересекаться, и необходимо не допустить появления двух и более объектов в одно и то же время в одном и том же месте.

Мобильный робот по своей сути является внутрицеховым транспортом. Он может быть подразделен на отдельные виды по многим признакам, например, по характеру перемещаемых грузов (сыпучие или штучные), методу перемещения (пневматический и механический), направлению перемещения (вертикальное и горизонтальное).

В принятой классификации транспорт делится на две основные группы по времени действия – транспорт периодического действия и транспорт непрерывного действия.

К первому виду транспорта относятся напольный безрельсовый и рельсовый транспорт, краны, подвесные монорельсовые дороги и подъемные механизмы; ко второму – конвейеры всех видов, пневматический и гидравлический транспорт.

Выбор того или иного вида внутрицехового транспорта в основном зависит от технологического процесса, характера грузов, строительных возможностей, необходимости модернизации и изменения процесса производства или самого производства.

Прямая зависимость между выбранным видом транспорта и структурой производственного здания велика и важна. В последнее время стремятся применять виды транспорта, наименее влияющие на конструкцию и объемно-планировочное решение производственного здания. Например, отказываются, где это возможно, от применения мостовых кранов, затрудняющих модернизацию производственного процесса. В так называемых гибких цехах должен быть и гибкий вид транспорта.

**Транспорт периодического действия.** Напольный транспорт, передвигающийся непосредственно по полу, дает возможность доставлять грузы в любую точку здания. Не оказывая влияния на строительную часть здания, за исключением конструкции пола, напольный транспорт требует создания сети проездов, что ведет к потере производственных площадей.

Напольный транспорт может быть рельсовый, безрельсовый и прицепной. К рельсовому виду транспорта относятся козловые (портальные) краны, вагонетки, платформы, управление которыми может быть ручным и моторизованным. Направление его движения связано с колеей, устройство которой требует значительных строительных работ.

К безрельсовому транспорту относятся автопогрузчики, тележки, платформы – ручные или моторизованные, снабженные приспособлениями для погрузки или разгрузка либо без них, а также различные виды автомобильных кранов.

Прицепной транспорт состоит из тягача с прицепными тележками или платформами, образующими поезд. Тягачи могут быть с авто- или электродвигателями. Напольный транспорт – наиболее гибкий вид транспорта.

### Список используемых источников

1. Indoor Geolocation Using Wireless Local Area Networks (Berichte Aus Der Informatik), Michael Wallbaum (2006)
2. On a Routing Problem / R. Bellman // Quarterly of Applied Mathematics. – 1958. – Vol 16, No. 1. – PP. 87–90.
3. A note on two problems in connexion with graphs / E. W. Dijkstra // Numerische Mathematik. – 1959. – V. 1. – PP. 269–271.

*Статья представлена научным руководителем канд. техн. наук, доцентом С. В. Акимовым.*

**УДК 004.588**

**Н. Н. Горлушкина (заведующая кафедрой ИТГС НИУ ИТМО)**  
**Д. А. Денисова (студентка группы 4707 НИУ ИТМО)**

## **ПРОЕКТИРОВАНИЕ ОБРАЗОВАТЕЛЬНОГО МОДУЛЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДОЙ В СФЕРЕ ИНЖЕНЕРНЫХ ИЗЫСКАНИЙ**

Современный этап развития образования связан с широким использованием современных информационно-коммуникационных технологий. В современном мире ежегодно обновляется 5 % теоретических и 20 % практических знаний, которыми обладают инженеры, врачи, биологи и представители других групп специалистов [1]. В сфере инженерных изысканий постоянно обновляется нормативная база, появляется новое оборудование, в частности приборы, совершенствуются методы обработки информации и прикладные программные средства. Инженерные изыскания относятся к работам, оказывающим влияние на безопасность объектов капитального строительства. Поэтому важно развивать организационные, методические и технологические основы построения системы дополнительного профессионального образования и оценки профессиональных квалификаций в сфере инженерных изысканий. Для своевременного приобретения новых знаний специалистами применяется электронная форма обучения.

Актуальность исследований, связанных с эффективностью и результативностью современных форм электронного обучения, не вызывает сомнений. Был проведен опрос в социальной сети «В Контакте» (рис. 1) в официальных группах: «НИУ ИТМО», «Абитуриент НИУ ИТМО», «eLearning ИТМО», и за пункт «проходил электронное обучение, понравилось» проголосовало большинство пользователей, а именно 39,1 % от общего числа опрошенных. Никогда не проходили электронное обучение 21,5 % опро-

шенных. Интересно было посмотреть результат 17,2 % опрошенных, 11,4 % проходили электронное обучение и им не понравилось, почти 7 % считают, что общение преподавателя и студента не может быть удаленным, а 4 % вообще не знают, что такое электронное обучение». Всего в опросе приняли участие 325 пользователей. В целом следует отметить существующий интерес к электронному обучению.

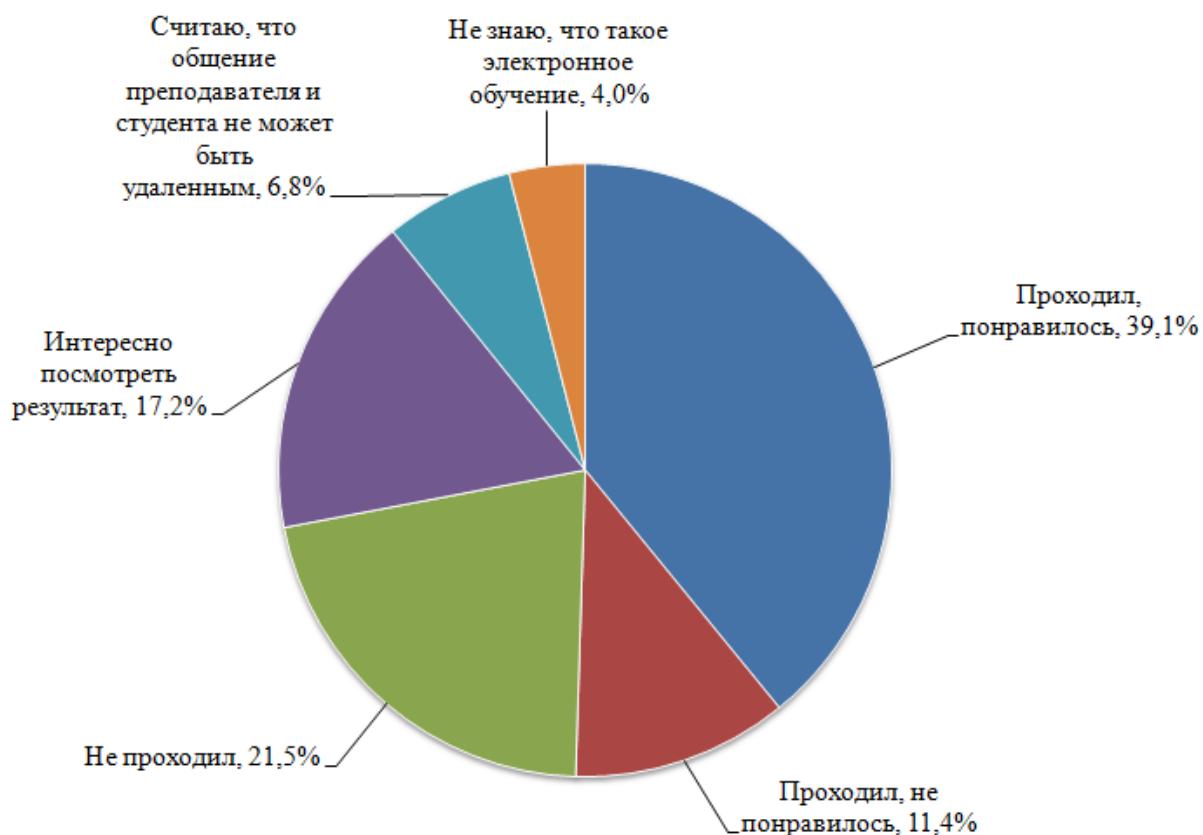


Рис. 1. Опрос в социальной сети «ВКонтакте» «Проходили ли вы когда-нибудь электронное обучение?» (все целевые группы)

Анализируя данные опроса, были выделены целевые группы: «Студенты», «Выпускники», «Абитуриенты», «Сотрудники».

К самой активной целевой группе можно отнести студентов Университета. Однако в ней процент неопределившихся увеличился на 4,3 %, на трех пользователей, положительно оценивающих электронное обучение, приходится один пользователь отрицающий возможность использования электронного обучения, то есть скепсис по отношению к электронному обучению у студентов удельно больше.

Если рассматривать все остальные целевые аудитории в совокупности, то ситуация изменяется. Здесь 61,8 % от числа всех опрошенных пользователей оказались «в теме», а соотношение пользователей, проголосовавших «за» и «против» выросло до 5:1.

Анализ открытого опроса показал, что наиболее востребованным электронное обучение является для целевых групп: «Выпускники», «Абитуриенты», «Сотрудники».

Можно сделать вывод, что пользователи на данный момент рассматривают процесс электронного обучения как возможность повысить свою квалификацию, получить второе высшее образование, дополнительное профессиональное образование и т. д., а не как возможность пройти обучение по основным образовательным программам.

В рамках научно-исследовательской работы Национального объединения изыскателей «Система оценки профессиональных квалификаций и дополнительного профессионального образования НОИЗ» предлагается создание автоматизированной системы управления информационно-образовательной средой в сфере инженерных изысканий (АСУ ИОС). Основная составляющая системы – подсистема электронных онлайн курсов, выполняющая образовательные функции. При проектировании подсистемы учитываются лучшие практики создания таких систем за рубежом – Coursera, Udacity, MITx и EdX. На их сайтах в свободном доступе находятся учебные материалы лучших университетов США и других стран. Из российских аналогов стоит отметить «Универсариум». Он разрабатывается при участии РИА Новости и МГУ им. Ломоносова. Его миссия – предоставить возможность получения качественного образования от лучших российских преподавателей и ведущих университетов для миллионов российских граждан.

Создание автоматизированной системы управления информационно-образовательной средой в сфере инженерных изысканий позволит улучшить качество и доступность образования. Система позволит обеспечить непрерывное дополнительное профессиональное образование в сфере инженерных изысканий.

Образовательный модуль выше описанной системы разрабатывается с использованием стандарта SCORM. SCORM – это сборник спецификаций и стандартов, разработанный для систем дистанционного обучения. Содержит требования к организации учебного материала и всей системе дистанционного обучения. SCORM позволяет обеспечить совместимость компонентов и возможность их многократного использования: учебный материал представлен отдельными небольшими блоками, которые могут включаться в разные учебные курсы и использоваться системой дистанционного обучения независимо от того, кем, где и с помощью каких средств они были созданы. SCORM основан на стандарте XML [2].

Использование стандартов при проектировании АСУ ИОС позволит решить ряд проблем, связанных с взаимодействием с другими обучающими продуктами, а также использовать уже разработанные курсы. Стандарты являются основой единого информационного образовательного пространства.

Функциональные возможности образовательного модуля описаны с помощью диаграммы вариантов использования.

В системе есть три роли пользователей: студент, преподаватель и администратор. Студент может просматривать лекции, пройти обучающий тест, подать заявку на аттестующий тест, задать вопрос, посмотреть журнал успеваемости и новости (рис. 2). После просмотра лекций студент может прикрепить выполненные практические задания.

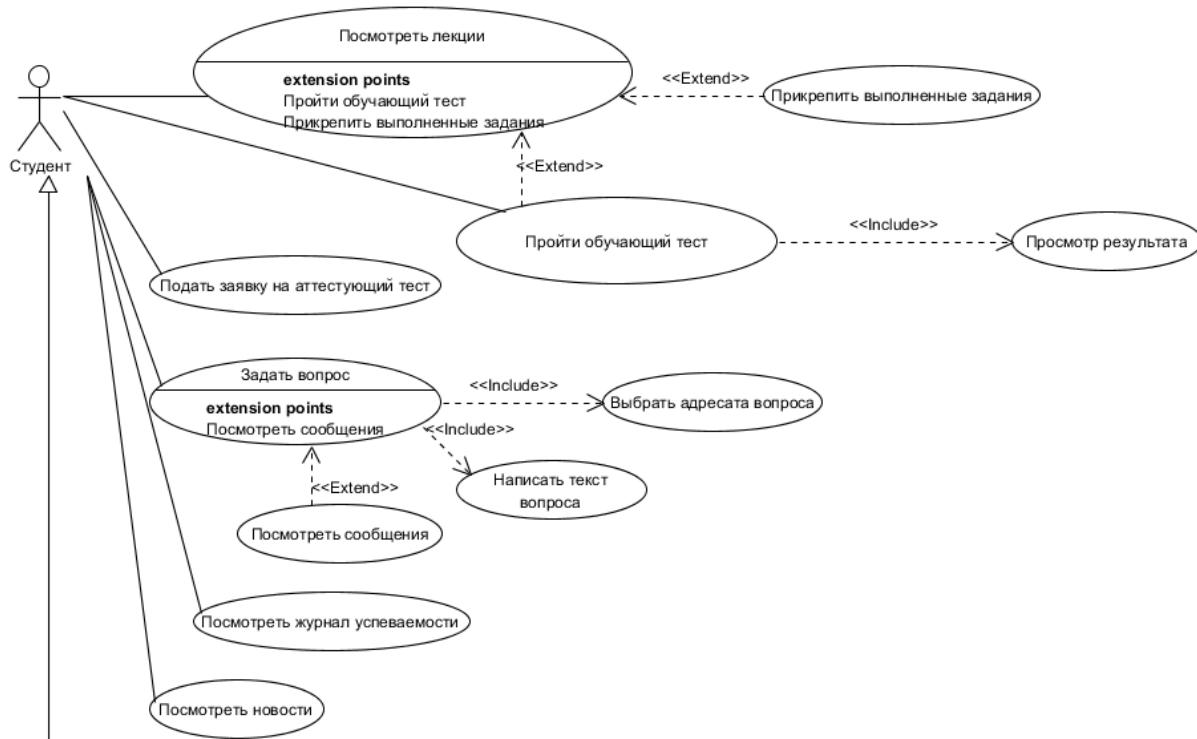


Рис.2. Диаграмма вариантов использования для роли «студент»

Преподаватель может создавать электронные курсы, редактировать курсы, управлять новостями и создавать направления подготовки. Создание курса включает в себя ввод дисциплины, материалов лекций, создание обучающих тестов. При вводе лекций можно прикреплять презентации, практические задания и лабораторные работы.

Администратор может управлять пользователями и базой данных. Также администратор может делать всё, что может делать преподаватель, а преподаватель может делать всё, что может делать студент.

Для реализации системы предлагается использовать БД MySQL Enterprise Edition [3]. Серверная часть реализуется на языке программирования PHP, с использованием фреймворка Yii. Выбор фреймворка обусловлен его популярностью и большим количеством документации на русском языке. Общая оценка наиболее популярных фреймворков приведена в работе [4], Yii единственный фреймворк, который набрал по всем критериям максимальное количество баллов.

В результате выполнения работы спроектирован образовательный модуль, который:

- обеспечивает возможность быстрого обновления информации;
- обеспечивает гибкость графика обучения студентов;
- обеспечивает возможность учиться по индивидуальному плану согласно собственным потребностям и возможностям;
- обеспечивает объективную и независимую от преподавателя оценку знаний;
- обеспечивает возможность консультироваться с преподавателем в ходе обучения;
- увеличивает доступность учебных материалов.

#### **Список используемых источников**

1. **Вызовы** научно-технической революции и образование [Электронный ресурс] / С. Г. Вершловский. – Режим доступа: [http://www.znanie.org/jurnal/n3\\_08/Versh13.pdf](http://www.znanie.org/jurnal/n3_08/Versh13.pdf) (Дата обращения 17.04.2014).
2. **Sharable Content Object Reference Model (SCORM) 2004** [Электронный ресурс] / Ф. Доддс, Ш. Е. Тропп. – Режим доступа: <http://www.edu.ru/db/portal/e-library/00000053/SCORM-2004.pdf> (Дата обращения 15.04.2014).
3. **Develop, deploy, and manage MySQL applications** [Электронный ресурс]. – Режим доступа: <http://www.oracle.com/us/products/mysql/mysqlenterprise/overview/index.htm> (Дата обращения 17.04.2014).
4. **Анализ** характеристик различных веб-фреймворков [Электронный ресурс] / Ю. В. Демчишин. – Режим доступа: <http://vestnik.msmu.ru/files/2/20130508151539.pdf> (Дата обращения 20.04.2014).

**УДК 004.052.32**

**И. О. Грабко (студент СПбГПУ)**  
**Т. Х. Черкасова (преподаватель СПбГПУ)**

#### **КОДЫ С СУММИРОВАНИЕМ И ИХ МОДИФИКАЦИИ В ФУНКЦИОНАЛЬНЫХ СИСТЕМАХ КОНТРОЛЯ**

В функциональных схемах контроля используются коды с суммированием [1–4]. Классический код с суммированием – это код Бергера. Код Бергера – нелинейный равномерный двоичный код, в котором в контрольных разрядах содержится двоичная запись количества единиц или нулей информационных разрядов. Для определенности рассмотрим случай, когда подсчитывается количество единиц. Количество единиц в информационных разрядах равно сумме всех чисел информационных разрядов. Такой код часто используется в симметричных каналах связи. Код Бергера обна-

руживает нечетное количество ошибок в информационных разрядах. Могут быть не обнаружены такие ошибки четной кратности, когда какое-то количество единиц превращается в нуль, такое-же количество нулей превращается в единицы. В данной работе предлагаются некоторые модификации кода Бергера, которые авторы назвали комбинированными кодами Бергера. В работе предлагаются две модификации с проверкой на четность. Пусть длина информационной части кода равна  $m$ . Тогда в комбинированных кодах первого типа по правилу Бергера контролируем ( $m - 1$ ) информационных разрядов, а  $m$ -й информационный разряд контролируем на четность вместе с первыми информационными разрядами. В кодовом слове  $\alpha_1\alpha_2 \dots \alpha_{m-1}\alpha_m\alpha_{m+1} \dots \alpha_{m+k}\alpha_{m+k+1}$ , первые  $m$  разрядов информационные, следующие  $k + 1$  разрядов – контрольные, причем первые  $k$  контрольных разрядов организованы как в коде Бергера для  $m - 1$  первых информационных разрядов – это двоичное число единиц в  $m - 1$  разрядах, а  $k + 1$ -й контрольный разряд содержит сумму всех  $m$  информационных разрядов по модулю 2:  $\alpha_{k+1} = \alpha_1 + \alpha_2 + \dots + \alpha_m \bmod 2$ . Можно организовать проверку на четность в комбинированном коде только по части разрядов, например, находим сумму по модулю 2 половины информационных разрядов для четного количества этих разрядов или половину информационных разрядов плюс еще один разряд для нечетного количества разрядов.

Если в комбинированном коде Бергера  $m$  информационных разрядов, то в кодовом слове будет такое же количество разрядов, как и в обычном коде Бергера, или на 1 больше (табл. 1).

ТАБЛИЦА 1. Сравнение длин кодов Бергера

<i>m</i>	Длина обычного кода Бергера	Длина комбинированного кода Бергера первого типа	Длина комбинированного кода Бергера второго типа
4	7	7	8
5	8	9	9
7	10	11	12
8	12	12	13
16	21	21	22

Для примера получим коды для информационного слова 0110. Код Бергера будет 0110010. Здесь 3 контрольных разряда, в трех разрядах записано число 2 – количество информационных 1. Всего отведено 3 контрольных разряда, так как наибольшее количество информационных 1 всего 4, число 4 в двоичной записи 100 занимает 3 разряда. Комбинированный код Бергера 0110100. Тоже три контрольных разряда, в первых двух контрольных разрядах записано число информационных 1 в первых 3 разря-

дах, 3-й контрольный разряд содержит сумму всех 4-х информационных разрядов по модулю 2. Как известно, код Бергера обнаруживает любое нечетное количество ошибок. Предложенный комбинированный код Бергера с проверкой на четность всех разрядов тоже обнаруживает любое нечетное количество ошибок. Если нечетное количество ошибок в первых  $m - 1$  информационных символах, то они обнаружатся кодом Бергера для этих разрядов; нечетное количество ошибок может быть такое, что четное количество в первых  $m - 1$  разрядах, а одна ошибка в  $m$ -м разряде, но тогда при проверке на четность они тоже обнаружатся. Итак, как и для обычных кодов Бергера надо найти не обнаруживаемые ошибки четной кратности  $d$ , но только в  $m - 1$  разрядах. Если в комбинированном коде первого типа проверять на четность только часть разрядов, то появляются не обнаруживаемые ошибки нечетной кратности. Но общее количество необнаруживаемых ошибок для комбинированных кодов первого типа одинаково.

Для количества обнаруживаемых и необнаруживаемых ошибок получены комбинаторные формулы [5], но в данном сообщении приводятся только сравнительные таблицы для количеств необнаруживаемых ошибок.

В таблицах 2, 3 и 4 приведены количества необнаруживаемых ошибок в информационных разрядах рассматриваемых кодов. В последнем столбце приведено число всех необнаруживаемых ошибок.

ТАБЛИЦА 2. Распределение необнаруживаемых ошибок информационных разрядов кода Бергера

Код $n, m$	Кратность $d$									
	2	3	4	5	6	7	8	9	10	$\Sigma$
4,2	2	0	0	0	0	0	0	0	0	2
5,3	12	0	0	0	0	0	0	0	0	12
7,4	48	0	6	0	0	0	0	0	0	54
8,5	160	0	60	0	0	0	0	0	0	220
9,6	480	0	360	0	20	0	0	0	0	860
10,7	1344	0	1680	0	280	0	0	0	0	3304
12,8	3584	0	6720	0	2240	0	70	0	0	12614
13,9	9216	0	24192	0	13440	0	1260	0	0	48108
14,10	23040	0	80640	0	67200	0	12600	0	252	183732

ТАБЛИЦА 3. Распределение необнаруживаемых ошибок информационных разрядов комбинированного кода Бергера первого типа с контрольной суммой по всем информационным разрядам

Код, $n, m$	Кратность, $d$									
	2	3	4	5	6	7	8	9	10	$\sum$
4,2	0	0	0	0	0	0	0	0	0	0
6,3	4	0	0	0	0	0	0	0	0	4
7,4	24	0	0	0	0	0	0	0	0	24
9,5	96	0	12	0	0	0	0	0	0	108
10,6	320	0	120	0	0	0	0	0	0	440
11,7	960	0	720	0	40	0	0	0	0	1720
12,8	2688	0	3360	0	560	0	0	0	0	6608
14,9	7168	0	13440	0	4480	0	140	0	0	25228
15,10	18432	0	48384	0	26880	0	2520	0	0	96216

ТАБЛИЦА 4. Распределение необнаруживаемых ошибок комбинированного кода Бергера первого типа с контрольной суммой по части разрядов

Код $n, m$	Кратность									
	2	3	4	5	6	7	8	9	10	$\sum$
6,3	0	4	0	0	0	0	0	0	0	4
7,4	8	16	0	0	0	0	0	0	0	24
9,5	32	64	12	0	0	0	0	0	0	108
10,6	128	192	72	48	0	0	0	0	0	440
11,7	384	576	432	288	0	40	0	0	0	1720
12,8	1152	1536	1824	1536	240	320	0	0	0	6608
14,9	3072	4096	7296	6144	1920	2560	140	0	0	25228
15,10	8192	10240	25344	23040	12800	14080	1400	1120	0	96216

*Второй тип комбинированного кода.* Пусть код с суммированием организован так, что первые  $m - 2$  разрядов контролируются по Бергеру, и добавляется еще 2 контрольных разряда с проверкой на четность: один разряд содержит сумму первых  $m - 1$  разрядов, а второй контрольный раз-

ряд содержит сумму первых  $m - 2$  разрядов и последнего  $m$ -о разряда. Для таких кодов необнаруживаемых ошибок будет еще меньше, чем в кодах первого типа (табл. 5).

ТАБЛИЦА 5. Количество необнаруживаемых ошибок  
для комбинированного кода второго типа

Код $n, m$	Кратность									
	2	3	4	5	6	7	8	9	10	$\Sigma$
6,3	0	0	0	0	0	0	0	0	0	0
8,4	8	0	0	0	0	0	0	0	0	8
9,5	48	0	0	0	0	0	0	0	0	48
11,6	192	0	24	0	0	0	0	0	0	216
12,7	640	0	240	0	0	0	0	0	0	880
13,8	1920	0	1440	0	80	0	0	0	0	3440
14,9	5376	0	6720	0	1120	0	0	0	0	13216
16,10	14336	0	26880	0	8960	0	280	0	0	50456

### Список используемых источников

1. A note on an error detection code for asymmetric channels / J. M. Berger // Information and Control. – 1961. – № 4. – PP. 68–73.
2. Три теоремы о кодах Бергера в схемах встроенного контроля / Д. В. Ефанов // Надежность и техническая диагностика. – 2013. – №1. – С. 77–86.
3. О свойствах кода с суммированием в схемах функционального контроля / Д. В. Ефанов, В. В. Сапожников, Вл. В. Сапожников // Автоматика и телемеханика. – 2010. – № 6. – С. 155–162.
4. Предельные свойства кода с суммированием // В. В. Сапожников, Вл. В. Сапожников, Д. В. Ефанов // Известия Петербургского университета путей сообщения. – 2010. – № 3. – С. 290–299.
5. Комбинированный код Бергера / И. О. Грабко, Т. Х. Черкасова // 42 неделя науки СПбГПУ. – 2013.

УДК 004.62

**К. С. Дегтева (студентка группы 53506/10 СПбГПУ)**

**ИССЛЕДОВАНИЕ АППАРАТНО-ПРОГРАММНЫХ  
КОМПЛЕКСОВ *ORACLE EXADATA* В КОМПАНИИ  
*JAPAN TOBACCO INTERNATIONAL***

Oracle Exadata Storage Server (*Exadata*) – решение для хранения данных, оптимизированное для использования с базой данных Oracle. Exadata обеспечивает эффективность операций ввода-вывода и высокую скорость обработки SQL-запросов для хранилищ данных (*Data Warehouse, DW*), транзакционных систем (*online transaction processing, OLTP*) и систем со смешанной нагрузкой. Высокая производительность Exadata распространяется на все типы приложений благодаря параллельной архитектуре и технологии Exadata Smart Flash Cache. Exadata представляет собой сочетание прикладной и аппаратной частей, используемых для хранения данных и доступа к СУБД Oracle. Продукт реализует прозрачные, с точки зрения приложений для БД и SQL-операций, сервисы хранения, например, возможность передавать обработку операций системе хранения, чтобы разгрузить основной сервер. Хранилище под управлением Exadata гораздо эффективнее обрабатывает данные, повышает масштабируемость операций ввода-вывода, просто в использовании и управлении, а также предоставляет критически важную для компании доступность данных и надежность ПО [1].

Продукты Exadata решают следующие основные проблемы ввода-вывода, которые способны замедлить производительность хранилища:

1. Exadata основана на параллельной архитектуре, которая дает большую пропускную способность и скорость для передачи данных между серверами и хранилищами.

2. Exadata создана с использованием более широких каналов передачи, обеспечивающих невероятно высокую пропускную способность канала между сервером БД и системой хранения.

3. Exadata знает структуру блока БД и способен находить только те данные, которые действительно необходимы для завершения SQL-запроса. Это приводит к меньшей загрузке канала между серверами БД и устройствами хранения.

4. Exadata преодолевает механические ограничения дисковых устройств, автоматически кешируя часто востребованные данные и обеспечивая недостижимую ранее пропускную способность и количество операций ввода-вывода в секунду.

Все сервера бизнес-аналитики в компании объединены по географическому расположению рынков и количеству пользователей в 7 групп для удобства конфигурации и поддержки [2].

Этапы внедрения представлены ниже [3].

### *Этап 1. Тестовые испытания*

1. На начальном этапе каждая из семи групп рынков имеет определенную начальную техническую архитектуру (рис. 1).
2. Для реальных баз данных создаются резервные копии, чтобы сохранить состояние перед внесением существенных изменений (рис. 2).
3. Созданная резервная копия БД переносится на настроенный Data Migration Server для настройки переноса данных на Exadata.
4. Oracle осуществляет миграцию базы данных на тестовый программно-аппаратный комплекс Oracle Exadata.
5. Созданная резервная копия БД переносится на настроенный Report Validation Server для проверки отчетов.

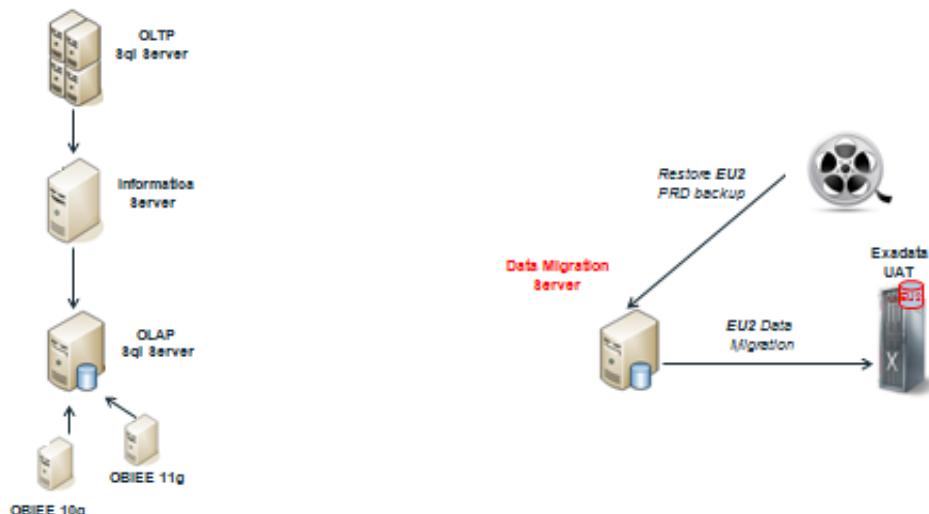


Рис. 1. Начальная архитектура

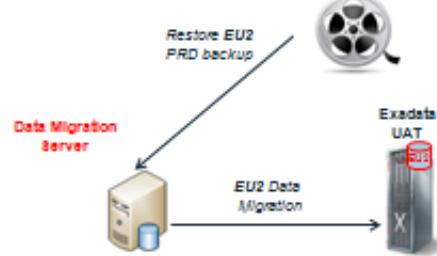


Рис. 2. Создание резервных копий баз данных

6. Настраиваются 2 сервера OBII1g: один указывает на Exadata, другой на Report Validation Srv. Oracle Business Intelligence-приложение, предназначенное для решения задач бизнес-анализа (рис. 3). Продукт представляет собой единый набор инструментов, с помощью которых можно выполнять произвольные запросы, анализировать данные, работать с интерактивными информационными панелями, формировать регламентные отчеты, настраивать систему автоматического оповещения пользователей о важных событиях, анализировать информацию в режиме offline [4].

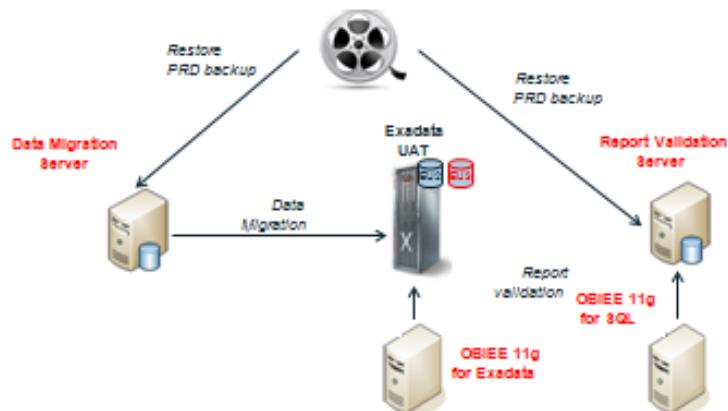


Рис. 3. Настройка серверов OBIEE 11g

7. Рынки, входящие в тестируемую группу, предоставляют отчеты, которые могут быть использованы для тестирования результатов и производительности на обоих серверах.

8. Действия повторяются для каждой группы рынков.

### *Этап 2. Тесты по интеграции*

1. Настроен новый сервер Informatica для загрузок данных. Процессы ETL работают на базах данных SQL и Oracle.

2. Настраивается новый ETL процесс для Oracle. Extract Transform Load процесс используется для переноса большого объема данных из транзакционных систем, приложений и хранилищ данных.

3. Тесты проводятся для ETL: целостность данных, производительность, стесс-тесты) и OBI (производительность, стресс-тесты) (рис. 4).

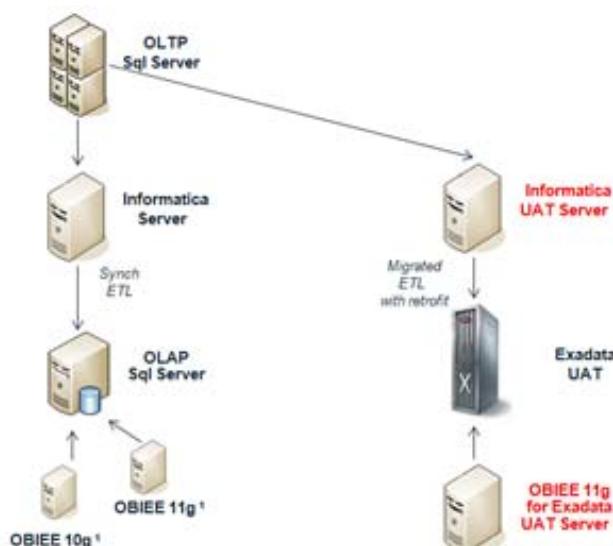


Рис. 4. Тестирование ETL и OBI

### *Этап 3. Тесты пользователей*

Тесты проводятся для сравнения OBI на Microsoft SQL Server и OBI на Oracle Exadata.

### *Этап 4. Внедрение*

1. SQL база данных переносится на Exadata.
2. Настраивается новый ETL для Production системы.
3. Созданные до этого OBI 11g сервера настраиваются под Exadata.

### *Этап 5. Использование*

Старые сервера Informatica, OLAP DB и OBIEE 10g отключаются.  
На данный момент Exadata была внедрена для двух групп рынков.

На сегодняшний день компании все больше интересует единая платформа для консолидации всех их приложений в одной общей инфраструктуре. Неважно для каких типов нагрузки – OLTP, хранилища или смешанной – общая инфраструктура обеспечивает эффективность центров данных. Построение специализированных решений для каждого типа приложений очень дорого и не эффективно. Потребность в обработке большего количества данных возрастает каждый день, в то время как компании с каждым днем урезают ИТ-бюджет.

Внедрив решение Exadata в свою ИТ-инфраструктуру, компании:

1. Увеличат производительность БД и смогут обрабатывать больше данных за тот же промежуток времени.
2. Решат проблемы роста при добавлении и удалении данных и ячеек, а также при росте пропускной способности канала обеспечат защиту и доступность критически важных данных.

### **Список используемых источников**

1. Техническая документация по Exadata. – URL:  
[http://www.partner.fors.ru/registered/Exadata2\\_new1.pdf](http://www.partner.fors.ru/registered/Exadata2_new1.pdf). (Дата обращения 04.10.2009).
2. Методика разработки аналитических отчетов для компании JTI на основе Oracle Business Intelligence / К. С. Дегтева, О. Ю. Сабинин // Компьютерные системы и программные технологии. – 2014. – С. 258–260.
3. Исследование аппаратно-программных комплексов Oracle Exadata в компании Japan Tobacco International: отчёт о НИР (промежут.): 47-04 / СПбГПУ; рук. Сабинин О. Ю.; исполн. Дегтева К. С. . – СПб., 2014. – 25 с. – Библиогр.: с. 25.
4. Техническая документация по Oracle BI 11g. – URL:  
[http://www.rdtex.ru/download/oracle\\_business\\_intelligence\\_suite\\_enterprise\\_edition\\_newgen.pdf](http://www.rdtex.ru/download/oracle_business_intelligence_suite_enterprise_edition_newgen.pdf). (Дата обращения 14.10.2012).

*Статья представлена научным руководителем канд. техн. наук, доцентом О. Ю. Сабининым.*

УДК 004.382:658.58

**Е. В. Катунцов (доцент кафедры БИС СПбГУТ)**

## МЕТОДИКА РАСЧЕТА ОБОБЩЕННОГО ПАРАМЕТРА ФУНКЦИОНАЛЬНОЙ ГОТОВНОСТИ КОМПЛЕКСА ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ

Объективной тенденцией развития комплексов программно-технических средств в настоящее время является постоянный рост сложности аппаратуры, связанный с расширением круга решаемых ею задач при одновременном повышении требований к качеству функционирования. Развитие мобильных устройств, усложнение схемотехнических решений и функциональных связей в современной радиоэлектронной технике вместе с резким увеличением количества элементов в единице оборудования приводит к снижению коэффициентов запаса и порождает значительные трудности в обеспечении необходимой надежности разрабатываемых устройств. Решение задачи анализа состояния функциональной готовности производится обычной статистической обработкой данных множества измерений с фиксированием апостериорного результата [1]. Поэтому необходимость разработки методов и алгоритмов, адекватно отражающих процессы изменения и оценки функциональной готовности определяет актуальность задачи расчета и прогнозирования обобщенного параметра, характеризующего состояние аппаратуры.

В общем виде состояние функциональной готовности комплекса программно-технических средств необходимо охарактеризовать значением одного определяющего параметра  $Q$  [2]. Тогда задачу прогнозирования можно сформулировать следующим образом. Задана допусковая область  $[a, b]$  такая, что при выполнении неравенства  $a < Q < b$  объект анализа считается работоспособным [3]. На интервале  $[0, t)$  осуществляется наблюдение за состоянием комплекса, в результате чего становится известным отрезок реализации  $Q(t)$  случайного процесса изменения на этом интервале.

Естественным путем решения этой задачи является продолжение отрезка реализации  $Q(t)$ ,  $0 < t < t_k$  в область  $t > t_k$  и определение искомого остатка времени «жизни»  $T_{ж}$  как наименьшего из корней одного из двух уравнений  $Q^*(t) - a = 0$  или  $Q^*(t) - b = 0$ , где  $Q^*(t)$  – продолжение искомой реализации  $Q(t)$  в область  $t > t_k$ .

Таким образом, необходимым элементом прогноза функциональной готовности в данной постановке является экстраполяция известной части реализации в область будущих значений.

Для решения этой задачи предлагается использовать метод обобщенного параметра [4], который обеспечивает точность прогнозирования  $e < 0,1...1,0 \%$ , где  $e$  – ошибка прогнозирования, и достоверность прогнози-

рования  $P_{\text{пр}} < 0,95 \dots 0,99$ , где  $P_{\text{пр}}$  – вероятность принятия верного решения. При этом полагается, что вероятность работоспособности системы прогнозирования функциональной готовности –  $D = 1$ .

Метод обобщенного параметра заключается в том, что процесс изменения контролируемых параметров, характеризуемый многими компонентами, описывается одномерной функцией, численное значение которой зависит от измеренной величины параметров. Такая функция рассматривается как обобщенный параметр процесса. При этом обобщенный параметр не имеет конкретного физического смысла, а является математическим выражением, построенным искусственно из контролируемых компонентов прогнозируемого процесса. Все контролируемые параметры следует привести к единой системе счисления, в которой они могут быть сравнимы. Такой системой является система безразмерного (нормированного) относительного счисления.

Реально для каждого анализируемого параметра  $\xi_s$  при  $s = 1, 2, \dots, k$ , можно выделить допустимое значение  $\xi_s^*$ , при достижении которого объект теряет работоспособность, и оптимальное, с точки зрения надежности, значение  $\xi_{s \text{ опт}}$ .

В этом случае безразмерный параметр  $\hat{\xi}_s$  в общем виде запишется так

$$\hat{\xi}_s(t_k) = \frac{\xi_{\text{изм}}(t_k) - \xi_s^*}{\xi_{s \text{ опт}} - \xi_s^*}. \quad (1)$$

Итак, с помощью выражения (1) нормируется параметр  $\xi(t_k)$ , а безразмерная величина  $\hat{\xi}_s(t_k)$  изменяется с течением времени от 1 до 0. Отсюда по величине  $\hat{\xi}_s(t_k)$  можно судить о степени работоспособности комплекса программно-технических средств по данному параметру. Теоретически величина  $\hat{\xi}_s(t_k)$  может быть меньше 0, но это обозначает, что на практике аппаратура комплекса неработоспособна.

Если  $\xi_{\text{изм}}(t_k) > \xi_{s \text{ опт}}$ , то выражение (1) примет вид

$$\hat{\xi}_s(t_k) = \frac{\xi_{\max} - \xi_{\text{изм}}(t_k)}{\xi_{\max} - \xi_{s \text{ опт}}},$$

а при  $\xi_{\text{изм}}(t_k) < \xi_{s \text{ опт}}$ , то формула (1) запишется как

$$\hat{\xi}_s(t_k) = \frac{\xi_{\text{изм}}(t_k) - \xi_{\min}}{\xi_{s \text{ опт}} - \xi_{\min}},$$

где  $\xi_{\max}$  – максимальное допустимое значение прогнозируемого параметра, а  $\xi_{\min}$  – минимальное допустимое значение параметра.

Однаковые количественные изменения величин не всегда являются равнозначными по степени влияния на изменение функциональной готовности аппаратуры комплекса программно-технических средств. Учет влияния осуществляется с помощью весовых коэффициентов, величины кото-

рых характеризуют степень важности соответствующих параметров для решения задачи определения технического состояния. Таким образом, анализируемым параметрам  $\xi_s$  системы соответствуют весовые коэффициенты  $v_1, v_2, \dots, v_s$ , удовлетворяющие тем или иным заданным критериям, причем  $0 < v_s < 1$ , и удовлетворяют условию  $\sum_{s=1}^k v_s = 1$ .

В общем случае определяющий параметр  $Q(t)$  связан сложной зависимостью с частными параметрами системы, которые, в свою очередь, могут находиться в функциональной зависимости друг с другом. Влияние частных параметров на главный показатель можно определить, взяв полный дифференциал функции  $Q_s^*(t)$ , аппроксимированной по значениям  $Q(t_k)$

$$dQ_s^*(t) = \frac{dQ_s^*(t)}{\xi_1(t_k)} d\xi_1(t_k) + \frac{dQ_s^*(t)}{\xi_2(t_k)} d\xi_2(t_k) + \dots + \frac{dQ_s^*(t)}{\xi_s(t_k)} d\xi_s(t_k). \quad (2)$$

Частные производные перед значениями  $d\xi_s(t_k)$  можно рассматривать как весовые коэффициенты частных параметров системы  $\xi_1(t_k), \xi_2(t_k), \dots, \xi_{s-1}(t_k), \xi_s(t_k)$ , связанных функциональной зависимостью с главным обобщенным показателем  $Q_s^*(t)$ . Выражение (2) показывает скорость и направление изменения обобщенного параметра контролируемого комплекса программно-технических средств при изменении одного частного контролируемого параметра и фиксированных остальных частных параметрах.

Тогда выражение для весового коэффициента определится в виде

$$v_s = \frac{dQ_s^*(t)}{\xi_s(t_k)}, \quad (3)$$

где  $v_s$  – весовой коэффициент  $s$ -го частного параметра, а выражение (2) в виде

$$dQ_s^*(t) = v_1 d\xi_1(t_k) + v_2 d\xi_2(t_k) + \dots + v_s d\xi_s(t_k).$$

Таким образом, рассчитанные весовые коэффициенты адаптивны к изменению технического состояния аппаратуры комплекса и изменяют значение главного показателя системы  $Q(t_k)$  в соответствии с ее техническим состоянием.

Запишем обобщенный параметр для комплекса программно-технических средств

$$Q(t_k) = \sum_{s=1}^k \hat{\xi}_s(t_k) v_s, \quad (4)$$

где  $v_s$  – весовой коэффициент измеряемого параметра [5].

Тогда на интервале прогнозирования  $(t_i, t_{i+1})$  значение безразмерного параметра  $\hat{\xi}_S(t_k)$  определяется интегральным значением  $\int_{\tau_i}^{t_{i+1}} \hat{\xi}_S(t_k) dt$ . В тех случаях, когда часть параметров  $\xi_1, \xi_2, \dots, \xi_m$  возрастает, а часть  $\xi_{m+1}, \xi_{m+2}, \dots, \xi_k$  – убывает, нормированный параметр можно представить в виде  $\int_{\tau_i}^{t_{i+1}} \hat{\xi}_S(t_k) dt$  и  $\int_{\tau_i}^{t_{i+1}} \frac{dt}{\hat{\xi}_S(t_k) + b_S}$ , где  $b_S > 0$ .

С учетом всех вышеизложенных выражений обобщенный параметр комплекса (4) можно представить выражением

$$Q(t_k) = \sum_{S=1}^m v_S \int_{\tau_i}^{t_{i+1}} \hat{\xi}_S(t_k) dt + \sum_{m+1}^k v_S \int_{\tau_i}^{t_{i+1}} \frac{dt}{\hat{\xi}_S(t_k) + b_S}. \quad (5)$$

Данное выражение позволяет получить точечное значение обобщенного параметра  $Q_S(t_k)$  в момент времени  $t_k$ , т. е. функция  $Q_S(t_k)$  задана значениями  $Q_1, Q_2, \dots, Q_k$  в точках  $t_1, t_2, \dots, t_k$  на отрезке  $[t_0, t_k]$ .

Таким образом, обобщенный параметр контролируемых систем, рассчитанный на момент времени  $t_k$  по формуле (5) с учетом весового коэффициента (3) определяет степень функциональной готовности комплекса программно-технических средств и оценивается нахождением его в пределах  $0 \leq Q(t_k) \leq 1$ .

Приведенная методика расчета и прогнозирования обобщенного параметра функциональной готовности позволяет оценить момент достижения предельно допустимого значения по обобщенному параметру в зависимости от фактической функциональной готовности комплекса программно-технических средств.

#### Список используемых источников

1. Контроль устройств на интегральных схемах / Н. К. Жердев, Б. П. Креденцер, Р. Н. Белоконь; под ред. д–ра техн. наук Б. П. Креденцера. – К. : Техніка, 1986. – 160 с.
2. Информационный подход к выбору прогнозирующих параметров функциональной готовности РТС / Е. В. Катунцов // Актуальные вопросы развития радиоэлектронной техники РТВ ВВС: Тематический научный сборник – 2006. – № 14. – С. 38–42.
3. Автоматизация контроля радиоэлектронной аппаратуры / В. Д. Кудрицкий, М. А. Синицин, П. И. Чинаев; под ред. П. И. Чинаева. – М. : Сов. радио, 1977. – 256 с.
4. Техническая диагностика. Методика определения периодичности диагностирования технических систем / В. В. Гуляев, Г. Г. Костанди, И. К. Коршунов. – Киев, 1987. – 25 с.
5. Количественные оценки в теории надежности / В. В. Калашников // Математика. Серия Кибернетика. – 1989. – № 10. – 48 с.

УДК 004.43

**М. А. Квасова (студентка группы ИСТ-91 СПбГУТ)**

## **ВОПРОСЫ ДИЗАЙНА И БЕЗОПАСНОСТИ ПРИ МОДЕРНИЗАЦИИ САЙТА**

Успешность в любой сфере деятельности не в последнюю очередь определяется предоставлением объективной информации об участниках взаимодействия и оказываемых ими услугах. Это в полной мере касается и гостиничного бизнеса. Настоящий доклад посвящен информационной системе (ИС) мини-отеля «Аквамарис» [1].

Основная задача данной информационной системы состоит в представлении пользователю полной информации об организации и оказываемых ею услугах. Кроме того, Web-ресурс является, по сути, визитной карточкой организации и создает первое впечатление о ней. В этом контексте особую роль выполняют дизайнерские решения, применяемые при создании сайта.

В цветовой гамме предложенного для анализа ресурса преобладает красный. Данный компонент градиентом переходит в чёрный, усугубляя и без того уже неблагоприятное впечатление от подобранной палитры. Кроме того, для людей, испытывающих затруднения с различением цвета, красный цвет является одним из наиболее проблемных для распознавания.

Нарекания вызывают также используемые для надписей шрифты семейств Arial, Helvetica, Sans-Serif, затрудняющих чтение.

Имеет место также наличие повторяющихся ссылок. Так, ссылка на бронирование повторяется три раза. Не лишен дизайн и проблемы наличия так называемых бесполезных ссылок, таких как, например, «Галерея» и «Цены». Информация о последних дублировалась в разделе «Номера» и не было необходимости выделять под них отдельные страницы.

Дальнейшее усиление положительного эргономического эффекта от использования сайта, а также обеспечение его безопасности невозможно без организации персонального подхода к взаимодействию информационного ресурса с конкретным пользователем. Решение проблемы различения пользователей при организации функционирования многопользовательского приложения выполняется с помощью последовательно выполняемых процедур идентификации, аутентификации и авторизации [2].

Идентификация – процедура распознавания пользователя по его идентификатору, присвоенному ему ранее и занесенному в БД в момент регистрации в качестве легального пользователя системы.

Аутентификация – процедура проверки подлинности входящего в систему объекта, предъявившего свой идентификатор. В качестве такого идентификатора выступают, как правило, пароль или сертификат.

Процессы идентификации и аутентификации взаимосвязаны друг с другом и являются основой для следующего этапа – авторизации – процедуры предоставления пользователю определенных прав доступа к ресурсам системы после успешного прохождении им процедуры аутентификации.

Реализация процедур идентификации, аутентификации и авторизации основывается на использовании механизма сессий. Сессии создаются и завершаются в коде различных web-страниц ИС в зависимости от определенных условий. При генерации сессии появляется возможность сохранять индивидуальную информацию о пользователе в автоматически создаваемых переменных с последующим сохранением данных в БД по окончании сессии. В зависимости от наличия данных о пользователе, правильности указания логина и пароля осуществляется переадресация клиента на ту или иную страницу. Состав системы авторизации и связь между ее составляющими представлены на рисунке 1 [3].

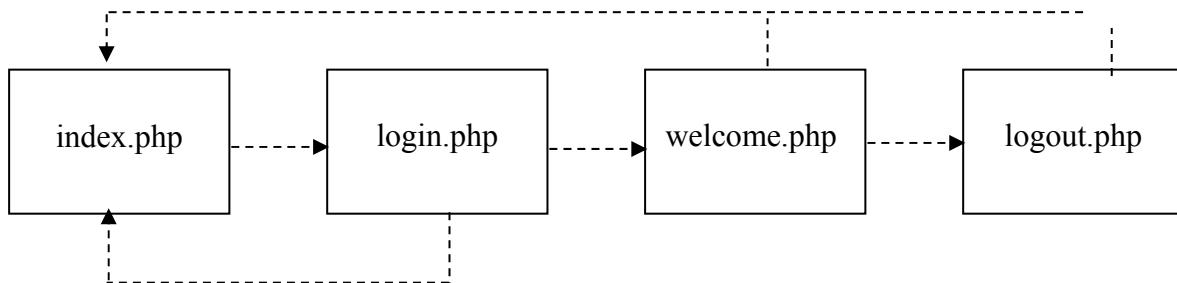


Рис. 1. Система авторизации

Дальнейшее повышение защищенности ИС требует введения механизма разграничения прав доступа на основе ролей. Система разграничения прав доступа изображена на рисунке 2 [3].

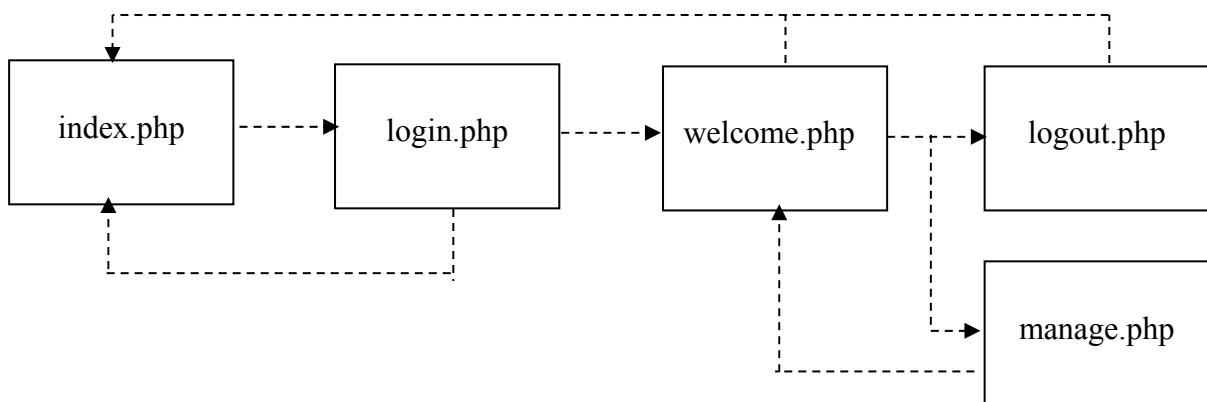


Рис. 2. Система разграничения прав доступа

Реализация принципа разграничения прав предполагает наличие дополнительных файлов с описанием логики обеспечения доступа к тем или иным страницам в зависимости от категории пользователя (файл *map-*

*age.php* на рис. 2). Информация о категориях и принадлежности пользователей к тем или иным категориям сохраняется в дополнительных таблицах БД.

Для данной ИС выделяются следующие категории-роли:

- администратор отеля и администратор сайта;
- зарегистрированный пользователь (постоянный клиент);
- обычный посетитель сайта.

Администратор – роль, предоставляющая неограниченные полномочия – как просмотр личных данных пользователей, так и изменения контента.

Зарегистрированный пользователь – роль, позволяющая клиенту бронировать номера по специальной цене, а также участвовать в различных акциях.

Обычный посетитель – роль, позволяющая пользователю посещать сайт, осуществлять бронирование номеров, а также обратиться за консультацией к администратору отеля.

Таким образом, изменения в дизайне сайта и введение механизма авторизации пользователей с последующим разграничением прав доступа позволяет повысить, с одной стороны, качество оказываемых услуг, с другой – защищенность ресурса, осуществляющего поддержку реализации данных услуг.

#### **Список использованных источников**

1. **Aximaris** [Электронный ресурс]. – Режим доступа: <http://www.aximaris.ru> (Дата обращения 01.04.2014).
2. **Комплексная** защита информации в корпоративных системах : учеб. пособие / В. Ф. Шаньгин. – М. : ИД «ФОРУМ» : ИНФРА-М, 2010. – 592 с. : ил. – (Высшее образование).
3. **PHP**. Трюки / Д. Харрингтон. – СПб. : Питер, 2008. – 448 с.

*Статья представлена научным руководителем канд. техн. наук, доцентом В. Б. Айвазяном.*

**УДК 004.422**

**М. Е. Лю (студент группы РТ-32 СПбГУТ)**

**РАЗРАБОТКА ЛОКАЛЬНОЙ ВЕРСИИ СИСТЕМЫ  
РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ В КОРПОРАТИВНОЙ  
ИНФОРМАЦИОННОЙ- СИСТЕМЕ ВУЗА**

***Цель***

Разработка программного обеспечения для автоматизации учета посещаемости и промежуточного контроля знаний студентов в корпоративной информационной системе (КИС) вуза.

***Задачи***

1. Аутентифицировать студента по его индивидуальной пластиковой карте во время проведения практических, лабораторных или лекционных занятий с помощью локального рабочего кабинета преподавателя.

2. Предоставить преподавателю возможность фиксировать в локальной базе данных (ЛБД) [1] оценки, выставляемые студентам при выполнении ими соответствующих заданий.

Локальный рабочий кабинет преподавателя представляет собой систему для автоматического ввода данных о посещаемости занятий и для учета выполнения учебных планов (лабораторные и практические занятия).

***Фрагмент структуры таблиц ЛБД***

Таблица 1. Дисциплины

ID дисциплины	Имя дисциплины

Таблица 2. Преподаватели

ID преподавателя	Фамилия	Имя	Отчество	Логин	Пароль

Таблица 3. Связи преподавателей, учебных групп и дисциплин

ID преподавателя	ID дисциплины	ID группы

Таблица 4. Учебные группы

ID группы	Имя группы

Таблица 5. Студенты

Номер пласти-ковой карты	Фамилия	Имя	Отчество	ID группы

Пример основной таблицы с данными о присутствующих на занятиях студентах; в названии таблицы указана дата по типу 010114 – 1 января 2014 года (табл. 010114).

Таблица 6. 010114

ID записи	ID учеб-ной пары	ID дисци-плины	Номер карты	Вид ра-боты	Оценка	Комментарий

*Используемая среда разработки:*

++ Builder XE4 – интегрированная среда разработки полнофункциональных приложений на C++ [2].

*Валидатор:*

RFID считыватель;  
модель: Z-2 USB.

Основные характеристики валидатора:

- рабочая частота: 13,56MHz & 125KHz;
- дальность чтения: 4–8 см;
- питание: USB;
- выходной интерфейс: USB;
- размер: 110×80×24.

*Решение задач*

1. Необходимо считывать данные с пластиковой карты с помощью валидатора Z2-USB, подключенному к персональному компьютеру (ПК).

В ходе решения этой задачи используется асинхронное чтение с виртуального COM-порта ПК с ожиданием события «получения данных на порт» (приложение карты к валидатору), после чего данные записываются в буфер и система переходит в исходное состояние.

2. Вывод на экран таблицы с данными о присутствующих на занятиях с возможностью ввода оценок по результатам проверки знаний.

Вывод данных из буфера происходит в таблицу StringGrid, являющуюся составной частью среды разработки, с полями для ввода промежуточной оценки знаний и комментария к ней.

3. Сохранение информации в ЛБД.

Запись в ЛБД, как и чтение из нее, осуществляется посредством таких модулей, как DataSource, ADOConnectoin, ADOTable [3].

### *Выход*

Разработанное программное обеспечение позволяет автоматизировать процесс учета посещений занятий студентами и позволяет вводить данные об оценках тестирования знаний итоге мы получаем необходимое ПО для реализации системы автоматической регистрации посещения студентами занятий пользователей в КИС вуза.

### **Список используемых источников**

1. Microsoft Access 2010. Разработка приложений на реальном примере / Г. Гурвиц. – СПб. : БХВ-Петербург, 2010. – 497 с.
2. Полный справочник по C++ / Г. Шилдт. – М. : Вильямс, 2007. – 800 с.
3. Язык программирования C++ / Б. Страуструп. – М. : Бином, 2011. – 1136 с.

*Статья представлена научным руководителем старшим преподавателем  
В. А. Евстигнеевым.*

**УДК 004.75**

**М. П. Моржаков (студент группы ТСС-95 СПбГУТ)**

## **РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДИСТАНЦИОННОГО МОНИТОРИНГА АВТОМАТИЗИРОВАННОГО ТЕХНОЛОГИЧЕСКОГО ОБОРУДОВАНИЯ**

Цель данного проекта разработка системы мониторинга оборудования на предприятии, которая позволит улучшить эффективность используемого оборудования.

Цели мониторинга:

- Повышение эффективности использования оборудования.
- Своевременное реагирование на аварийные ситуации.
- Наглядность процессов производства.

Функции, которые выполняет система мониторинга:

- Отслеживание текущего состояния объекта.
- Сохранение статистики состояний.
- Оповещение об аварийных ситуациях.
- Визуализация полученной информации.

Зная текущее состояние объекта, оператор может делать выводы о нормальной работе оборудования, сохранение истории этих состояний, даёт возможность восстановить ситуацию, предшествующую аварии, или получить информацию, когда оборудование простоявало, что повысит эффективность использования.

Визуализация всей полученной информации позволяет в реальном времени следить за ситуацией на предприятии, строить графики с параметрами оборудования, а также своевременно реагировать и останавливать работу оборудования, до устранения неполадок, если произошла авария.

Разрабатываемая система мониторинга, в отличие от SCADA систем [1], не нуждается в дополнительном оборудовании и поэтому реализация является чисто программной, так же системе неважно какое оборудование отслеживается, так как она ориентирована на компьютеризированное оборудование и взаимодействие с программной средой этого оборудования.

Далее будет описано, какие технологии были использованы в разработке и принципы функционирования системы.

- Среда разработки – MS Visual Studio 2010.
- Язык программирования – C# [2].
- .NET Framework 4.0.
- Windows Communication Foundation.
- Windows Presentation Foundation.
- Класс Socket.

Система строится по клиент-серверной архитектуре, то есть существует основной сервер, куда поступает вся информация от компьютеров, подключенных к технологическому оборудованию, после чего она сохраняется в базу данных и по необходимости обрабатывается и выводится на экран оператора.

WCF (*Windows Communication Foundation* [3]) специально разработанный фреймворк (*API* – интерфейс) Microsoft предназначенный для построения распределенных систем. WCF предоставляет единую, стандартную и масштабируемую объектную модель, которая позволяет взаимодействовать с большим количеством разрозненных технологий, в итоге мы получаем единый API – интерфейс, который интегрирует технологии распределенной обработки.

Windows Presentation Foundation [4] является программным фреймворком, служащий системой для построения пользовательских интерфей-

сов. Использует язык XAML (*eXtensible Application Markup Language* – расширяемый [язык разметки](#) приложений) для определения элементов пользовательского интерфейса, привязки данных, поддержки обрабатываемых событий. Но при этом остается возможность настроить весь графический интерфейс с помощью объектно-ориентированного языка C#.

Сетевое взаимодействие обеспечивает класс Socket, который позволяет использовать транспортные протоколы (*TCP, UDP*) модели OSI (*open systems interconnection*). Модель OSI ([рис. 1](#)) является базовой эталонной моделью взаимодействия открытых систем или сетевой моделью стека сетевых протоколов.

В разрабатываемой системе использовался протокол транспортного уровня UDP (*User Datagram Protocol* – протокол пользовательских [датаграмм](#)), так как в отличие от протокола TCP (*Transmission Control Protocol* – протокол управления передачей), он не требует предварительного соединения с сервером.

Предварительная установка соединения с сервером и повторные запросы потерянных пакетов не требуется, так как клиенту просто нужно отослать на сервер значения параметров оборудования.

## Модель OSI

Данные	Прикладной доступ к сетевым службам
Данные	Представления представление и кодирование данных
Данные	Сеансовый Управление сеансом связи
Блоки	Транспортный безопасное и надёжное соединение точка-точка
Пакеты	Сетевой Определение пути и IP (логическая адресация)
Кадры	Канальный MAC и LLC (Физическая адресация)
Биты	Физический кабель, сигналы, бинарная передача данных

Рис. 1. Модель OSI

UDP и TCP используют в качестве протокола сетевого уровня, протокол IP (*Internet Protocol*), который позволяет обращаться к любому удаленному компьютеру, зная его 4-байтовый IP адрес.

Рассмотрим теперь всю систему в целом, используя рисунок 2.

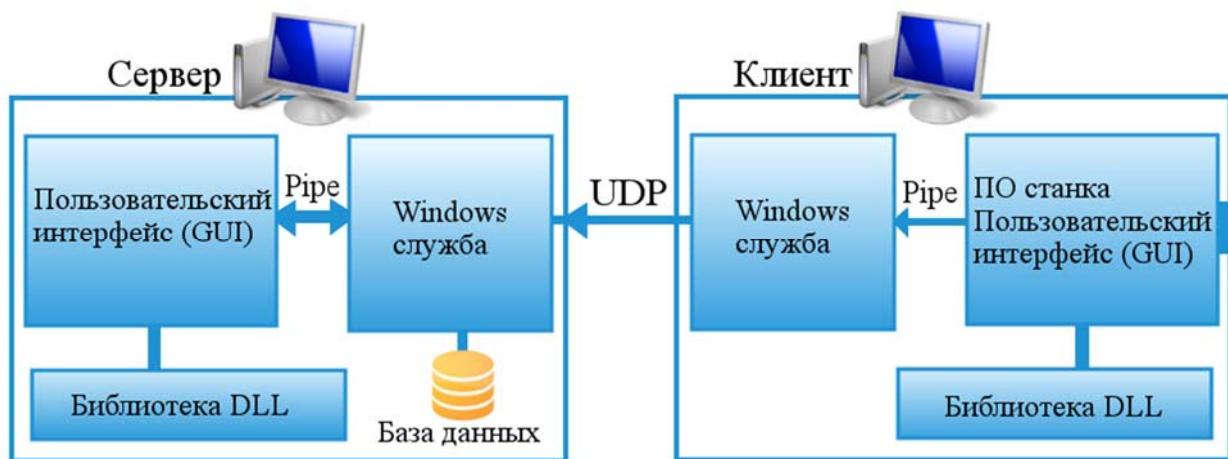


Рис. 2. Схема взаимодействия в системе

К компьютеру клиента подключено какое-либо оборудование, которые управляется с помощью программы на компьютере, предоставляется открытый WCF-интерфейс в виде DLL-библиотеки, которая подключается к ПО оборудования. Это позволяет ПО оборудования через именованный канал (*Pipe*) вызывать метод Windows службы, который отправляет информацию о параметрах оборудования на конечный сервер через UDP протокол. Также при установке Windows службы на компьютер задается его местоположение на предприятии (помещение), что поможет в 3D-визуализации или для получения информации, где именно сломалось оборудование.

Когда информация приходит на сервер, то Windows служба, которая «прослушивает» порт UDP, обрабатывает полученную информацию и сохраняет её в базу данных.

Используя WCF-интерфейс, появляется возможность использовать не только пользовательский интерфейс, разрабатываемый в данном проекте, но и подключать свои графические оболочки. Этот интерфейс позволяет вызывать метод в Windows службе, который обращается к базе данных и получает необходимую информацию. В итоге получается система мониторинга, которая не требует установки дополнительного оборудования и затрат, однако данная система не может управлять оборудованием, только отслеживать значения параметров оборудования и оповещать об авариях, хотя за пределами данного проекта функционал можно расширить и до управления оборудованием.

Данные из базы данных можно использовать в статистике, для получения графиков, для получения информации о простоях оборудования или для 3D-визуализации предприятия (рис. 3).

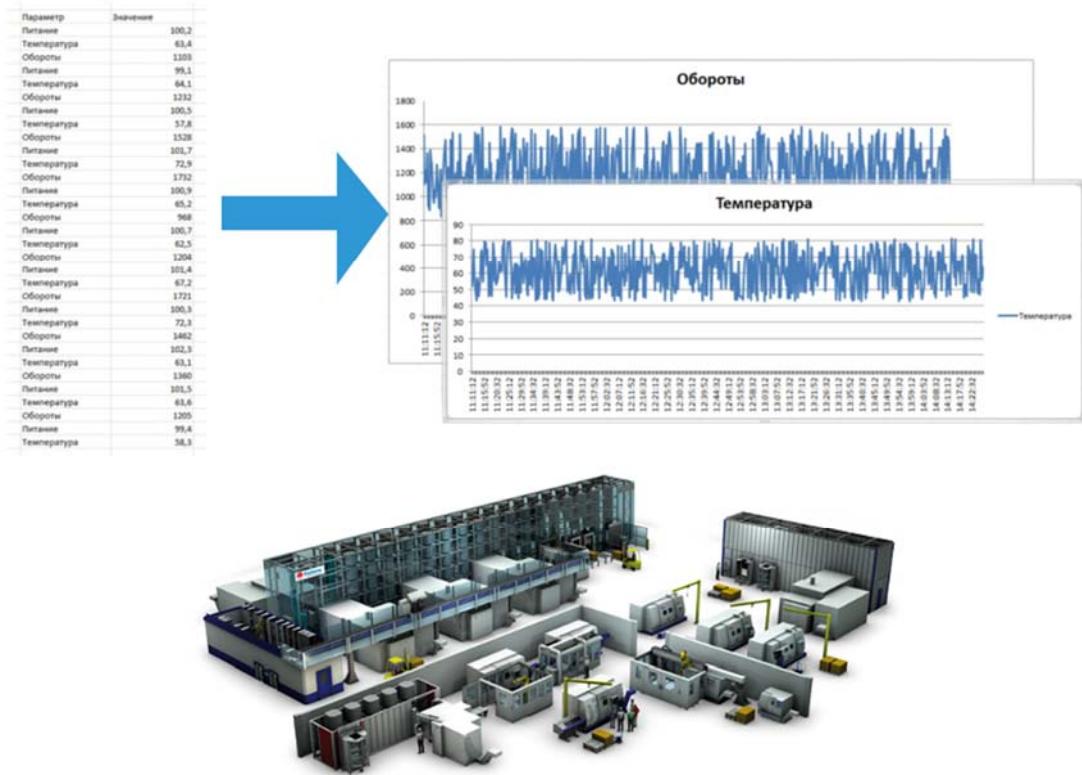


Рис. 3. Визуализация информации

Данную систему можно масштабировать, например, на несколько зданий, расширять функционал путем добавление новых методов в WCF-интерфейс (возможно создание *HTTP*-привязки *WCF*-службы, для дальнейшего использования на мобильных устройствах, где необходимо будет разработать отдельные приложения со своей визуализацией) и добавление возможности управлять оборудованием. Также с учетом того, что компьютерам присваивается идентификатор и указывается место их расположения, то возможно расширить функционал клиентской Windows службы, для передачи данных о том, что происходит на компьютере (какие программы запущены и сколько они потребляют памяти, сколько сетевого трафика потребляет пользователь и т. п.)

#### Список используемых источников

1. SCADA-системы: взгляд изнутри / Е. Б. Андреев, Н. А. Куцевич, О. В. Синенко. – М. : РТСофт, 2004. – 176 с.
2. Язык программирования C# 2010 и платформа .NET 4 / Э. Троелсен. – М. : Вильямс, 2011. – 1392 с.
3. Создание служб WCF / Д. Леве. – СПб. : Питер, 2008. – 592 с.
4. WPF 4. Подробное руководство / Н. Адам. – СПб. : Символ-Плюс, 2011. – 880 с.

Статья представлена научным руководителем канд. техн. наук, доцентом С. В. Акимовым.

УДК 621.391.28

**Н. Н. Мошак (студент группы ИСТ-91СПбГУТ)**

## **МОДЕЛЬ КАНАЛА СВЯЗИ УЛЬТИСЕРВИСНОЙ БАНКОВСКОЙ СЕТИ НА ТЕХНОЛОГИИ *IP/FRAME RELAY***

Мультисервисные сети связи (МСС) обеспечивают интегральное обслуживание различных видов информации (речи, телевизионной, графической, факсимиле, телеметрии, данных др.), представленной в цифровой форме, в общей физической среде. В зависимости от требований к доставке трафика в МСС возможны три стратегии использования физических сетевых ресурсов (пропускной способности каналов связи, вычислительной мощности и емкости буферной памяти маршрутизаторов) в режиме установленного соединения. Соответственно возможны и три стратегии построения коммуникационного ядра МСС или ее транспортной системы (ТС) [1]:

- ТС с детерминированным или «жестким» закреплением физических ресурсов – КТС;
- ТС с динамическим или «нежестким» закреплением ресурсов – ПТС;
- ТС с гибридным закреплением физических ресурсов – ГТС.

В мультисервисной банковской сети на технологии IP/FrameRelay реализована гибридная ТС. В ней для речевого и факсимильного трафика физические ресурсы в сеансе связи закрепляются в режиме TDM (детерминировано) без возможности перераспределения между другими соединениями, а для трафика данных – динамически, т. е. физические ресурсы соединению предоставляются на коллективной основе с образованием очередей. Непременным атрибутом архитектуры МСС является функция «совмещения» разнородного трафика, позволяющая «окрасить» соединение типом трафика с целью организации соответствующей дисциплины его обслуживания на транзитных маршрутизаторах [1]. В архитектуре мультисервисной банковской сети на технологии IP/FrameRelay функция «совмещения» разнородного трафика реализована на уровне сетевого доступа протоколом FrameRelay.

Одной из главных задач при проектировании любой сети связи является разработка инженерных методов расчета основных числовых характеристик ее транспортных соединений. Наиболее естественной методологической базой для построения указанных методов расчета, удовлетворяющих перечисленным выше требованиям, является концепция архитектуры сети. В рамках этой концепции, эффективность сети в режиме установленного соединения предлагается оценивать набором функциональных критериев использования пропускной способности ЛЦТ разнородным трафиком

применительно к каждой паре «отправитель-получатель», при заданных условиях передачи (например, среднее время пребывания кадров данных в сети фиксировано и т. д.), т. е. на транспортном уровне ТС выступает как набор трактов передачи [1]. Согласно логической структуре архитектуры МТКБС общие критерии эффективности использования пропускной способности ЛЦТ  $K_{ЛЦТ}$  должны «расслоиться» на критерии эффективности использования пропускной способности ЛЦТ отдельных уровней архитектуры сети, которые зависят от протоколов функционирования данного уровня и необходимой для их работы служебной информации соответствующих объемов. При этом  $K_{ЛЦТ}$  должны учитывать все затраты на реализацию соответствующих протоколов сети (избыточность протокольных блоков на управление и борьбу с ошибками, задержки в очередях и т. п.). Оптимизируя эти критерии, можно получить оптимальные для заданных условий передачи величины протокольных блоков различных логических уровней и допустимые режимы их передачи, а также определить оптимальные загрузки каналов связи с учетом требований на передачу трафика различной природы.

Пусть каждый уровень архитектуры ТС МТКБС характеризуется своим критерием эффективности использования пропускной способности ЛЦТ речевым трафиком  $K_{h,ЛЦТ}^B$  ( $h=1$ ) и трафиком данных  $K_{h,ЛЦТ}^C$  ( $h=3$ ). В силу относительной независимости уровней архитектуры друг от друга и «вложенности» протокольного блока каждого уровня в протокольный блок более низкого уровня общие критерии эффективности использования пропускной способности ЛЦТ обладают мультипликативным свойством и соответственно равны:

$$K_{ЛЦТ}^B = K_{FR,ЛЦТ}^B,$$
$$K_{ЛЦТ}^C = \prod_{h=1}^3 K_{h,ЛЦТ}^C = \prod K_{TCP,ЛЦТ}^C \times K_{IP,ЛЦТ}^C \times K_{FR,ЛЦТ}^C. \quad (1)$$

Общие критерии эффективности использования пропускной способности определяют требуемую долю пропускной способности ЛЦТ –  $V_{ЛЦТ}$  для передачи разнородного трафика (речи и данных). Здесь  $h$  – номер логического уровня модели архитектуры ТС МТКБС: соответственно – транспортного, межсетевого взаимодействия и сетевого интерфейса для трафика данных и сетевого интерфейса – для речевого трафика). Введем следующие обозначения:  $b_c$  – коэффициенты, учитывающие механизм организации обратной связи на транспортном уровне (протокол TCP) с целью защиты от ошибок соответствующих сегментов. В предположении, что распределение числа переспрашиваемых пакетов подчиняется геометрическому закону и кадры независимы друг от друга, то для каналов ЛЦТ с решающей обратной связью

$$\beta^C = -\frac{p_0}{1-p_0} \ln p_0,$$

(здесь  $p_0$  – вероятность отсутствия ошибок в пакете данных длины  $L_c + H_{ip}$ );  $p_c$  – коэффициенты загрузки межсетевого уровня пакетами данных;  $L_b$  – длина речевого пакета, бит;  $L_c$  – длина пакета данных, бит;  $H_{ip}$  – длина IP-заголовка, бит;  $H_{tcp}$  – длина заголовка TCP-сегмента данных, бит;  $H_{fr}$  – длина заголовка протокольного блока сетевого интерфейса;  $S_c$  – средняя длина сообщения данных на транспортном уровне, включая связной заголовок транспортного уровня, бит;  $N_c$  – среднее число информационных частей пакета данных в сегменте данных на транспортном уровне.  $w_c$  – скорость работы абонентской установки данных, бит/с;  $T_c$  – заданное среднее время пребывания в тракте пакета данных, включающее в себя время накопления информационной части пакета у абонента, равное  $(L_c - H_{tcp})/w_c$ , с.

Воспользовавшись введенными выше обозначениями можно показать, что с учетом (1) выражения для указанных критериев соответственно имеют следующий вид

$$K_{ЛЦТ}^B = \frac{L^B}{L^B + H_{FR}}, K_{ЛЦТ}^C = \frac{S^C \rho_{ЛЦТ}^C \beta_{ЛЦТ}^C}{N^C (L^C + H_{IP} + H_{FR})}.$$

В предположении, что процесс передачи речевого трафика в канале связи МТКБС моделируется полнодоступным пучком марок минимальной емкости, а процесс передачи трафика данных – однофазной однолинейной СМО типа M/M/1 [2], математическая модель канала передачи ЛЦТ для изохронного трафика (например, речевой и факсимильный трафик) в режиме установленного виртуального соединения (с учетом потерь по вызовам  $b_{ЛЦТ}$ ) имеет вид:

$$V_{ЛЦТ}^B = \frac{L^B}{L^B + H_{FR}} Mark^B c_{min} Y_{ЛЦТ}^B (1 - b_{ЛЦТ}).$$

Суммарная марка речевого и факсимильного трафика (число полос базовой минимальной пропускной способности ЛЦТ)  $c_{min}$ , требуемых для обслуживания всего изохронного трафика в ЛЦТ

$$Mark^B = \sum_{k=1}^K \left\lceil \frac{\nu_{речь}}{c_{min}} \right\rceil + \sum_{n=1}^N \left\lceil \frac{\nu_{факс}}{c_{min}} \right\rceil,$$

где  $\lceil$  – знак наибольшего целого;  $\nu_{речь}$  и  $\nu_{факс}$  – минимальная скорость передачи соответственно речевого и факсимильного трафика в виртуальном канале, бит/с.

Учитывая, что с введением избыточности на FR-уровне в кадры изохронного трафика максимальная скорость его передачи в ЛЦТ равна:

$$V_{ЛЦТ}^{B_{max}} = \frac{L^B}{L^B + H_{FR}} V_{ЛЦТ}.$$

Трафик данных обслуживается оставшейся эффективной пропускной способностью ЛЦТ, т. е. той его частью, которая остается за вычетом числа полос базовой минимальной пропускной способности ЛЦТ, необходимых для обслуживания пропущенной изохронной нагрузки

$$V_{\text{ЛЦТ}}^{\mathcal{E}} = \frac{L^B}{L^B + H_{FR}} V_{\text{ЛЦТ}} - \frac{L^B}{L^B + H_{FR}} \text{Mark}^B c_{\min} Y_{\text{ЛЦТ}}^B (1 - b_{\text{ЛЦТ}}).$$

Математическая модель канала передачи ЛЦТ для трафика данных имеет вид:

$$V_{\text{ЛЦТ}}^C = V_{\text{ЛЦТ}}^{\mathcal{E}} K_{\text{ЛЦТ}}^C = V_{\text{ЛЦТ}}^{\mathcal{E}} \times \left( \frac{L^C - H_{TCP}}{L^C + H_{IP} + H_{FR}} \left( 1 - \frac{L^C + H_{IP}}{\left( T_{\text{ЛЦТ}}^C - \frac{L^C - H_{IP}}{\omega^C} \right) V_{\text{ЛЦТ}}^{\mathcal{E}}} \right) \right) - \frac{p_0}{1 - p_0} \ln p_0.$$

Показателем качества работы МТКБС IP/FR может служить коэффициент использования ЛЦТ на транспортном уровне, который может быть подсчитан по формуле:

$$R = \frac{V_{\text{ЛЦТ}}^B + V_{\text{ЛЦТ}}^C}{V_{\text{ЛЦТ}}}.$$

На базе предложенных математических моделей разработаны алгоритмы расчета основных числовых характеристик каналов связи ЛЦТ МТКБС IP/FR в режиме установленного транспортного соединения. Результаты расчета параметров канала связи МТКБС IP/FR в зависимости от величины входной речевой нагрузки (факсимильный трафик отсутствует) для  $\text{Mark}b = 2$ ,  $c_{\min} = 8000$  бит/с,  $v^{\text{речь}} = 8000$  бит/с,  $L_b = 1600,0$  бит,  $b_{\text{ЛЦТ}} = 0,005$ ,  $V_{\text{ЛЦТ}} = 512000$  бит/с,  $H_{fr} = 24$  бт,  $H_{ip} = 320$  бит,  $H_{tcp} = 192$  бит.  $T_{\text{ЛЦТ},c} = 2,0$  с,  $w_c = 64000$  бит/с – представлены в таблице.

ТАБЛИЦА. Зависимость значений параметров канала связи МТКБС от величины входной речевой нагрузки

$Y_{b,\text{ЛЦТ}}$ , Эрл	$V_{b,\text{ЛЦТ}}$ , бит/с	$V_{e,\text{ЛЦТ}}$ , бит/с	$V_{c,\text{ЛЦТ}}$ , бит/с	$L_c$ , бит	$R$
1	15684,73	488748,77	464204,4	18802,58	0,937283
2	31369,46	473064,04	448954,1	18554,81	0,938132
3	47054,19	457379,31	433710	18301,03	0,938992
4	62738,92	441694,58	418472,2	18040,92	0,939866
5	78423,65	426009,85	403241,3	17774,11	0,940752
6	94108,37	410325,12	388017,6	17500,24	0,941652
7	109793,1	394640,39	372801,4	17218,89	0,942567
8	125477,8	378955,67	357593,3	16929,57	0,943498

$Y_{b,\text{лцт}}$ Эрл	$V_{b,\text{лцт}}$ бит/с	$V_{\varnothing,\text{лцт}}$ бит/с	$V_{c,\text{лцт}}$ бит/с	$L_c$ , бит	$R$
9	141162,6	363270,94	342393,8	16631,8	0,944446
10	156847,3	347586,21	327203,4	16325	0,945412

Общий характер зависимости эффективности передачи от величины входного речевого трафика следующий: с ростом входной речевой нагрузки эффективность использования пропускной способности ЛЦТ растет.

#### Список используемых источников

1. **Теоретические** основы проектирования транспортной системы инфокоммуникационной сети: учеб. пособие / Н. Н. Мошак. – СПб. : Энергомашиностроение, 2006. – 159 с.
2. **Вычислительные** системы с очередями / Л. Клейнрок. – М. : Мир, 1979. – 600 с.

*Статья представлена научным руководителем, доцентом А. В. Перервенко.*

**УДК 004.422**

**М. М. Осипенко (студент группы ИСТ-341 СПбГУТ)**

## **РАЗРАБОТКА СИСТЕМЫ АВТОМАТИЧЕСКОЙ ТРАНСЛЯЦИИ ДАННЫХ ИЗ ТАБЛИЦ РАСПИСАНИЙ ЗАНЯТИЙ, ПРЕДСТАВЛЕННЫХ В ФОРМАТЕ *EXCEL* В ТАБЛИЦЫ СУБД *MySQL***

#### *Цели и задачи проекта*

Целью данного проекта является частичная автоматизация сложных и трудоемких процессов составления расписания занятий в вузе с использованием современных средств информационных технологий (ИТ).

Основная задача проекта – трансляция данных из существующих таблиц MS Excel в таблицы СУБД MySQL.

#### *Актуальность проекта*

Актуальность проекта обусловлена низкой автоматизацией и высокой трудоемкостью процессов формирования расписания занятий в вузе.

Практическая значимость данной работы состоит в возможности использования ее результатов при решении задач полной автоматизации составления расписания для вуза.

### *Методы решения поставленной задачи*

Для решения поставленной задачи используется свободное открытое программное обеспечение (ПО), распространяемое по лицензии GNU/GPL.

Пользовательский интерфейс разрабатывался на основе web-технологий, что обусловлено отсутствием необходимости установки дополнительного программного обеспечения на компьютере конечного пользователя. В качестве основного языка программирования был выбран язык PHP [1], так как этот язык стал практически одним из стандартов, используемых при разработки web-приложений.

В качестве СУБД была выбрана MySQL [2], которая распространяется также по лицензии GNU/GPL и позволяет решать задачи любой сложности, связанные с построением и использованием баз данных.

### *Постановка задачи*

Исходными данными для решения задачи являются таблицы MS Excel 2003 [3]. Сложность поставленной задачи заключается в использовании в таблицах объединенных ячеек с данными. Классические библиотеки языка PHP позволяют легко считывать данные из таблиц MS Excel по ячейкам только при отсутствии объединенных ячеек.

Исходя из условий поставленной задачи данные из таблиц MS Excel (фрагмент исходной таблицы показан на рис. 1) должны быть транслированы в таблицы реляционной базы данных, имеющие структуру, приведенную на [рисунке 2](#).

День недели	Время Группа	Код направления (специальности) 210700.62					
		ИКТ - 201	ИКТ - 202	ИКТ - 203	ИКТ - 204	ИКТ - 205	ИКТ - 206
ПОНЕДЕЛЬНИК	9.00-10.35	ИКГ, пр. Волков, Колесникова, еж., 3-17н, а. 514/2, 518/2				ВТиИТ, лаб. Неелова, Желтова, чет/нед, 4-16н, а. 508/1	
			ВТиИТ, пр. Неелова, неч/нед, 3-17н, а. 508/1	ИКГ, пр. Джакония, Соловьева, неч/нед, 3-17н, а. 510/2, 516/2	ОТС, пр. Щербатый, неч/нед, 3-17н, а. 709/1	ВТиИТ, пр. Воронцова, неч/нед, 3-17н, а. 501/1	
		Вычислительная техника и информационные технологии (ВТиИТ), лекция, доц. О.Л. Неелова, 1н, а. 110/1					
	10.45-12.20	ВТиИТ, лаб. Игнатьев, Губанова, чет/нед, 4-16н, а. 508/1	Электроника, пр. Бочаров, 2,4,10,18н, а. 646/1, лаб. Бочаров, 6,8,12,14н, а. 646/1			ОЗИТ, лаб. чет/нед, 4-16н, а. 603/1	
Вычислительная техника и информационные технологии (ВТиИТ), лекция, доц. О.Л. Неелова, неч/нед, 1-17н, а. 110/1							

Рис. 1. Пример исходной таблицы в формате Excel

Колонка	Тип	Комментарий
<code>id</code>	<code>int(11)</code> Автоматическое приращение	Идентификатор записи
<code>group_id</code>	<code>int(11)</code>	Идентификатор группы
<code>den_ned</code>	<code>varchar(50)</code>	День недели
<code>time_para</code>	<code>varchar(50)</code>	Время «пары» по расписанию
<code>predmet</code>	<code>varchar(50)</code>	Дисциплина
<code>rod</code>	<code>varchar(50)</code>	Род работы
<code>prepod1</code>	<code>varchar(50)</code>	Преподаватель 1
<code>prepod2</code>	<code>varchar(50)</code>	Преподаватель 2
<code>prepod3</code>	<code>varchar(50)</code>	Преподаватель 3
<code>time1</code>	<code>varchar(50)</code>	Дни недели, когда «пара» проводится
<code>aud</code>	<code>varchar(50)</code>	Номер аудитории

Рис. 2. Структура таблицы СУБД MySQL

### Алгоритм решения поставленной задачи

Как отмечено выше, исходным материалом для решения поставленной задачи, являются данные о расписании в формате MS Excel ([рис. 3](#)). Данные из таблицы Excel считывается PHP программой с использованием специальной библиотеки «ExcelReader». Далее необходимо их корректно «разложить» по ячейкам таблицы БД MySQL. Предварительно перед этим производится следующая проверка:

- является ли ячейка таблицы Excel объединенной, и если да, то данные обрабатываются с помощью специального алгоритма, позволяющего получить корректные значения;
- определяется количество преподавателей, ведущих занятия, и записывается ФИО каждого преподавателя в соответствующее поле;
- учитывается формат учебных недель и эти значения записываются в соответствующие поля.

После анализа всех данных, полученных из таблицы Excel, и выполнения соответствующей обработки программа загружает данные в таблицу СУБД MySQL.

### Заключение

На основании полученных результатов можно сделать следующие выводы:

- при создании удобного web-интерфейса конечный пользователь ПК (работник группы расписания) может значительно сократить время, необходимое на составление расписания;
- данная разработка является первыми фундаментальным шагом к полной автоматизации процесса составления расписания.

### Список используемых источников

1. **Разработка** веб-приложений с помощью PHP и MySQL / Л. Веллинг, Л. Томсон. – М. : Вильямс, 2010. – 837 с.
2. MySQL на примерах / М. Кузнецов, И. Симдянов. – СПб. : БХВ-Петербург, 2007. – 592 с.
3. Использование макросов в Excel / С. Роман. – СПб. : Питер, 2004. – 507 с.

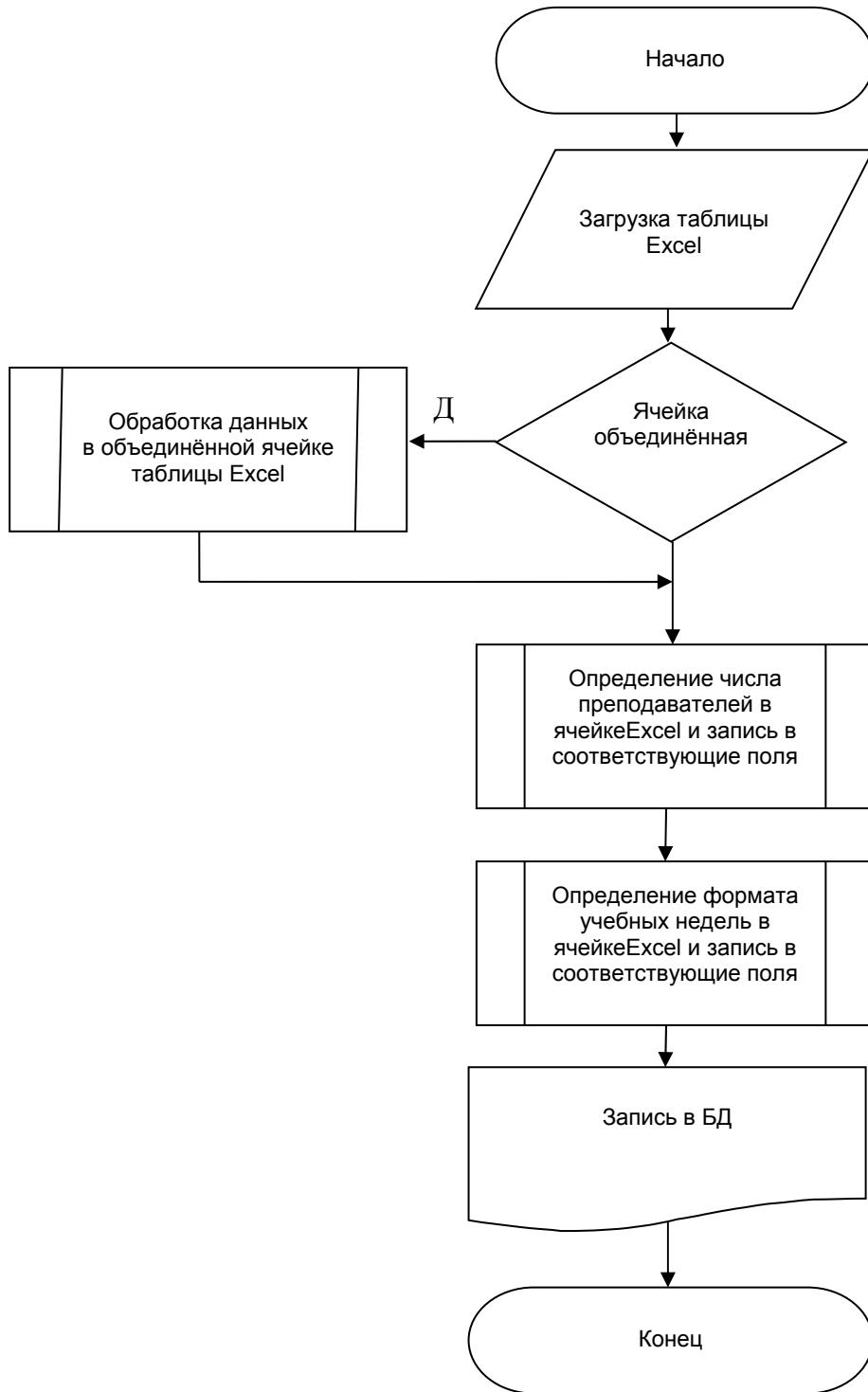


Рис. 3. Обобщенная структура работы системы

*Статья представлена научным руководителем, старшим преподавателем  
В. А. Евстигнеевым.*

УДК 654.026

Е. В. Плотникова (аспирант кафедры ИКД СПбГУТ)

## СРАВНЕНИЕ СТАТИСТИЧЕСКИХ ПАРАМЕТРОВ РЕЧЕВЫХ СИГНАЛОВ ГОРТАННОЙ И ПРОИЗНОСИМОЙ ВСЛУХ РЕЧИ

В процессе речеобразования воздух из легких проходит через трахею, голосовые связки, гортань и затем разветвляется на два потока: носовую и горловую полость [1]. Основная идея беззвучной речи, состоит в том, чтобы снять речевой сигнал в области гортани, до произношения его вслух.

Для того чтобы сравнить речевые сигналы гортанной речи и речи произнесенной вслух записаны два аудиофайла, в которых диктором произносится одинаковое слово. В «Файл 1» записана речь, произнесенная вслух (рис. 1), в «Файл 2» записано слово, произнесенное гортанной речью (рис. 2).

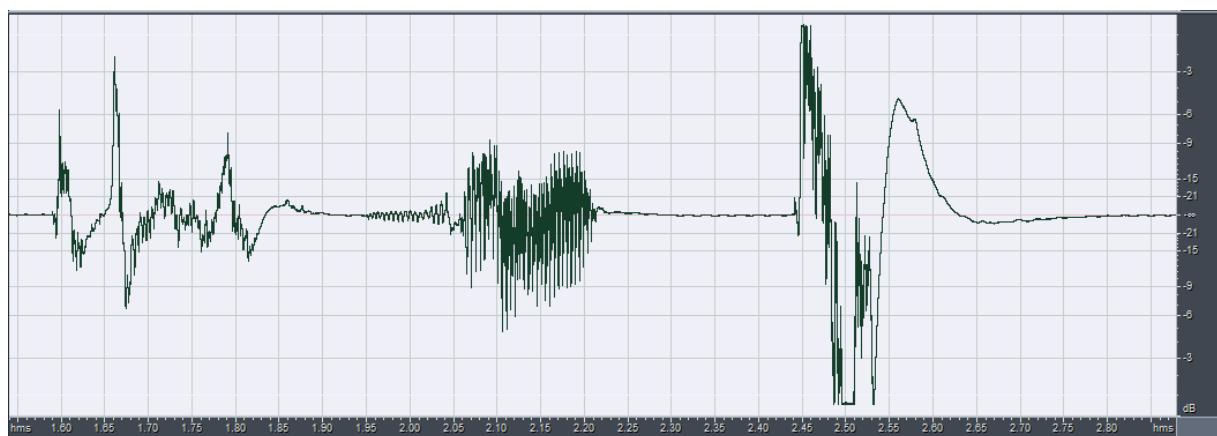


Рис. 1. Волновая форма «Файла 1»

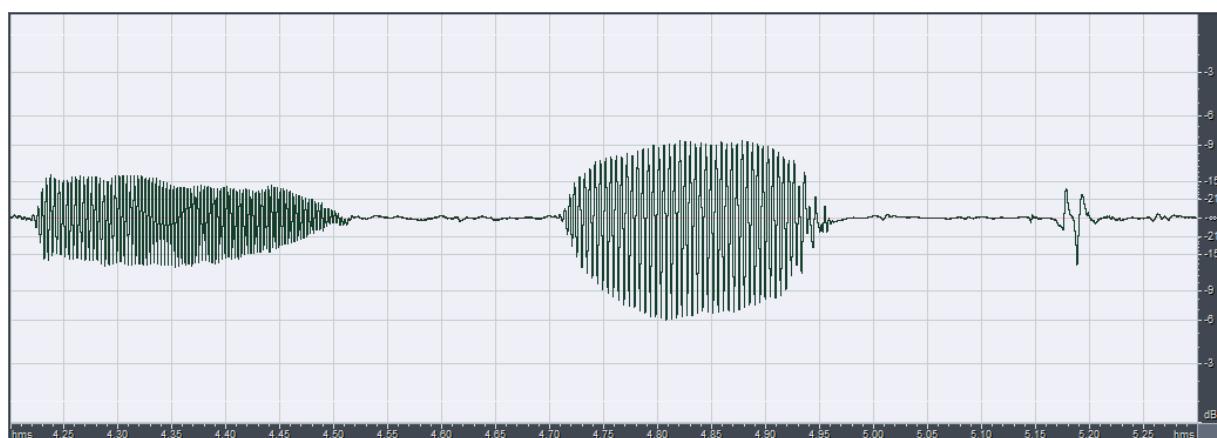


Рис. 2. Волновая форма «Файла 2»

На данном этапе сравнение будет происходить по статистическим характеристикам сигнала, не учитывая характеристики разборчивости и ка-

чества записанной в файлы речи. Сбор статистической информации о волновой форме осуществляется по параметрам. Значение параметров для «Файла 1» и «Файла 2» отображены в таблице. Количество клипированных отсчетов показывает количество отсчётов, имеющих уровень максимальной или минимальной границы характеристики аналого-цифрового преобразователя. Среднее значение отсчетов описывает уровень постоянной составляющей волновой формы [2].

ТАБЛИЦА. Статистическая информация о параметрах волновой формы «Файла 1» и «Файла 2»

Параметр	Файл 1		Файл 2	
Стерео/монофонического сигнала	стерео		стерео	
	Левый	Правый	Левый	Правый
Минимальное значение звукового отсчета	-30839	-30833	-16547	-16412
Максимальное значение звукового отсчета	30894	30896	12533	12441
Пиковая амплитуда сигнала	-53 дБ	-53 дБ	5,93 дБ	6 дБ
Количество клипированных отсчетов	0	0	0	0
Среднее значение отсчетов	-312 %	-311 %	-019 %	-019 %
Минимальное среднеквадратическое значение сигнала	-48,43 дБ	-48,47 дБ	-53,03 дБ	-53,08 дБ
Максимальное среднеквадратическое значение сигнала	-3,15 дБ	-3,14 дБ	-10,97 дБ	-11,04 дБ
Среднеквадратическое значение сигнала	-13,13 дБ	-13,14 дБ	-17,87 дБ	-17,94 дБ
Фактическая разрядность представления звуковых данных	16 Бит		16 Бит	
Установленный размер временного окна для расчета среднеквадратичных значений	50 мс	50 мс	50 мс	50 мс

Максимальное среднеквадратическое значение сигнала «Файла 1» равно -3,15 дБ, из чего следует что положительный результат может дать ограничение сигнала на уровне -3 дБ с последующим усилением на 3 дБ. Для «Файла 2» максимальное среднеквадратическое значение сигнала равно -10,97 дБ, соответственно положительный результат может дать ограничение сигнала на уровне -10 дБ с последующим усилением на 10 дБ.

Для анализа распределения значений отсчетов рассмотрим гистограммы левой части записанного стереосигнала «Файла 1» ([рис. 3](#)) и «Файла 2» ([рис. 4](#)). Гистограмма представляет собой график зависимости количества

отсчетов, среднеквадратическое значение от величины отсчета, выраженной в децибелах. Гистограмма – широко распространенная (особенно в вероятностном анализе) форма представления информации о каком-либо случайном процессе. Анализ гистограмм сигналов позволяет оптимально принимать решения об их обработке. В нашем случае используем гистограмму для сравнения параметров записанных сигналов.

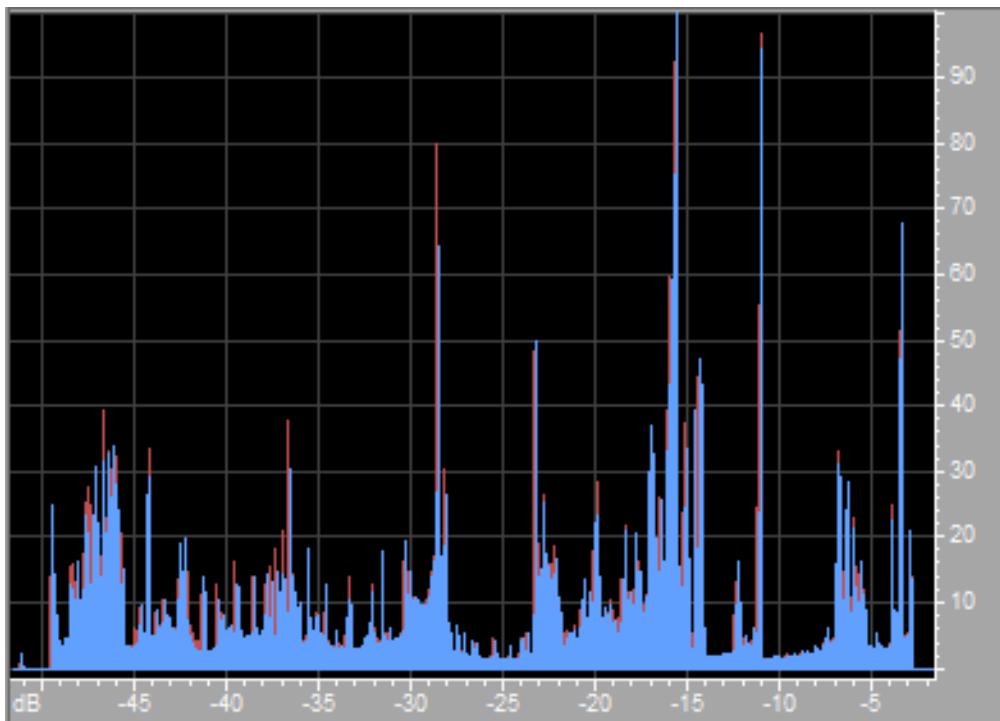


Рис. 3. Гистограмма сигнала «Файл 1»

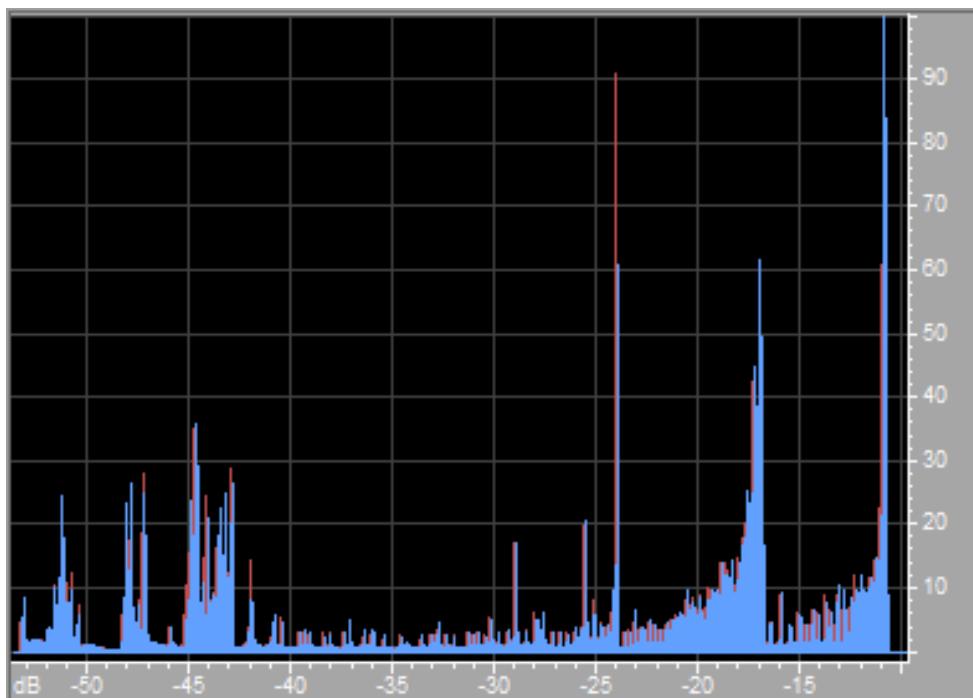


Рис. 4. Гистограмма сигнала «Файл 2»

Во-первых, следует проанализировать поведение графика, уменьшении или увеличении уровня среднеквадратического значение сигнала. В «Файле 1» уменьшение проявляется на 5, 10, 12, 25, 33, 40, 45 дБ. В «Файле 2» на 15, 20–43, 47, 50 дБ. Полученные данные определяют значения отсчетов, при которых можно использовать пороговое шумоподавление, но в процессе обработки их следует уточнить, контролируя результат на слух. Также по данным видно, что гистограмма второго файла обладает большим количеством шума, полученной при записи слова.

Во-вторых, из анализа гистограммы Записи 1 следует, что доля отсчетов, уровень которых превышает –8 дБ, чрезвычайно мала, а превышающих –1 дБ – практически нет. Если точнее, то следует вспомнить, что максимальное среднеквадратическое значение сигнала –3,14 дБ (табл.). Поэтому положительный результат может дать ограничение сигнала на уровне –3 дБ с последующим усилением на 3 дБ.

Для более информативного анализа гистограмм, потребуется записать файлы с большей информацией, порядка 30 слов.

Статистические характеристики сигнала, не выявили сходства сигналов «Файла 1» и «Файла 2», но полученные данные в дальнейшем помогут в обработке сигналов, позволяют при минимальных искажениях максимально увеличить среднюю энергию сигнала и уменьшить уровень шума.

#### **Список используемых источников**

1. Расчет и измерение качества речевых сигналов / М. Н. Гусев, В. М. Дегтярев. – СПб. : Геликон Плюс, 2008. – 277 с.
2. Cool Edit Pro 2 Секреты мастерства / Р. Петелин, Ю. Петелин. – СПб. : БХВ-Петербург Арлит, 2002. – 429 с.

*Статья представлена научным руководителем д-ром техн. наук, профессором В. М. Дегтяревым.*

**УДК 004.421**

**И. С. Пономарев (студент группы ИСТ-341м СПбГУТ)**

#### **РАЗРАБОТКА ГЕНЕТИЧЕСКОГО АЛГОРИТМА СИНТЕЗА ЭЛЕКТРИЧЕСКИХ ЦЕПЕЙ**

Любую электрическую цепь можно представить как многомодульную систему, которая отражает конкретную структуру цепи и набор параметров. Следовательно, для построения цепи, с целью получения требуемого

результата, необходимо реализовывать структурно-параметрический синтез. Для этого актуально использовать генетические алгоритмы.

Рассматриваемая в статье методология является шаблоном разработки генетических алгоритмов для синтеза лестничных цепей. По ней разрабатывался генетический алгоритм для САПР Multisim [1].

При решении практических задач с использованием генетических алгоритмов, необходимо выполнить четыре предварительных этапа [2]:

- выбрать способ представления решения;
- разработать операторы случайных изменений;
- определить законы выживания решения;
- создать начальную популяцию.

Каждая лестничная цепь представлена в виде хромосомы. Хромосома содержит список морфологических параметров, который включает порядок цепи (количество подсхем) и тип соединения первой подсхемы, с помощью которого можно определить тип подключения любой последующей подсхемы благодаря чередованию. Генотип хромосомы является списком комплексных генов. Каждый ген в генотипе является комплексным объектом, содержащим несколько типов данных, описывающих структуру подсхемы. Структуры хромосомы и комплексного гена, используемые в алгоритме, изображены на рисунке 1.



Рис. 1. Представление лестничной цепи

Структурный идентификатор является генератором набора компонентов для подсхемы. Он включает в себя номер типа структуры и сам набор компонентов. Для генерации каждого типа компонента указываются нижние и верхние пределы рабочих номиналов. Структура подсхемы определяется случайно сгенерированным числом. Это число указывает на вид структуры в заранее определенном наборе.

Начальная популяция генерируется следующим образом:

- устанавливается размерность популяции (количество хромосом);
- указывается максимальный порядок цепи (максимальное количество подсхем);
- выполняется общий цикл создания хромосом размерностью, указанной в размере популяции.

В общем цикле сначала создается пустая хромосома. В морфологические параметры хромосомы добавляются случайно сгенерированные порядок цепи и тип подключения первой подсхемы (последовательное или параллельное). Далее выполняется внутренний цикл по созданию комплексных генов размерностью, указанной в порядке цепи.

В начале цикла создания генов случайным образом генерируется тип структуры, который далее передается в структурный идентификатор. В нем задаются пределы номиналов и, на основании типа структуры, генерируется список компонентов с их номиналами. Структурный идентификатор передается в комплексный ген. В соответствии с ним в комплексном гене создается пара списков компонентов и номиналов. После указанных действий комплексный ген добавляется в генотип хромосомы. Цикл будет выполняться до тех пор, пока не будет создано нужное для хромосомы количество генов. Алгоритм генерации начальной популяции представлен на рисунке 2.

Закон выживания решения (целевая функция) определяется характером требуемого поведения искомой цепи. В качестве примера рассмотрим фильтр нижних частот.

Для вычисления целевой функции вводятся два значения частоты, т. к. реальные фильтры не способны мгновенно изменять коэффициент передачи. Первое значение – частота среза  $f_{\text{ср}}$ , до значения которой коэффициент передачи фильтра должен составлять 1. Второе – частота заграждения  $f_3$ , после которого коэффициент должен равняться 0.

Целевой функцией является сумма максимальных отклонений значений коэффициента передачи в зонах пропускания и заграждения от требуемых значений. Минимальная целевая функция считается лучшей. Эти отклонения вычисляется следующим образом:

$$\begin{aligned} K_1 &= \min(K(f)), \text{ при } f \in [0; f_{\text{ср}}] \\ K_2 &= \max(K(f)) \text{ при } f \in [f_3; \infty) \end{aligned} \quad (1)$$

В настоящем алгоритме целевая функция на 70 % учитывает отклонение в зоне заграждения, а на 30 % учитывает отклонение в зоне пропускания. При таких долях учета она вычисляется по следующей формуле:

$$K = 0,3 * (1 - K_1) + 0,7 * K_2 \quad (2)$$

Все описанные выше показатели отображены на примере АЧХ представленном на рисунке 3.

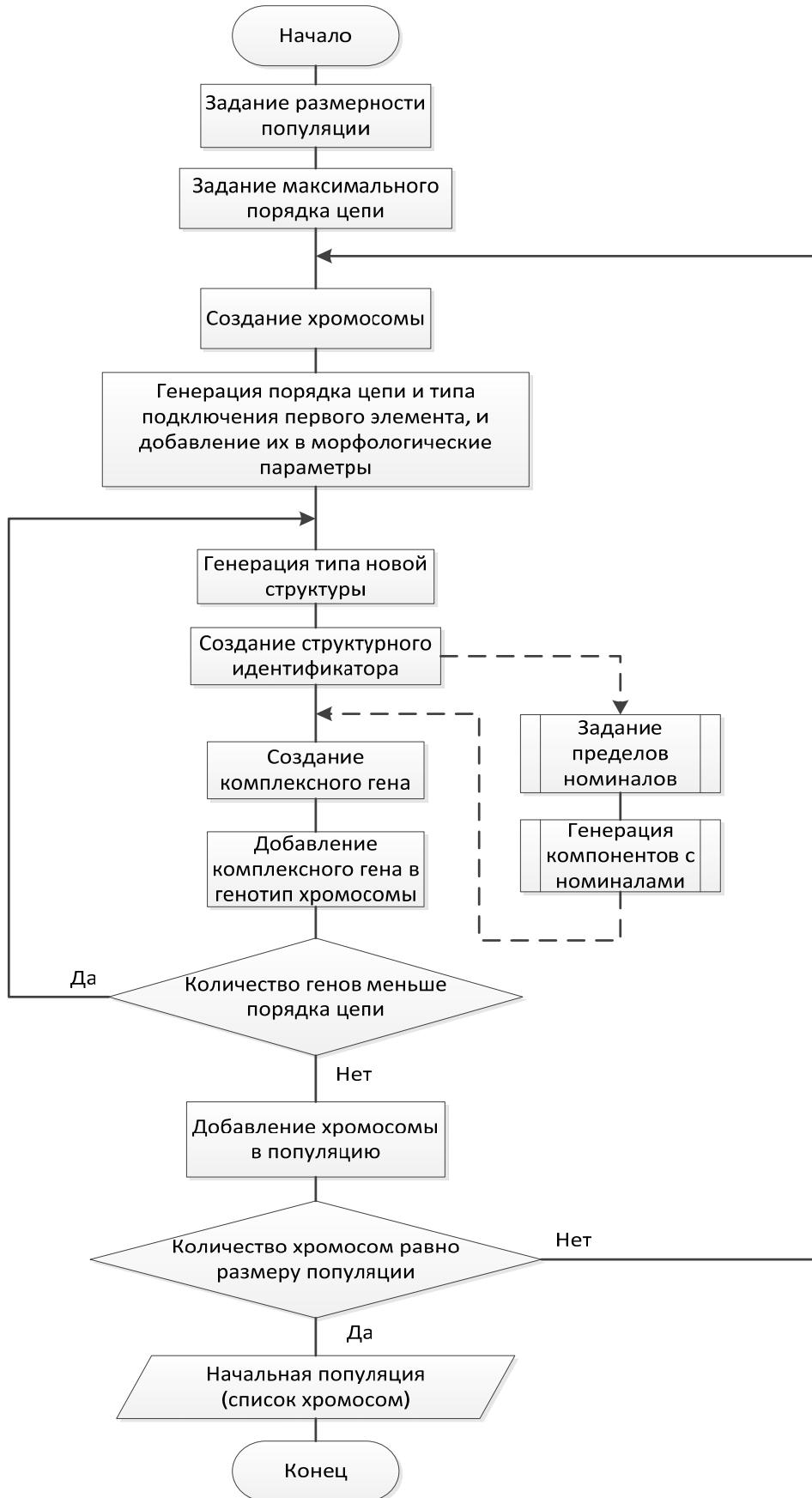


Рис. 2. Алгоритм генерации начальной популяции

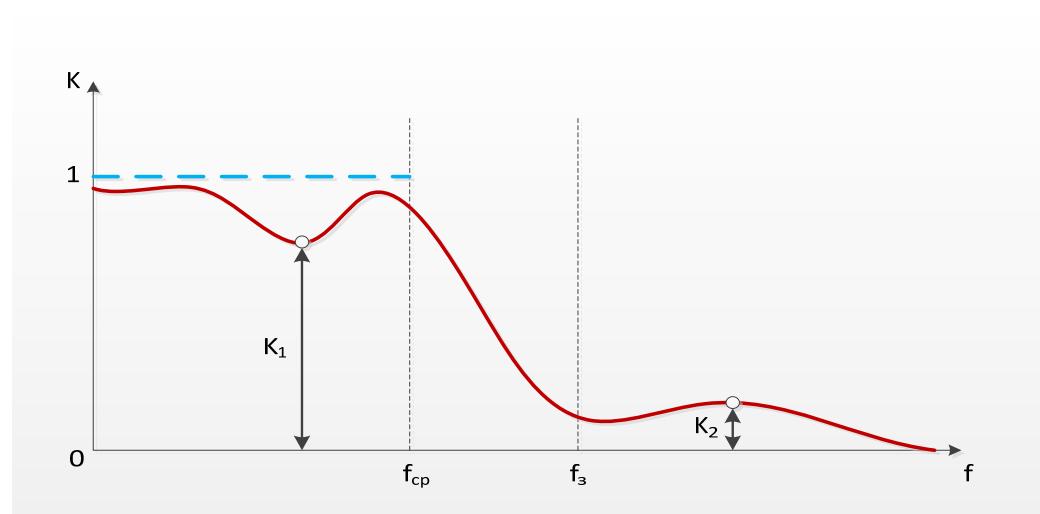


Рис. 3. Пример АЧХ с отображением параметров целевой функции

В качестве генетического оператора выступает одноточечный кроссинговер. В настоящем алгоритме используются хромосомы различной длины, что отличает его от классического генетического алгоритма, и выполнения операции кроссинговера в нем. При реализации кроссинговера предполагается целочисленно разделять хромосомы надвое и обменивать их половины между собой, учитывая чередование подсхем (рис. 4). Алгоритм реализации кроссинговера представлен на рисунке 5.

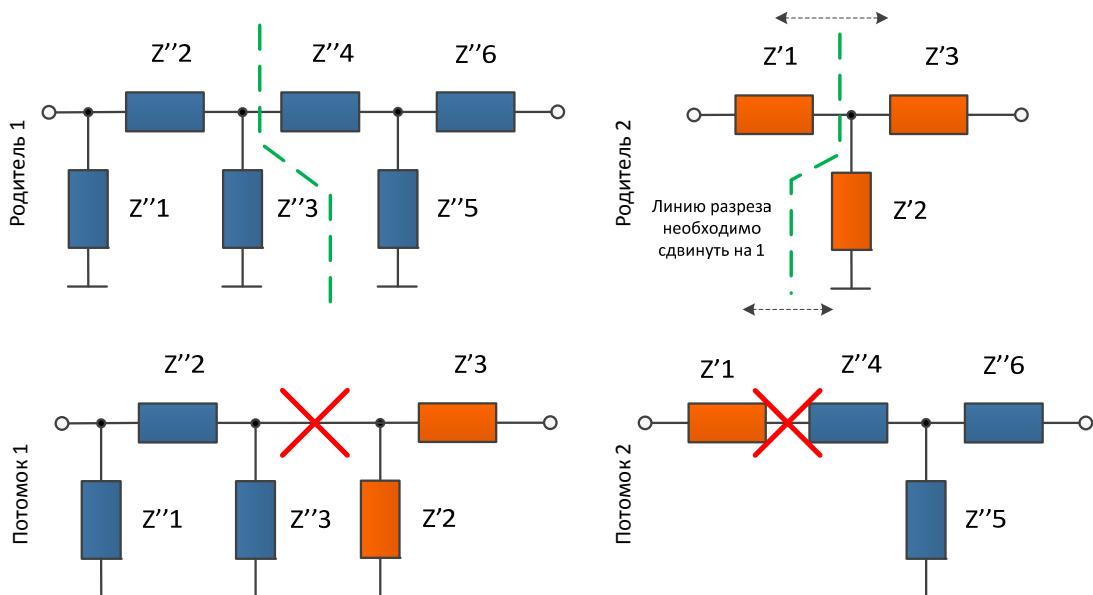


Рис. 4. Одноточечный кроссинговер лестничных цепей

Таким образом, используя данную методологию, можно разработать генетические алгоритмы для структурно-параметрического синтеза электрических цепей.

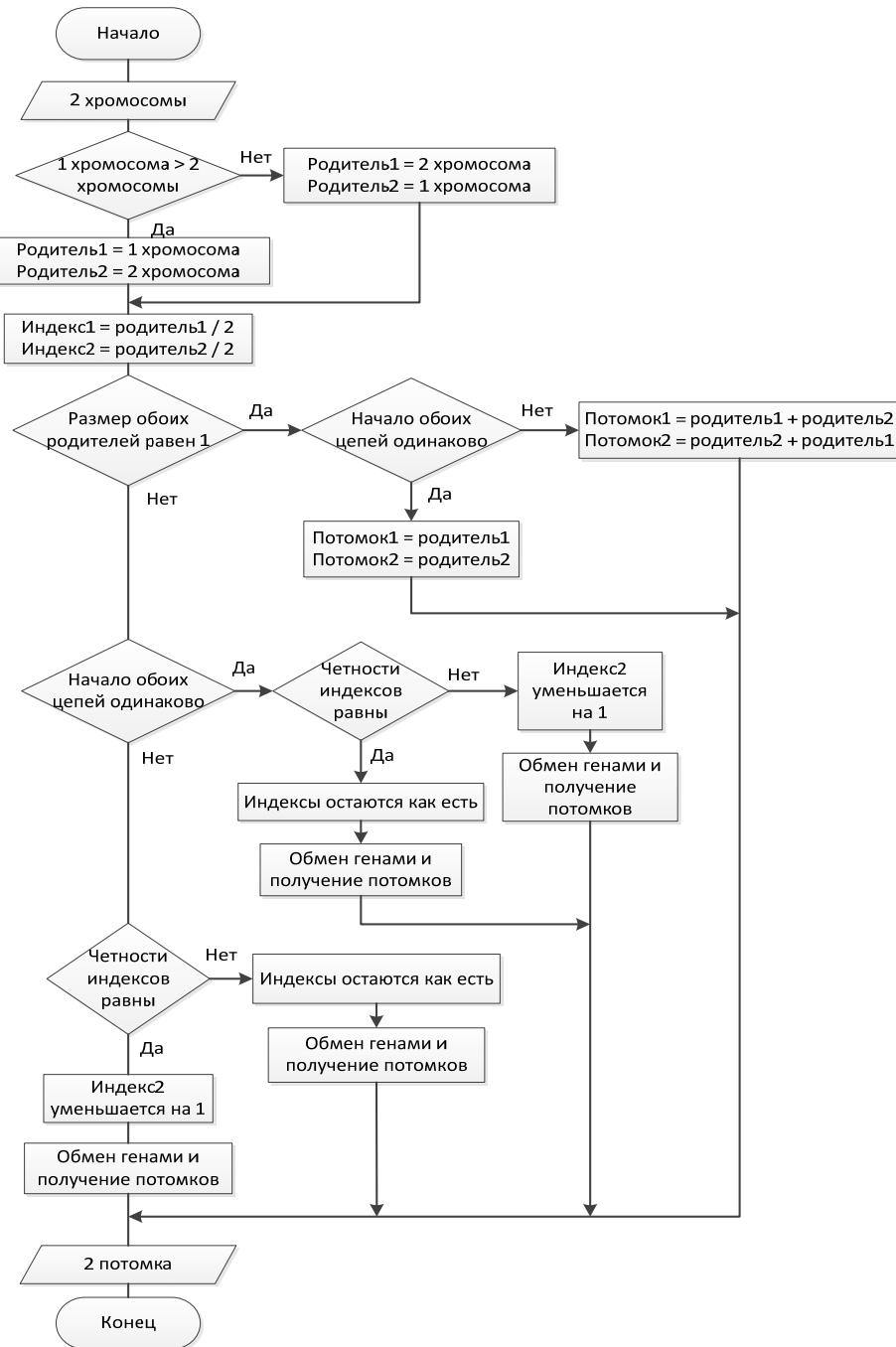


Рис. 5. Алгоритм реализации кроссинговера

### Список используемых источников

1. Программный модуль генетических алгоритмов для САПР Multisim / И. С. Пономарев // Технические науки – от теории к практике. – 2014. – № 30. – С. 23–27.
2. Генетические алгоритмы / В. В. Курейчик, Л. А. Гладков. – М. : ФИЗМАТЛИТ, 2006. – 320 с.

*Статья представлена научным руководителем д-ром техн. наук, доцентом Г. В. Верховой.*

УДК 004.627

**И. С. Рубина (доцент кафедры «Вычислительная техника»  
НИУ ИТМО)**

## **ПРИМЕНЕНИЕ ИНТЕРПОЛЯЦИИ ДЛЯ УСТРАНЕНИЯ АРТЕФАКТОВ В КАДРАХ ВИДЕОПОСЛЕДОВАТЕЛЬНОСТИ**

В ходе сжатия видеокадров различной природы, как правило, возникают искажения или артефакты, связанные с динамическими свойствами объектов и используемыми алгоритмами компрессии. Наиболее распространеными из них принято считать блокинг-эффект, блеринг-эффект и рингинг-эффект. При этом ряд исследований показал, что наиболее заметным для восприятия человеком является блокинг-эффект, возникающий при сжатии блочными алгоритмами кодирования преобразованием (ДКП, ДПХ и пр.).

Интерполяция отсчетов сигнала используется при сжатии изображений. В рамках данного исследования предложено использовать интерполяцию для сжатия и улучшения качества видеопоследовательностей. Тогда основным требованием к интерполятору является как можно более высокая точность при малой вычислительной сложности алгоритма. Таким образом, целью данной работы является разработка метода повышения степени сжатия и качества восстановленных видеоданных путем устранения артефактов на границах сегмента путем интерполяции кадров видеопоследовательности.

В основе разработанного адаптивного алгоритма интерполяции отсчетов сигнала лежит подход представленный в работе [1]. В данном подходе для определения коэффициента центрального отсчета по четырем смежным опорным отсчетам используется одна из трех интерполирующих функций:

$$\begin{aligned}f^0(2m+1,2n+1) &= \frac{[f(2m,2n) + f(2m+2,2n+2)]}{2} \\f^1(2m+1,2n+1) &= \frac{[f(2m,2n) + f(2m+2,2n) + f(2m,2n+2) + f(2m+2,2n+2)]}{4} \\f^2(2m+1,2n+1) &= \frac{[f(2m+2,2n) + f(2m,2n+2)]}{2}\end{aligned}$$

Графическое представление рассматриваемых интерполирующих функций представлено на рисунке 1.

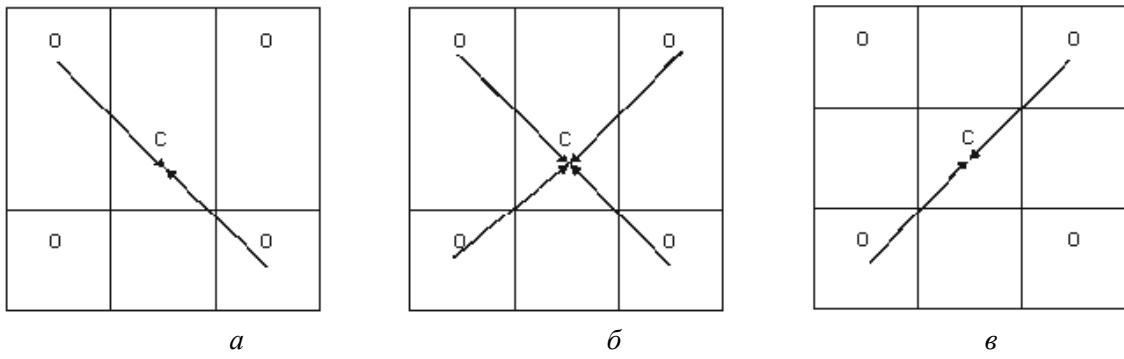


Рис. 1. Адаптивная интерполяция центрального отсчета,  
где о – опорные отсчеты, с – центральные отсчеты, остальные – крайние отсчеты

Выбор функции в каждой точке изображения осуществляется на основе признака

$$\mu(2m+1,2n+1) = |f(2m,2n) - f(2m+2,2n+2)| - |f(2m,2n+2) - f(2m+2,2n)|$$

с помощью зависящего от параметров  $\alpha_1$  и  $\alpha_2$  решающего правила, которое в каждой точке изображения определяет номер используемой интерполирующей функции по значению этого признака:

$$f(2m+1,2n+1) = \begin{cases} 0, & \mu < \alpha_1 \\ 1, & \alpha_1 \leq \mu \leq \alpha_2 \\ 2, & \mu > \alpha_2 \end{cases}$$

Слабым местом прямого использования данного подхода является то, что непосредственной обработке данных в нем предшествует трудоемкий процесс обучения (настройки решающего правила), который заключается в отыскании этих параметров. При этом выбор значений параметров решающего правила осуществляется, исходя из минимизации суммарной ошибки интерполяции, и формулируется в виде:

$$\sum_{(m,n) \in I} |f'(m,n) - f(m,n)| \rightarrow \min_{\alpha_1, \alpha_2} \quad (1)$$

где  $I$  – множество индексов опорных отсчетов.

С целью устранения данного недостатка, уменьшения влияния артефактов, а также в связи с особенностями обработки видеоданных на предшествующих интерполяции стадиях, разработанный адаптивный алгоритм интерполяции реализует следующие технические решения:

- Используется адаптивный размер ядра интерполяции (рис. 2). Таким образом для блоков различного размера, полученных на этапе оценки и компенсации движения [1, 2], применяются соответствующие ядра интерполяции, обеспечивающие совместимость при стыковке блоков различного размера.

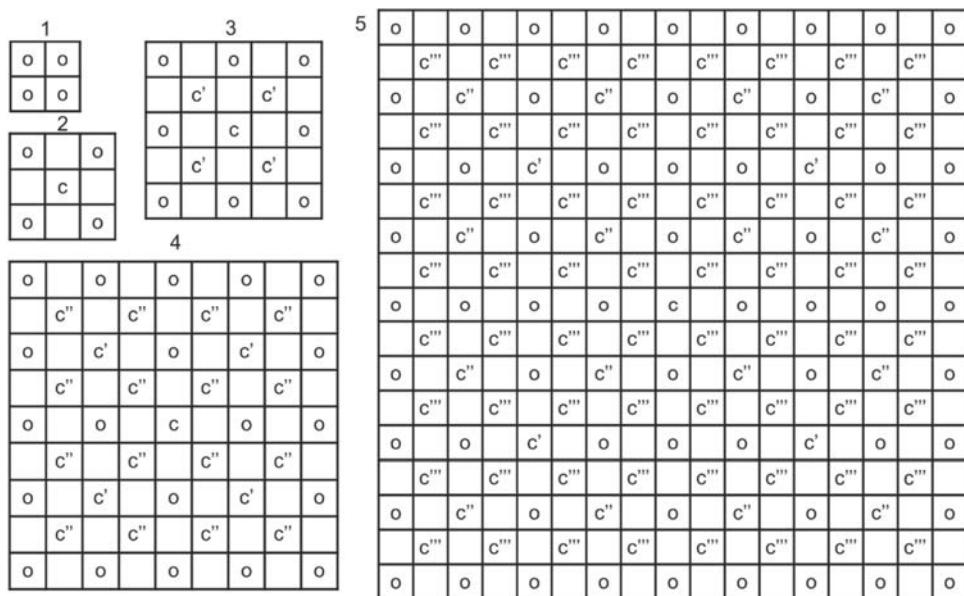


Рис. 2. Схема интерполяции с адаптивным размером ядра:  
1 – 2x2, 2 – 4x4, 3 – 8x8, 4 – 16x16, 5 – 32x32

– Предлагается передавать номер интерполирующей функции для каждого блока в виде 2-битного кода, определяемого на этапе кодирования путем минимизации суммарной ошибки интерполяции (1).

– Предложенный алгоритм интерполяции на основе адаптивного размера ядра является рекурсивным алгоритмом, в рамках которого центральный основной и побочные симметричные отсчеты, за исключением граничных отсчетов, вычисляются исходящим образом в рамках адаптивного алгоритма центрального отсчета.

– Направление предсказания определяется в целом для блока в соответствии с критерием минимизации суммарной ошибки интерполяции и передается кодовым словом длиной 2 бита на блок. Оставшиеся пиксели являются крайними или граничными и вычисляются в рамках алгоритма «прямой крест».

– Интерполяционный остаток предлагается формировать только для опорных кадров, а для ссылочных кадров предлагается обращать все коэффициенты кроме опорных коэффициентов в нуль.

Для проведения анализа описанных ранее алгоритмов интерполяции были выбраны стандартные тестовые последовательности группы MPEG такие, как «Теннис», «Бригадир» и «Береговая охрана».

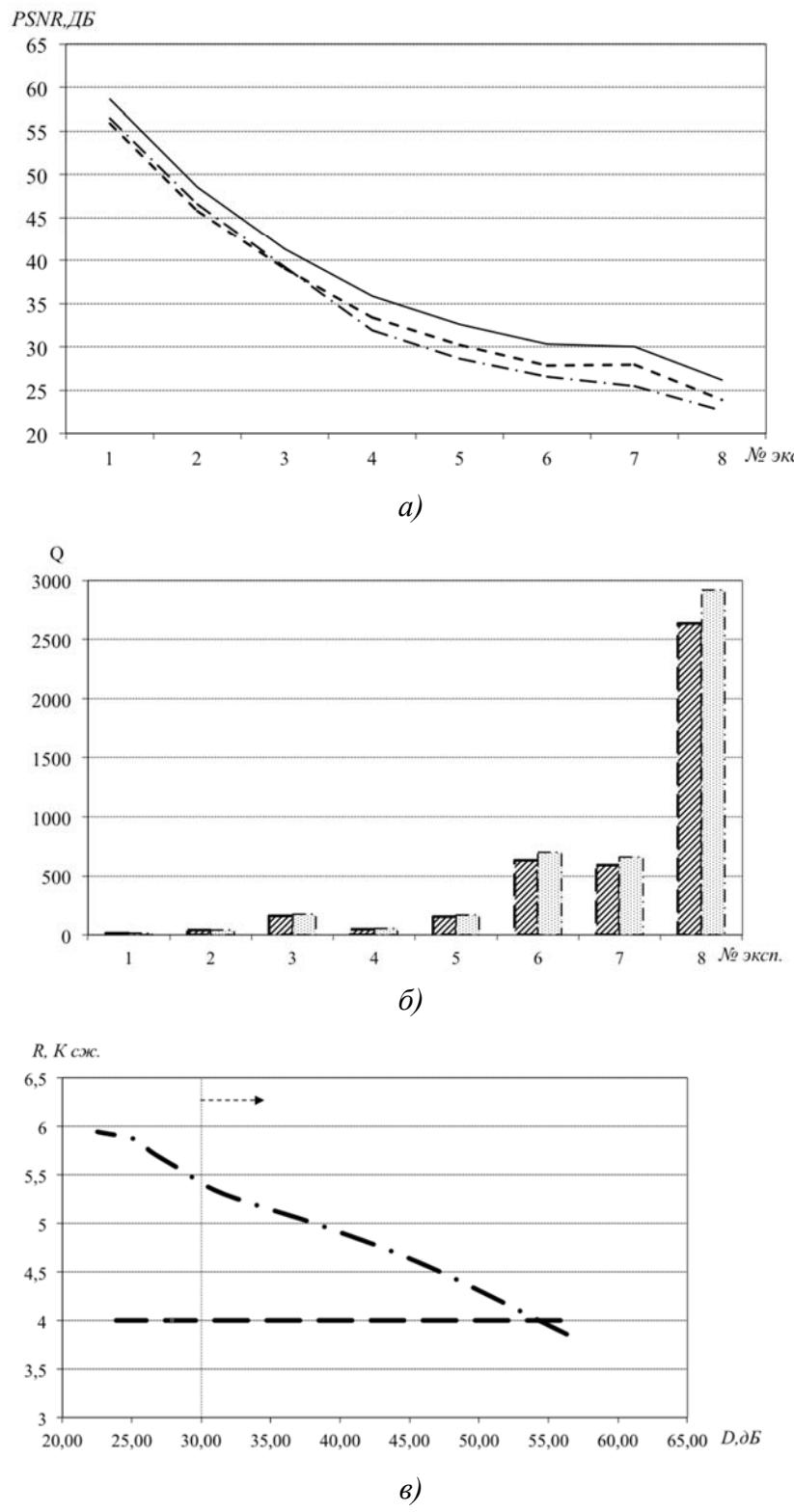


Рис. 3. Сравнительная оценка алгоритмов интерполяции для алгоритма адаптивной интерполяции центрального отсчета  $--$ ,  $\blacksquare$  алгоритма интерполяции с адаптивным размером ядра  $—\cdot-$ ,  $\blacksquare$  алгоритма без интерполяции — значений искажений сигнала (*a*), вычислительной сложности *Q* (*б*) для ряда экспериментов (табл. 1) и RD-характеристики (*в*).

ТАБЛИЦА 1. Значения размеров блока для ряда экспериментов

№ эксперимента	Минимальный размер блока, пиксель	Максимальный размер блока, пиксель
1	$2^2$	$2^4$
2	$2^2$	$2^6$
3	$2^2$	$2^8$
4	$2^4$	$2^6$
5	$2^4$	$2^8$
6	$2^4$	$2^{10}$
7	$2^6$	$2^{10}$
8	$2^6$	$2^{12}$

В ходе экспериментов для алгоритма без интерполяции, адаптивного алгоритма центрального отсчета и алгоритма с адаптивным размером ядра были получены следующие зависимости (рис. 3):

– Пиковое соотношение сигнал / шум, вычисляемое в соответствии с формулой:

$$PSNR_{dB} = 10 * \lg \frac{(2^n - 1)^2}{MSE},$$

где  $n$  – разрядность цветовой схемы, для YUV равная восьми, а MSE – среднеквадратичное отклонение исходного изображения от восстановленного после сжатия, определяемое по формуле.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|I(i, j) - K(i, j)\|^2,$$

где  $m, n$  – размеры кадра, а  $I(i, j)$  и  $K(i, j)$  – интенсивности соответствующих пикселей компенсируемого и ссылочного кадра. Необходимо отметить, что в рамках исследования применялось ограничение по допустимому уровню PSNR, равное 30 Дб, отмеченное на рисунке 5 в стрелкой.

– RD – характеристика, выражаяющая зависимость искажения сигнала ( $PSNR$ ) от степени его сжатия.

– Вычислительная сложность алгоритма, измеряемая количеством операций умножения и сложения на пиксель. Определяется средним значением количества таких операций для перечня размеров блока.

– В ходе анализа результатов для последовательности «Теннис» (рис. 3) было выявлено:

1. Использование интерполяции отсчетов сигнала является эффективным инструментом для устранения блокинг – эффекта на выходе блока кодирования преобразованием.

2. Предложенный алгоритм интерполяции на основе адаптивного выбора размера ядра позволил повысить степень сжатия на 30 % и качество восстановленной видеопоследовательности на 2 % для малых размеров блока по сравнению со сжатием без интерполяции.

В данной работе описан метод повышения качества видеоданных путем устранения артефактов на границах сегмента путем интерполяции кадров видеопоследовательности, также позволяющие повысить степень сжатия. Результаты исследования могут эффективно применяться в задачах обработки видеоданных, различных кодеках сжатия видео и системах потокового вещания.

#### **Список используемых источников**

1. Исследование алгоритмов кодирования преобразованием в задачах сжатия кадров видеопоследовательности / И. С. Рубина, А. Ю. Тропченко // Известия вузов. Приборостроение. – 2012. – Вып. 1. – С. 26–31.

2. Адаптивный алгоритм интерполяции для иерархической компрессии изображений / М. В. Гашников, Н. И. Глумов, В. В. Сергеев // Компьютерная оптика. – 2002. – вып. 23. – С. 89–93.

*Статья представлена научным руководителем д-ром техн. наук, профессором Т. И. Алиевым (НИУ ИТМО).*

**УДК 004.912**

**Е. Е. Семенова (студент группы 6709 НИУ ИТМО)**

## **МОДЕЛЬ СИСТЕМЫ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ QR-КОДА ДЛЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ**

Аутентификация – процедура проверки подлинности субъекта, которая позволяет достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует. Во времена активного использования мобильных устройств и, в частности, реализации процессов авторизации и аутентификации с использованием смартфонов, вопрос защищенности аутентификации становится все более актуальным.

Наиболее популярным методом аутентификации на сегодняшний день является парольная аутентификация. Основное ее достоинство – простота

и привычность использования, однако, такой метод аутентификации признается самым слабым методом проверки подлинности при учете его характеристик в совокупности.

Для повышения надежности хранимых данных стоит обратить внимание на другие технологии аутентификации, например, следующие: Enum-авторизация (авторизация через мобильное приложение с привязкой к мобильному телефону), SMS-авторизация; QR-код, цифровой сертификат (документ, подтверждающий права пользователя), биометрические методы (отпечатки пальцев, распознавание голоса и др.).

Согласно [1] основной характеристикой веб-образования является предоставление ключей идентификации другим пользователям или программам, способным пройти необходимые тесты вместо самого пользователя. Приведенная характеристика является основным недостатком веб-образования.

Риск возникновения основного недостатка веб-образования можно свести к минимуму, если усилить систему защиты передаваемых персональных данных пользователя и осуществлять проверку его местонахождения в ограниченной локации. Для этого была разработана модель функционирования системы, позволяющая повысить защищенность процедуры аутентификации. В качестве одного из инструментов аутентификации используется QR-код.

### *Описание модели*

В модели функционирования системы данными обмениваются клиент и сервер. В мобильном приложении содержится открытый ключ данного пользователя. В качестве способа проверки принадлежности пользователя текущей локации был выбран GPS навигатор мобильного телефона.

Алгоритм обмена данными состоит в следующем:

1. Мобильное приложение запускается на устройстве и отправляет серверу GPS-координаты и открытый ключ данного пользователя.

2. Сервер шифрует данные пользователя полученным секретным ключом.

3. Сервер формирует QR-код, в котором содержатся секретные данные всех пользователей, от которых была получена информация. Данные находятся в QR-коде в зашифрованном виде.

4. Пользователь получает QR-код через мобильное приложение, считывает его и видит только те данные, которые предназначены для него. Данные всех остальных пользователей отображаются в зашифрованном виде.

В качестве данных в QR-коде может выступать URL персональной страницы пользователя.

На рисунке 1 приведена модель функционирования системы.

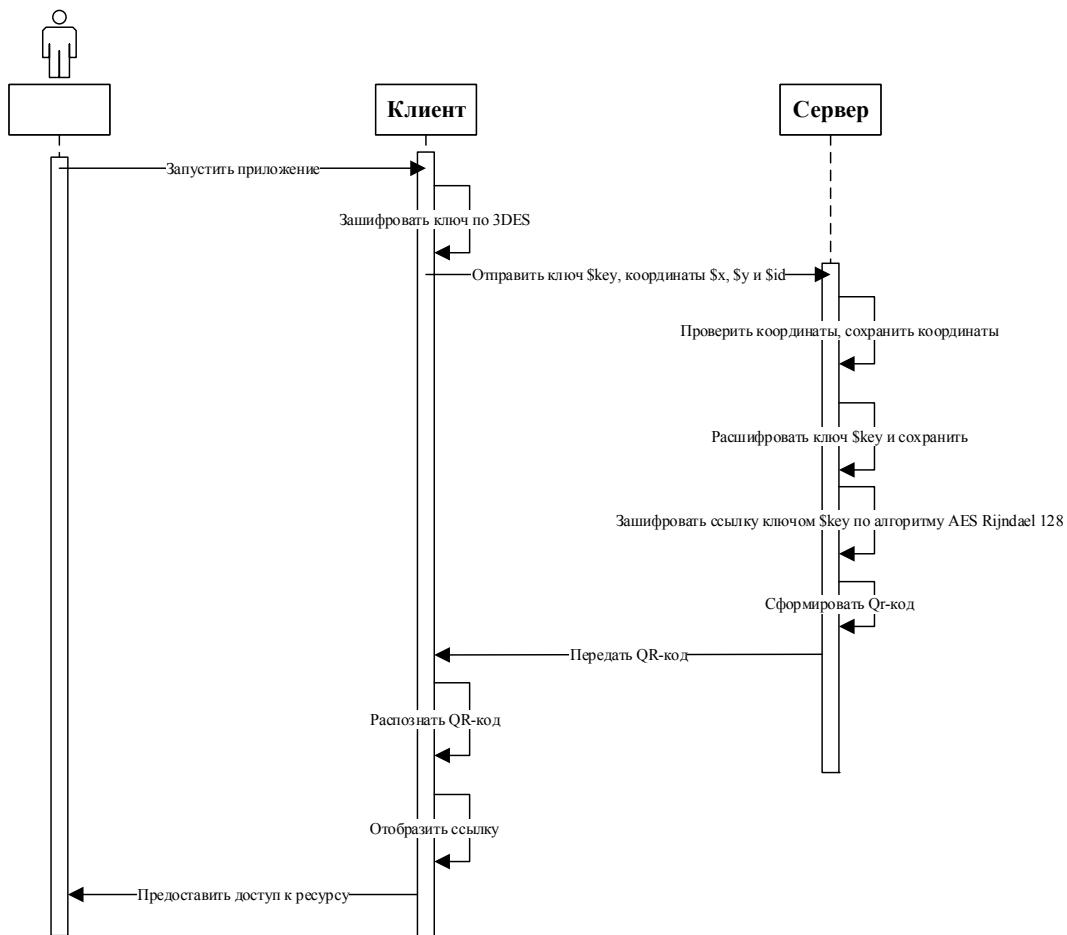


Рис. 1. Модель функционирования системы

### *Мобильное приложение*

Для получения прототипа системы было разработано мобильное приложение под Android с серверной реализацией на php. При запуске мобильное приложение предлагает пройти QRCode авторизацию. При нажатии на кнопку пользователь попадает в новое окно, в котором ему предлагается получить ссылку на QR-код. Пользователь нажимает кнопку и видит ссылку, по которой находится QR-код, сгенерированный сервером. Ниже пользователь видит две кнопки «Вывести QRCode» и «Получить ссылку для теста». При нажатии на кнопку «Вывести QRCode» на экране пользователю демонстрируется изображение QR-кода и расшифрованная ссылка. При нажатии «Получить ссылку для теста» пользователь видит ссылку без изображения QR-кода. Полученная ссылка открывается в браузере. Интерфейс мобильного приложения показан на [рисунке 2](#) и [рисунке 3](#).

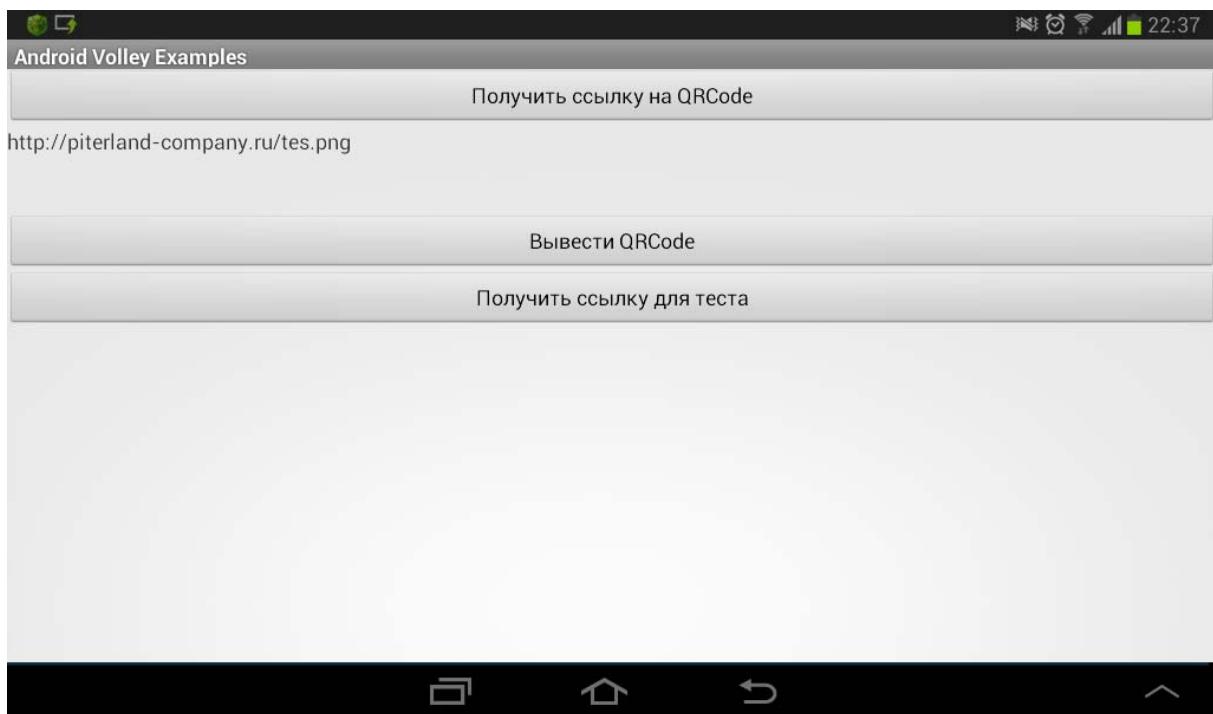


Рис. 2. Экран 2: получение ссылки на QR-код



Рис. 3. Экран 3: демонстрация QR-кода и ссылки

### *Достоинства метода*

Основными достоинствами предложенного метода аутентификации, представляющего собой частный случай идентификации посредством мобильных устройств, являются следующие [1]:

1. Возможность последующего использования дополнительной отличительной информации мобильного телефона (*IMEA* и др.) в качестве данных об идентификации.

2. Широкий охват аудитории. Практически все ученики обладают мобильными телефонами, что означает, что для доступа к обучающим тестам ученикам не потребуется взаимодействовать с дополнительным оборудованием.

3. Использование веб-функционала современных мобильных телефонов позволяют повысить наглядность обучающих ресурсов и удобство их взаимодействия с пользователем.

4. В системе учитываются GPS-координаты пользователя и его идентификатор, заложенный в мобильное приложение, что предотвращает возможность авторизации с другого устройства и за пределами необходимой локации с точностью до шестого знака после запятой.

5. Ключи находятся в мобильном приложении и защищены от редактирования. Кроме того, ключи формируются в соответствии с алгоритмом 3DES, а передаются согласно алгоритму AES-128.

Описанная модель аутентификации позволяет значительно уменьшить риск возникновения основного недостатка веб-образования за счет введения дополнительного шифрования ссылки и открытого ключа, а также проверки GPS-координат. Дальнейшая разработка системы предполагает идентификацию пользователя по *Android Id*, исследование других методов определения местоположения пользователя, а также исследование практических возможностей внедрения системы.

#### **Список используемых источников**

1. A web authentication system using location information from mobile telephones / H. Takamizawa and K. Kenji // Proceedings of the IASTED international conference Web-based Education (WBE 2009), March 2009, Phuket. – PP. 31–36.

*Статья представлена научным руководителем,  
доцентом И. В. Петровым (НИУ ИТМО).*

УДК 004.94

**А. В. Соловьева (старший преподаватель кафедры ИКД СПбГУТ)**

## **МЕТОД КОНЦЕНТРИЧЕСКИХ СФЕР ДЛЯ ПОСЛОЙНОГО ОПРЕДЕЛЕНИЯ ПРОДУКТОВ СГОРАНИЯ**

Обеспечение пожаробезопасности в различных сферах деятельности человека было и остается актуальным. Уже на этапе проектирования необходимо моделировать ситуации возникновения теплового явления, его распространение и воздействие на окружающие предметы в конкретных условиях.

Основным направлением в решении поставленной задачи является разработка новых методов моделирования, способных повысить точность расчетов за более короткое время [1, 2].

Целью настоящей работы является описание метода концентрических сфер для послойного определения продуктов сгорания.

### *Метод концентрических сфер*

Данный метод решает задачу послойного расчета полей температуры и давления в каждой точке замкнутого объекта сложной геометрической формы, внутри которого происходит тепловой процесс.

Как известно, в закрытом объеме происходит послойное сгорание продукта, что приводит к неоднородному состоянию, которое находит объяснение в зависимости величины температуры элементарного объема с продуктом горения не только от конечного давления, но и от давления, при котором произошло сгорание объема [3]. В связи с этим для математического моделирования физико-химических процессов с равномерным распространением относительно центра возгорания предложено использование метода концентрических сфер.

### *Алгоритм решения метода концентрических сфер для определения продуктов сгорания*

1. Геометрия поверхности замкнутого пространства [4] в общем виде представлена выражением (1)

$$A_m x^n + A_{m-1} y^n + A_{m-2} z^n + \dots + A_3 x + A_2 y + A_1 z + A_0 = 0, \quad (1)$$

где  $A$  – числовой коэффициент уравнения, любые положительные и отрицательные числа с любой точностью;  $x, y, z$  – переменные ортогональной системы координат, любые положительные и отрицательные числа с любой точностью;  $m$  – максимальный номер числового коэффициента урав-

нения, целые положительные числа;  $n$  – максимальный номер степени при переменных, целые и дробные положительные числа.

Для примера решения задачи методом концентрических сфер рассматриваем сложный геометрический объем (рис. 1) со следующим уравнением поверхности.

$$\begin{aligned} A_{34}x^4 + A_{33}y^4 + A_{32}z^4 + A_{31}x^3y + A_{30}x^3z + A_{29}y^3x + A_{28}y^3z + A_{25}x^2y^2 + A_{21}y^2xz + \\ + A_{19}x^3 + A_{18}y^3 + A_{17}z^3 + A_{16}x^2y + A_{15}x^2z + A_{14}y^2x + A_{13}y^2z + A_{12}z^2x + A_{11}z^2y + \\ + A_{10}xyz + A_9x^2 + A_8y^2 + A_7z^2 + A_6xy + A_5xz + A_4yz + A_3x + A_2y + A_1z + A_0 = 0 \end{aligned}$$

$A_0 = -100$ , остальные коэффициенты равны единице.

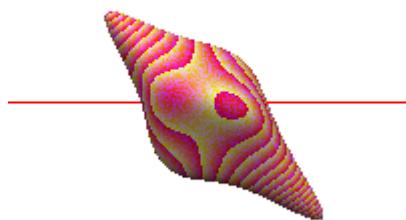


Рис. 1 Замкнутый объем сложной формы

В данном методе не предусмотрено изменение геометрии замкнутого пространства в процессе горения.

2. Химические свойства параметров газовой смеси и физические свойства объема даны в качестве начальных условий.

$T_0$  – исходная температура, одинаковая по всему объему,  $c_v$  – теплопроводность при постоянном объеме,  $P_0$  – начальное давление;  $M$  – исходная масса смеси.

3. Ввод координаты точечного источника возгорания внутри замкнутого объема ( $x, y, z$ ). Принимаем координаты точки возгорания  $(0, 0, 0)$ .

4. Выделение сферических объемов (2) вокруг центра возгорания  $V_1, V_2, V_3$  и т. д. Шаг сферы определяется в зависимости от скорости распространения горения и расстояния до границы замкнутого объема от центра возгорания.

$$B_3x^2 + B_2y^2 + B_1z^2 - B_0 = 0, \quad (2)$$

где  $B_1, B_2, B_3$  – числовые коэффициенты, принимающие любые положительные и отрицательные числа,  $B_0$  – квадрат радиуса концентрической сферы.

На данном этапе решения поставленной задачи выделяем сферический объем  $V_1$  с радиусом  $R_1 = 1$  и центром в источнике возгорания, коэффициенты равны единице.

5. Определение координат точек, лежащих на поверхности сферы с радиусом  $R_1 = 1$  относительно каждой оси. В таблице 1 показаны координаты точек на примере оси  $z$  для четырех концентрических сфер с квадратами радиуса  $B_0 = 1; 2; 7; 8$ .

ТАБЛИЦА 1. Координаты точек на поверхностях концентрических сфер

$x$	$y$	$z$	Уравн. объема	$x$	$y$	$z$	Уравн. объема	$x$	$y$	$z$	Уравн. объема
<b><math>B_0=1</math></b>				1,166	-0,8	0	-86,173	2,522	-0,8	0	-5,355
0	-1,0	0	-96	1,229	-0,7	0	-86,373	2,551	-0,7	0	-6,89
0,436	-0,9	0	-94,698	1,281	-0,6	0	-86,643	2,577	-0,6	0	-8,607
0,6	-0,8	0	-94,47	1,323	-0,5	0	-86,985	2,598	-0,5	0	-10,511
0,714	-0,7	0	-94,422	1,356	-0,4	0	-87,397	2,615	-0,4	0	-12,603
0,8	-0,6	0	-94,47	1,382	-0,3	0	-87,882	2,629	-0,3	0	-14,884
0,866	-0,5	0	-94,589	1,4	-0,2	0	-88,438	2,638	-0,2	0	-17,352
0,917	-0,4	0	-94,768	1,411	-0,1	0	-89,065	2,644	-0,1	0	-20,004
0,954	-0,3	0	-95,002	1,414	0	0	-89,757	2,646	0	0	-22,834
0,98	-0,2	0	-95,287	1,411	0,1	0	-89,065	2,644	0,1	0	-20,004
0,995	-0,1	0	-95,621	1,4	0,2	0	-88,438	2,638	0,2	0	-17,352
1	0	0	-96	1,382	0,3	0	-87,882	2,629	0,3	0	-14,884
0,995	0,1	0	-95,621	1,356	0,4	0	-87,397	2,615	0,4	0	-12,603
0,98	0,2	0	-95,287	1,323	0,5	0	-86,985	2,598	0,5	0	-10,511
0,954	0,3	0	-95,002	1,281	0,6	0	-86,643	2,577	0,6	0	-8,607
0,917	0,4	0	-94,768	1,229	0,7	0	-86,373	2,551	0,7	0	-6,89
0,866	0,5	0	-94,589	1,166	0,8	0	-86,173	2,522	0,8	0	-5,355
0,8	0,6	0	-94,47	1,091	0,9	0	-86,046	2,488	0,9	0	-3,997
0,714	0,7	0	-94,422	1,0	1,0	0	-86	2,449	1,0	0	-2,808
0,6	0,8	0	-94,47	0,889	1,1	0	-86,056	2,406	1,1	0	-1,781
0,436	0,9	0	-94,698	0,748	1,2	0	-86,267	2,358	1,2	0	-0,906
0	1,0	0	-96	0,557	1,3	0	-86,782	2,304	1,3	0	-0,174
<b><math>B_0=2</math></b>				0,2	1,4	0	-88,438	2,245	1,4	0	<b>0,425</b>
0,2	-1,4	0	-88,438	<b><math>B_0=7</math></b>				не удовлетворяет условию п. 6			
0,557	-1,3	0	-86,782	2,304	-1,3	0	-0,174	<b><math>B_0=8</math></b>			
0,748	-1,2	0	-86,267	2,358	-1,2	0	-0,906	-2,828	0	0	-2,544
0,889	-1,1	0	-86,056	2,406	-1,1	0	-1,781	2,827	0,1	0	<b>0,804</b>
1,0	-1,0	0	-86	2,449	-1,0	0	-2,808	не удовлетворяет условию п. 6			
1,091	-0,9	0	-86,046	2,488	-0,9	0	-3,997	2,828	0	0	-2,544

6. Проверка на условие недостижения границы замкнутого объема, т. е. нахождения концентрической сферы внутри замкнутого объема как слоя и этапа в распространении теплового фронта (3)

$$A_m x^n + A_{m-1} y^n + A_{m-2} z^n + \dots + A_3 x + A_2 y + A_1 z + A_0 < 0. \quad (3)$$

В таблице 1 показаны значения, которые принимает уравнение замкнутого объема с конкретными координатами точки на поверхности концентрической сферы. В случае отрицательного значения – точка поверхности сферы лежит внутри рассматриваемого объема, положительного – находится за его пределами.

7. Определение физико-химических характеристик продуктов сгорания на границе рассматриваемого слоя – определение температуры и давления в данных точках на поверхности сферы с радиусом  $R_1 = 1$ .

8. Цикл послойного температурного моделирования повторяется с п.4, где за начальные условия принимаются конечные температура и давление на предыдущем концентрическом сферическом слое; следующие рассматриваемые слои с радиусами  $R_2, R_3$  до тех пор, пока удовлетворяется условие п. 6.

### *Заключение*

Метод концентрических сфер решает задачу описания теплового процесса внутри замкнутого объема сложной геометрической формы, позволяет увеличить точность моделирования и уменьшить объем компьютерной модели при её реализации.

Данный метод может быть использован при проектировании различных технических объектов, связанных с тепловыми процессами или в которых возможно возгорание.

### **Список используемых источников**

1. Сравнение интегральной и зонной моделей пожара / А. М. Сивков // Безопасность в техносфере: сб. статей; под ред. В. М. Колодкина. – Ижевск : Удмуртский университет, 2011. – 196 с.
2. Выбор системы визуального моделирования для проектирования и расчета тепловых схем теплоэнергетических установок / Д. К. Смирнов, Н. Н. Галашов // Современные техника и технологии: сб. трудов XVI Международной научно-практической конференции студентов, аспирантов и молодых ученых. В 3 т. Т. 3. – Томск : Изд-во Томского политехнического университета, 2010. – 442 с.
3. Математическая теория горения и взрыва / Я. Б. Зельдович, Г. И. Баренблatt, В. Б. Либрович, Г. М. Махвидадзе. – М. : Наука, 1980. – 478 с.
4. Инженерная и компьютерная графика: учебник для учрежд. высш. проф. образов. / В. М. Дегтярев, В. П. Затыльникова. – М. : Академия, 2013. – 240 с.
5. Моделирование процессов горения в замкнутых объемах сложной формы / В. М. Дегтярев, А. В. Хижняк // II Международная научно-техническая и научно-

методической конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» : материалы конференции. – СПбГУТ, 2013. – С. 585–590

*Статья представлена заведующим кафедрой д-ром техн. наук, профессором Д. В. Волошиновым.*

**УДК 004.422**

**С. В. Ушанов (студент группы ТСС-17с СПбГУТ)**

## **РАЗРАБОТКА ФРАГМЕНТА ПРОГРАММЫ ДЛЯ АВТОМАТИЗАЦИИ УЧЕБНОГО ПРОЦЕССА**

В классических типах контроля знаний (письменный контроль, зачет, коллоквиум и т. д.) имеется ряд существенных проблем. К ним можно отнести следующие:

1. Большие затраты временных ресурсов со стороны преподавателя (проверяющего). Они зависят как от объема представленного к проверке материала, так и от разборчивости почерка испытуемого (в случае рукописного вида контроля).

2. Качество ручной проверки напрямую зависит от субъективного фактора проверяющего. А это в свою очередь, может зависеть от психофизического состояния проверяющего (усталость, утомление, нервные перегрузки и т. д.), а также от межличностных отношений проверяющего с обучающимся. Кроме того, при ручном контроле не исключен фактор коррупции.

Решением части этих проблем стали тесты. Но и на их проверку, подведение результатов и выставление оценок требуется довольно значительное время [1].

С появлением средств вычислительной техники стали разрабатываться и программные продукты по проведению тестирований. На сегодняшний день существует огромное количество разнообразных систем тестирования, как на конкретный раздел дисциплины, так и на дисциплину в целом. Системы тестирования как с предустановленными вопросами, так и вольного заполнения.

В результате анализа существующих систем автоматизированного тестирования выявлены следующие недостатки:

– при разработки теста программа должна быть установлена на сетевой компьютер. Это значит, что при необходимости составить тест в домашних условиях, а также при отсутствии или при выходе из строя локальной сети сделать это не возможно;

- испытуемый может выбрать любую фамилию из списка, без какого-либо контроля и ввода паролей;
- можно завершить работу программы и начать ответы на тест с самого начала столько раз сколько захочется;
- серверная и клиентская части лежат на сервере в общедоступной папке и могут быть легко удалены по ошибке, либо по злому умыслу;
- файл зашифрован. Но это не мешает загрузить его в серверную часть и посмотреть варианты вопросов и ответов;
- работа программы обеспечивается не всеми ОС;
- при отсутствии подключения к сети интернет провести тест невозможно.

Эти недостатки и стали основанием для разработки программы автоматизации учебного процесса [2].

Итак, требуется разработать программу, позволяющую заменить «бумажный» журнал, с возможностью просмотра результатов со стороны родителей (опекунов). И кроме того программа должна включать в себя автоматизированное тестирование знаний, обучающихся с возможностью работы в различных операционных средах (*any Unix, Linux or Windows, MacOS*), не зависящую от подключения компьютера как к локальной, так и к глобальной сети.

Решением этой проблемы может стать разработка программы, обладающая следующим функциями:

- регистрация пользователя;
- возможность составление и редактирования тестов преподавателем;
- обновление базы данных вопросов;
- формирование отчетов по успеваемости каждого отдельного обучающегося;
- оформление тестов в печатном виде;
- просмотр допущенных ошибок;
- автоматизированное внесение результатов тестирования в электронный журнал.

Такой программой стала АИС «Учета посещаемости и успеваемости» (рис. 1)

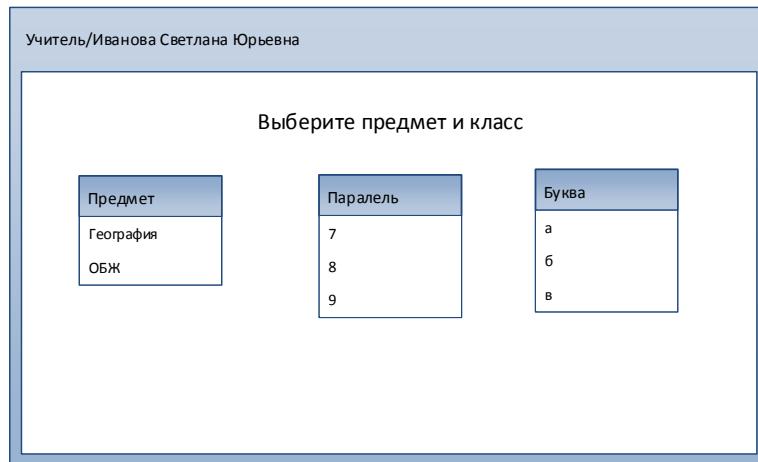


Рис. 1. Интерфейс АИС «Учета посещаемости и успеваемости»

Данная система обеспечивает:

- контроль всех результатов обучающегося, по каждой дисциплине как со стороны преподавателей так и со стороны родителей (опекунов) (рис. 2–4);

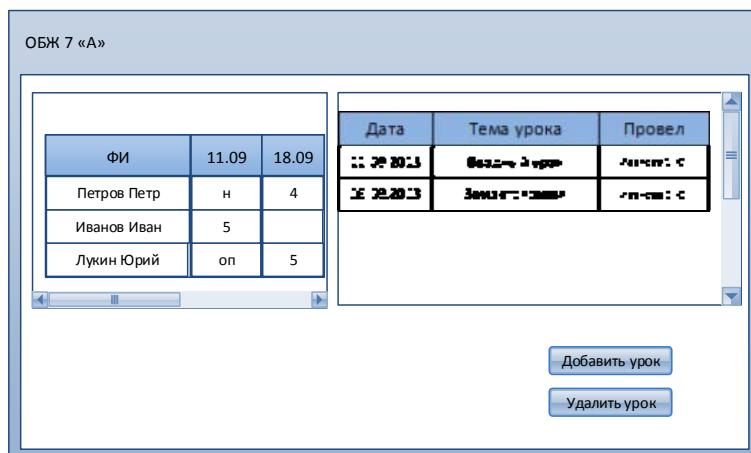


Рис. 2. Элемента интерфейса электронного журнала

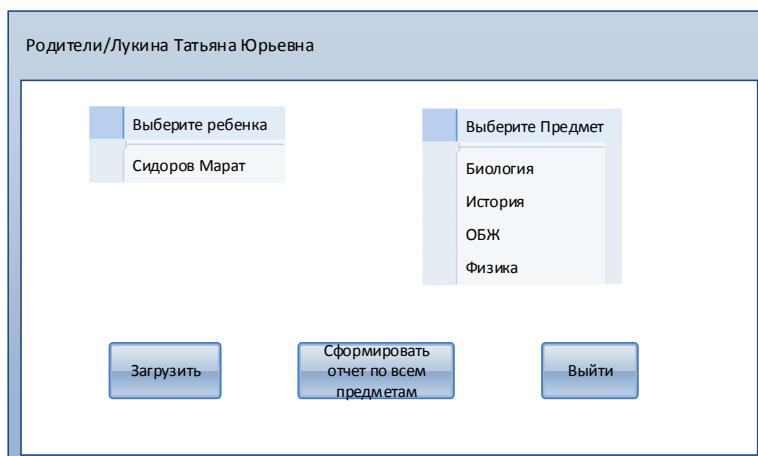


Рис. 3. Интерфейса домашней страницы электронного дневника

Родители/Лукина Татьяна Юрьевна/Лукин Юрий (ОБЖ)

Дата	11.09.2013	18.11.2013
Результат	оп	5

Сформировать отчет      Назад

Рис. 4. Интерфейс страницы успеваемости и посещаемости по конкретной дисциплине

– ограниченность интерфейса. АИС «Учета посещаемости и успеваемости» проста в использование. Данная программа понятна на интуитивном уровне. Для работы с АИС не требуется никакого дополнительного обучения. В программе соединены основные функции. Кроме того данная программа является кроссплатформенной (программное обеспечение, работающее более чем на одной аппаратной платформе или операционной системе) (рис. 5);

Добавить урок (ОБЖ 7 «А» урок №3)

Дата проведения урока:

◀	Октябрь 13	▶				
п	в	с	ч	п	с	в
1	2	3	4	5	6	
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Тема урока:

№ урока по п/п:

Добавить из планирования    Добавить урок    Отмена

Рис. 5. Процесс добавления нового урока в АИС «Учета посещаемости и успеваемости»

– синхронизация с системой тестирования АИС «Успех» (рис. 6).

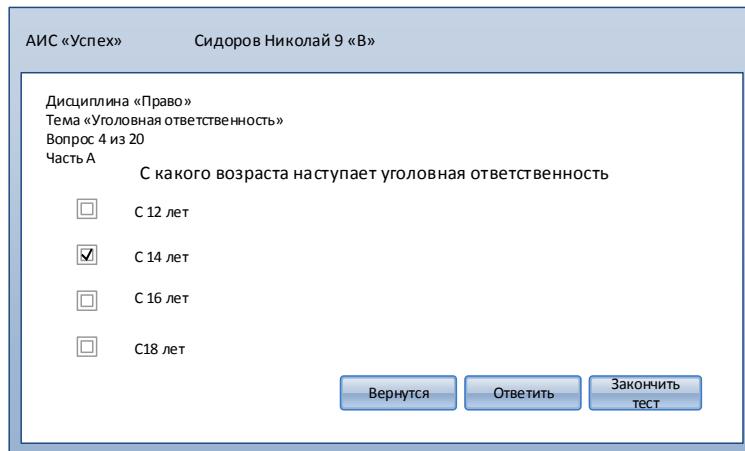


Рис. 6. Интерфейс АИС «Успех»

Так же, как и АИС «Учета посещаемости и успеваемости», АИС «Успех» очень просто использовать. Можно за считанные минуты создать и добавить тест. Обучение использованию программы не требуется. Еще одним огромным плюсом явилось то, что перед тем как программа загрузит тест необходимо авторизоваться, а после каждого ответа программа записывает ответ. То есть даже в случае если программа «вылетит», все ответы сохраняются.

Комплекс АИС «Учета посещаемости и успеваемости» в сочетании с АИС «Успех» позволяют:

- облегчить заполнение журналов;
- позволяет корректировать допущенные ошибки при заполнении документации;
- ускорить процесс проверки знаний обучающихся;
- онлайн контроль родителей (опекунов) за успеваемостью и посещаемостью обучающегося.

#### Список используемых источников

1. LMS Школа – электронная система для современного педагога [Электронный ресурс] – Режим доступа: <http://www.lms-school.ru/> (Дата обращения 22.02.2014).
2. Разработка и эксплуатация автоматизированных информационных систем : учебник [Электронный ресурс] / Д. Э. Фуфаев, Э. В. Фуфаев. – Режим доступа: [http://www.mdk arbat.ru/bookcard?book\\_id=658343](http://www.mdk arbat.ru/bookcard?book_id=658343) (Дата обращения 22.02.2014).

*Статья представлена научным руководителем канд. техн. наук, доцентом П. А. Волынкиным.*

УДК 654.739

Д. В. Шарафанов (аспирант кафедры БИС СПбГУТ)

## ЗАЩИТА ОТ DDoS-АТАК МЕТОДОМ ПРОКСИРОВАНИЯ

Построение эффективной защиты интернет – ресурса от внешних угроз является важным аспектом поддержания и развития любого востребованного и конкурентного проекта в сети. Часто встречающимся видом атак на ресурсы является DDoS-атака, которая, может существенно подорвать работоспособность ресурса.

Понятно, что большая часть владельцев средних и малых по популярности сайтов и сервисов зачастую не располагают достаточными ресурсами для организации собственной системы защиты от DDoS-атак, а многие провайдеры хостинг площадок и вовсе производят отключение своих серверов при обнаружении атаки [1]. Данный факт дал толчок для появления и развития сервисов, предлагающих комплексную защиту. Большая часть подобных компаний предлагают построение защиты методом проксирования – наиболее гибким и эффективным способом отражения DDoS-атак [2].

В данной статье рассмотрена технология построения защиты методом проксирования, применяемая в большинстве компаний, предлагающих защиту от DDoS-атак. Удаленная защита ресурса от атак проксированием или, как ее принято называть «защита без переноса проекта», фильтрует весь входящий трафик на серверных мощностях провайдера защиты, что позволяет противодействовать DDoS-атакам различных видов, в том числе атакам методом SYN Flood. Это решение дает возможность контролировать и анализировать входящий трафик при использовании злоумышленниками любых сетевых протоколов, в том числе HTTP, HTTPS, TCP, UDP с поддержкой SSL Certificates.

### *Процесс отражения DDoS-атаки с использованием метода проксирования*

Работу системы защиты от распределенных атак на обслуживание с применением метода проксирования можно разделить на несколько ключевых этапов.

#### *1 DNS перенаправление входящего трафика*

В основе работы сервисов обеспечения защиты от DDoS-атак лежит метод DNS перенаправления входящего трафика с последующей его фильтрацией на основе паттернов ложных запросов. Применение подобного метода позволяет полностью перенести всю нагрузку от процесса фильтрации и анализа данных входящих запросов на серверные мощности оператора защиты.

При применении метода защиты проксированием, все запросы, как от реальных пользователей, так и от компьютеров – ботов, задействованных в атаке, идут на домен атакуемого проекта, затем, путем изменения настроек параметров DNS, весь трафик и все полученные пакеты перенаправляются на предоставленный IP-адрес в сетевой инфраструктуре оператора защиты [3].

После регистрации запроса, все пакеты данных перенаправляются на принимающий сервер сервиса защиты от DDoS-атак, где происходит процесс их анализа и последующей фильтрации. Проксирование – особый вид сетевой маршрутизации, при котором входящий пул запросов к требуемому сетевому ресурсу изначально перенаправляется на сервера, предназначенные для фильтрации.

## *2 Фильтрация входящего трафика*

Входящие данные направляются на принимающий сервер оператора защиты, который анализирует трафик на предмет соответствия полученных пакетов данных введенным шаблонам вредоносных запросов различного типа. Фильтрация трафика может осуществляться на основе различных подходов, основными из которых являются автоматический и поведенческий методы анализа. В основе автоматического метода лежит сравнение заголовков принимаемых пакетов с набором шаблонов в постоянном режиме, без внесения корректировок в соответствии с текущими вредоносными запросами, что означает отсутствие явной реакции на модернизацию и изменение основы паразитного трафика.

В основе поведенческой защиты заложена глубокая инспекция пакетов вплоть до 7-го уровня (Deep Packet Inspection), что позволяет анализировать не только заголовки запросов, но и их содержание и оперативно менять модель паттернов атакующих запросов. Deep Packet Inspection (сокр. DPI) – метод агрегации статистических данных о принимаемых сетевых пакетах на серверах фильтрации оператора защиты [4]. Применение данного метода позволяет принять решение о степени ложности входящего трафика и произвести оперативное обновление заданных шаблонов в автоматическом режиме на основе не только содержимого полученных пакетов, но и на основе косвенных признаков, присущих определенным видам запросов или протоколам. Подобными признаками могут служить, к примеру, повторение спецсимволов в содержании запросов.

Грамотно реализованный механизм поведенческой фильтрации входящего трафика позволяет вести накопление и анализ статистики, обучение и адаптивное построение многомерной модели распределения трафика для штатных условий работы защищаемых сетей и сетевых сервисов, выявление DDoS-атак на основе отклонений и аномалий, блокирование нелегитимного трафика методом динамической фильтрации сетевых пакетов с автоматической генерацией сигнатур DDoS-атаки в реальном времени [4].

При этом уровень блокирования легитимных обращений крайне низок. Результат анализа статистических данных после фильтрации данным методом можно визуально отобразить в виде графика, изображенного на рисунке.



Рисунок. Трехмерная модель поведенческого анализа

После фильтрации, сервера оператора сервиса защиты пропускают прошедшие через все фильтры запросы от реальных пользователей на IP адрес сервера защищаемого проекта в сетевой инфраструктуре заказчика посредством проксирования трафика.

### 3 Перенаправление очищенного трафика

После фильтрации входящего трафика на ресурсах сетевой инфраструктуры провайдера защиты, легитимный трафик должен быть перенаправлен на рабочие сервера защищаемого проекта, для чего используется метод проксирования. Способ перенаправления прошедших проверку запросов вариативен и зависит от используемых проектом протоколов передачи данных в штатном режиме.

### Заключение

В данной статье рассмотрен принцип работы метода проксирования, являющимся одним из основных применяемых методологий сервисами по защите проектов от распределенных атак на отказ в обслуживании. В качестве заключения, следует выделить основные преимущества и недостатки использования сервисов защиты, использующих метод проксирования.

Данный метод защиты обладает несколькими значительными преимуществами перед построением собственной защиты непосредственно на

ресурсах проекта или перед полным переносом данных проекта в сетевую инфраструктуру провайдера защиты:

1. Быстрое внедрение – развертывание системы защиты от DDoS-атак осуществляется в течение 40 минут после обращения к оператору защиты, в том числе при действующей атаке.

2. Низкая стоимость в сравнении с покупкой дорогостоящего оборудования и поддержания квалифицированных кадров для работы и настройки систем фильтрации трафика за счет использования сервиса по модели SaaS.

3. Большая пропускная способность кластера фильтрации и возможность оперативной масштабируемости под серьезные атаки.

4. Большой опыт подобных компаний в отражении DDoS-атак, ведь, как правило, атаки различной силы на множество проектов происходят постоянно.

### **Список используемых источников**

1. **Типы** сетевых атак, их описания, средства борьбы [Электронный ресурс] / М. Кадер. – Cisco, 2009. – Режим доступа: [http://lagmanjoin.narod.ru/spy/CNEWS/cisco\\_attacks.html](http://lagmanjoin.narod.ru/spy/CNEWS/cisco_attacks.html) (Дата обращения 26.04.2014).
2. **Защита** от DDoS-атак: Механизмы предупреждения, обнаружения, отслеживания источника и противодействия / А. В. Уланов, И. В. Котенко. – 2007. – 43 с.
3. **Система** анализа устойчивости распределенных компьютерных сетей к атакам на «отказ в обслуживании» / М. В. Щерба // Омский научный вестник. Серия «Приборы, машины и технологии». – 2012. – № 1 (106). – С. 282–286.
4. **Метод** фильтрации входящего трафика на основе двухслойной рекуррентной нейронной сети / М. Е. Бурлаков // Ползуновский вестник. – 2012. – № 3/2. – 217 с.

*Статья представлена научным руководителем канд. техн. наук, доцентом С. В. Хорошенко.*

# ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОНИКИ

УДК 51-74:621

А. И. Андриянов (доцент кафедры ЭРЭС БГТУ)  
И. Ю. Бутарев (аспирант ЭРЭС БГТУ)

## НЕЛИНЕЙНАЯ ДИНАМИКА ОДНОФАЗНЫХ КОРРЕКТОРОВ КОЭФФИЦИЕНТА МОЩНОСТИ

Активные корректоры коэффициента мощности нашли широкое применение в составе современных источников электропитания. Основной задачей корректора коэффициента мощности является формирование синусоидального потребляемого тока, совпадающего по фазе с сетевым напряжением, что позволяет исключить потребление реактивной мощности, а также мощности искажений, негативно влияющей на потребителей, подключенных к той же сети.

Корректоры коэффициента мощности представляют собой замкнутые системы автоматического управления, имеющие в своем составе как контур тока, так и контур напряжения. Наилучшее качество потребляемого из сети тока обеспечивают корректоры мощности на основе повышающего преобразователя, работающего в режиме непрерывных токов [1].

Практика показывает, что при работе активных корректоров коэффициента мощности возможно возникновение непроектных динамических режимов, что сопровождается значительным снижением коэффициента мощности на входе и, соответственно, ростом искажений напряжения сети, к которой они подключены [2, 3]. Определение коэффициента мощности дано в [1]. Исключение непроектных режимов может быть выполнено как с использованием параметрического синтеза, когда выбирается определенный набор параметров, обеспечивающих проектный режим, так и с помощью структурного синтеза, когда проектный режим обеспечивается системой управления, реализующей специализированный алгоритм управления. Указанные методы соответствуют так называемому бифуркационному подходу к проектированию [2, 3].

На сегодняшний день подавляющее большинство работ, посвящено исследованию нелинейной динамики преобразователей постоянного напряжения [2, 3]. Основным отличием корректоров коэффициента мощности от

указанного класса систем является наличие внешнего периодического воздействия с частотой сети, что и определяет период повторяемости динамических процессов в подобных системах.

Корректор коэффициента мощности на основе повышающего преобразователя являлся объектом исследования целого ряда работ [4–6]. Основной их чертой является исследование физических явлений в рассматриваемых системах, зачастую базирующихся лишь на использовании метода установления, что ограничивает возможности бифуркационного анализа таких систем.

Кроме того, на сегодняшний день не сформированы требования к проектному динамическому режиму в однофазных корректорах коэффициента мощности. Данные требования будут существенно отличаться от требований к проектным динамическим режимам преобразователей постоянного напряжения.

Функциональная схема корректора коэффициента мощности представлена на рисунке 1. Здесь приняты следующие обозначения:

- $R$  – активное сопротивление дросселя,  
 $L$  – индуктивность дросселя,  
 $C$  – емкость конденсатора,  
 $R_h$  – сопротивление нагрузки,  
 $U_m$  – амплитуда входного напряжения,  
 $w$  – частота входного синусоидального напряжения,  
 $U_{zh}$  – задание на напряжение,  
 $U_{zt}$  – задание на ток,  
 $U_i$  – импульсы управления силовым ключом,  
 $U_{osn}$  – напряжение обратной связи по напряжению,  
 $U_{ost}$  – напряжение обратной связи по току,  
 $U_{osh}$  – ошибка по напряжению,  
 $U_{otsh}$  – ошибка по току,  
 $U_{un}$  – сигнал управления напряжением,  
 $U_{ut}$  – сигнал управления током,  
 $R_h$  – сопротивление нагрузки,  
 $U_p$  – развертывающее напряжение,  
 $\alpha_1$  – коэффициент усиления пропорционального регулятора напряжения,  
 $\alpha_2$  – коэффициент усиления пропорционального регулятора тока,  
 $\beta_1$  – масштабный коэффициент цепи обратной связи по напряжению,  
 $\beta_2$  – масштабный коэффициент цепи обратной связи по току,  
 $\beta_3$  – коэффициент датчика выходного напряжения выпрямителя.

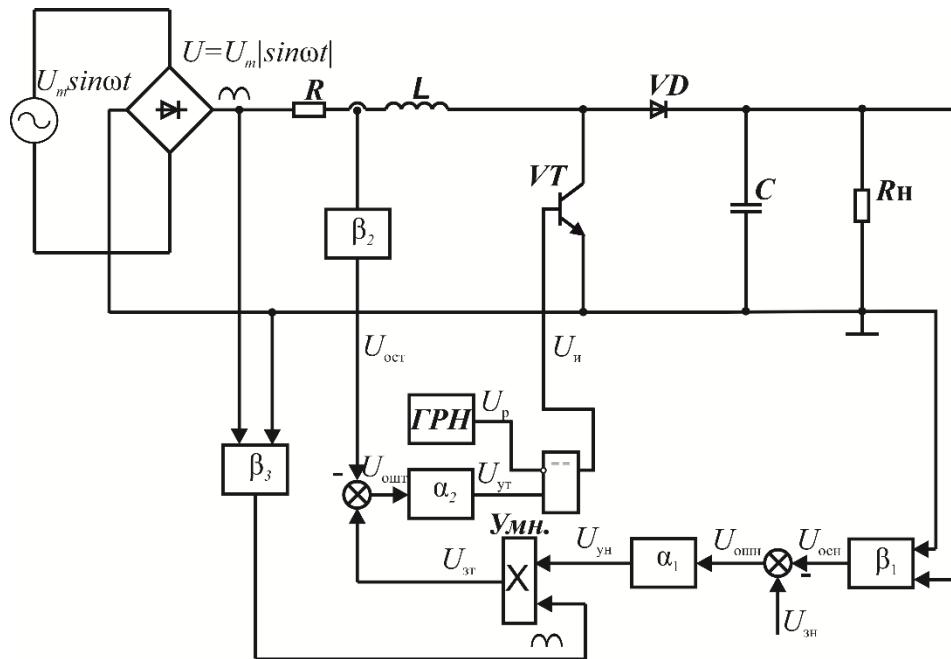


Рис. 1. Функциональная схема корректора коэффициента мощности

Исследование нелинейной динамики корректора коэффициента мощности проводилось с использованием универсальной математической модели преобразователей напряжения и специализированных алгоритмов, рассмотренных в [7].

В ходе расчетов выбран следующий набор параметров:

$U_m = 311$ В	$L = 0,8$ мГн	$\alpha_2 = 0,5$
$W = 314$ Гц	$C = 25$ мкФ	$\beta_1 = 0,015$
$R_H = 150$ Ом	$U_p = 10$ В	$\beta_2 = 1$
$f_{\text{кв}} = 40$ кГц	$U_{\text{зн}} = 7$ В	$\beta_3 = 0,0015$
$R = 1$ Ом	$\alpha_1 = 50$	коэффициент мощности не менее $K_{M\min} = 0,8$

На рисунке 2 представлена карта динамических режимов, на которой отмечены области существования различных режимов в пространстве двух параметров: напряжения задания на напряжение  $U_{\text{зн}}$  и амплитуды входного напряжения  $U_m$ . На карте символами  $\Pi_{i,j}$  будут отмечены области существования различных динамических режимов ( $i$  –  $m$ -цикл, характерный для данной области,  $j$  – номер области на карте динамических режимов). В частности, область  $\Pi_{1,1}$  представляет собой первую область существования основного (проектного) режима с частотой  $w$  (1-цикл). Область  $\Pi_X$  – соответствует недетерминированным режимам функционирования преобразователя ( $m \rightarrow \infty$ ).

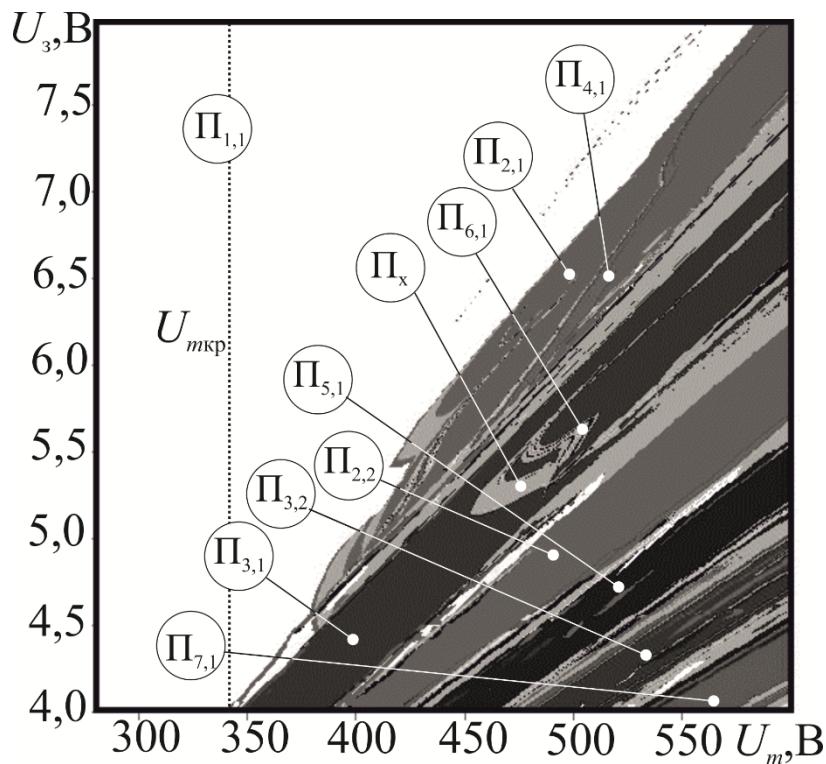
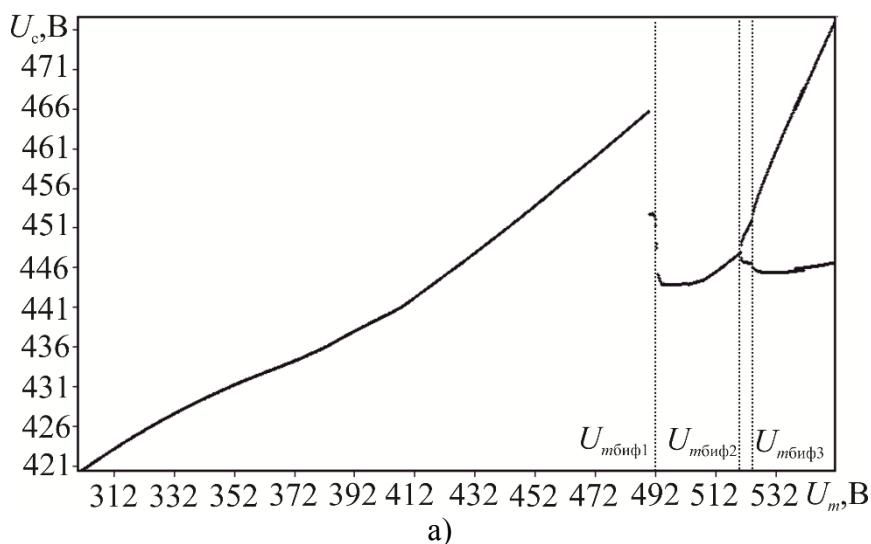


Рис. 2. Карта динамических режимов корректора коэффициента мощности

Как видно из рисунка 2, при амплитуде входного напряжения менее  $U_{m\text{кр}} = 339$  В в системе во всем диапазоне вариации задающего воздействия реализуется 1-цикл. Однако при высоких входных напряжениях в результате бифуркации возникают непроектные режимы с частотой повторяемости меньше, чем напряжение сети.

На рисунке 3 представлена однопараметрическая бифуркационная диаграмма и диаграмма мультиплликаторов матрицы монодромии периодических режимов.



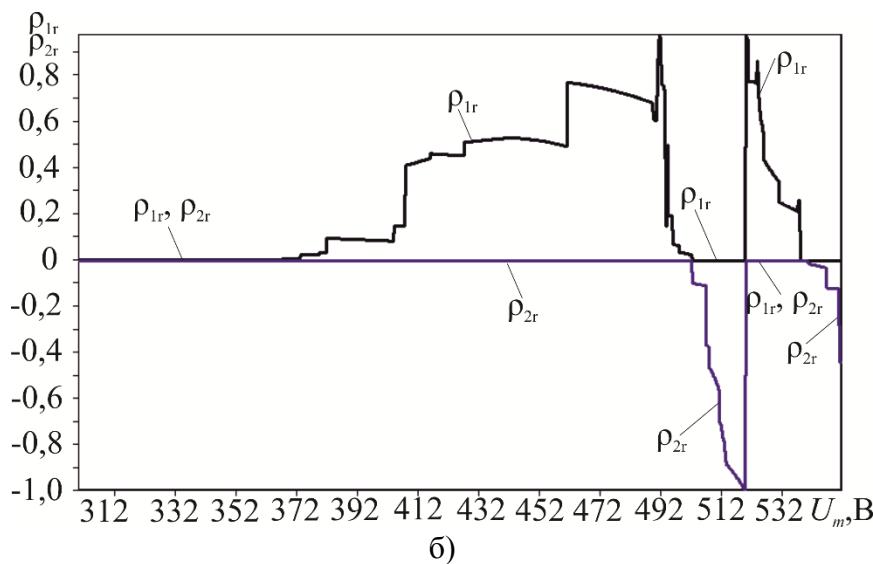


Рис. 3. Однопараметрические диаграммы: а) бифуркационная диаграмма;  
б) диаграмма мультиликаторов периодических режимов

Анализ показывает, что при увеличении амплитуды входного напряжения мультиликаторы претерпевают множественные разрывы первого рода. В точках разрывов реализуются *C*-бифуркации смены типа решения, при которых изменяется число участков гладкости на периоде решения [3]. Таким образом, при  $U_m \in [300 \text{ В} - 520 \text{ В}]$  существует 1-цикл, но при изменении амплитуды входного напряжения постоянно меняется его тип.

При  $U_{\text{биф}1} = 492 \text{ В}$  происходит смена типа решения 1-цикла, приводящая к существенному изменению формы входного тока, также одновременно резко меняются и мультиликаторы (рис. 3, б). В точке бифуркации  $U_{\text{биф}2} = 520 \text{ В}$  происходит классическая суперкритическая бифуркация, при которой действительная часть одного из мультиликаторов пересекает  $-1$  после чего возникает цикл удвоенного периода. При  $U_{\text{биф}3} = 524 \text{ В}$  происходит бифуркация смены типа решения, в результате которой возникает 2-цикл другого типа.

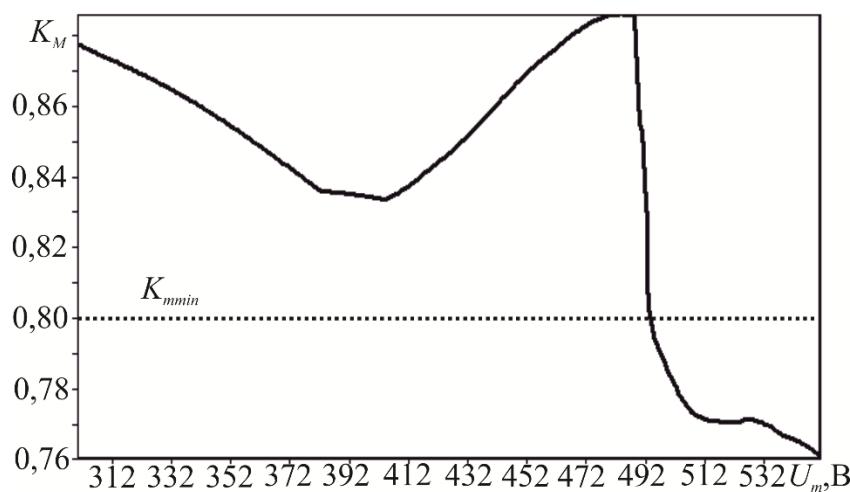


Рис. 4. Однопараметрические диаграммы коэффициента мощности

Таким образом, под проектным режимом корректора коэффициента мощности будем понимать цикл периода один, при котором коэффициент мощности входит в заданный диапазон, при этом коэффициенты заполнения ШИМ на некоторых тактовых интервалах могут принимать значения 0 или 1, что отличается от требований к проектному режиму преобразователей постоянного напряжения [2, 3] (рис. 4).

### Список используемых источников

1. Транзисторная преобразовательная техника / В. И Мелешин. – М. : Техносфера, 2005. – 627 с.
2. О недетерминированных режимах функционирования стабилизатора напряжения с широтно-импульсным регулированием / В. С. Баушев, Ж. Т. Жусубалиев // Электричество. – 1992. – № 8. – С. 47–53.
3. Бифуркации и хаос в релейных и широтно-импульсных системах автоматического управления / Ж. Т. Жусубалиев, Ю. В. Колоколов. – М. : Машиностроение-1, 2001. – 120 с.
4. Модель корректора коэффициента мощности с управлением внутри одного тактового цикла / А. И. Андриянов, А. А. Малаханов // Системы управления и информационные технологии. – 2007. – № 1.1 (27). – С. 108–113.
5. Control of Fast Scale Bifurcations in Power-Factor Correction Converters / D. Giaouris, S. Banerjee, B. Zahavi, V. Pickert // IEEE Transactions on Circuits and Systems – II: Express Briefs. – 2007. – Vol. 54, № 9. – PP. 805–809.
6. Fast-Scale Instability of Single-Stage Power-Factor-Correction Power Supplies / X. Wu, C. K. Tse, O. Dranga, J. Lu // Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on. – 2005. – Vol. 3. – PP. 2477–2480.
7. Алгоритмы для бифуркационного анализа обобщенной модели преобразователей постоянного напряжения / А. И. Андриянов, Н. И. Булохов // Справочник. Инженерный журнал. – 2013. – № 10. – С. 30–39.

## ЭКОНОМИКА И УПРАВЛЕНИЕ В СВЯЗИ

**УДК 339.13:654(470)**

**Ю. А. Кострикова (аспирант кафедры ЭУС СПбГУТ)  
Ю. В. Бобрик (студентка группы ЭМ-27 СПбГУТ)**

### **ИССЛЕДОВАНИЕ ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКИХ ПРОБЛЕМ РЕГУЛИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННОГО РЫНКА СВЯЗАННЫХ СО ВСТУПЛЕНИЕМ РОССИЙСКОЙ ФЕДЕРАЦИИ в ВТО**

22 августа 2012 года, после 18 лет переговоров, Российская Федерация стала членом Всемирной торговой организации. Соглашением, регулирующим телекоммуникационную отрасль в рамках ВТО, является «Соглашение по основным телекоммуникационным услугам», являющееся секторальным. Основной целью ВТО является стимуляция экономического роста и распространение принципа свободной торговли. Ученые расходятся в оценках произошедшего и прогнозах развития экономики. Большое количество работ посвящено изучению опыта зарубежных стран и прогнозам развития отраслей сельского хозяйства, пищевой промышленности, машиностроения, добывающей промышленности и т. д. Крайне ограниченное количество работ посвящено анализу последствий от вступления Российской Федерации в ВТО для отрасли электросвязь. Поэтому актуально исследовать возникшие в связи со вступлением Российской Федерации в ВТО последствия для телекоммуникационной отрасли, выделить основные организационно-экономические проблемы регулирования телекоммуникационного рынка, возникшие в связи с присоединением к данной международной организации, и предложить их решение.

Рассмотрим последствия от вступления Российской Федерации в ВТО с точки зрения основных участников рынка – государственного регулятора, поставщиков телекоммуникационных услуг, потребителей телекоммуникационных услуг и поставщиков телекоммуникационного оборудования.

В общем виде основные требования ВТО для телекоммуникационной отрасли страны – члена ВТО схожи с требованиями, задекларированными в российском законодательстве к работающим на российском рынке телекоммуникационным компаниям. Основное требование ВТО в области электросвязи – обеспечение абонентов качественной связью [1, 2]. Государственный регулятор оказался готов к требованиям ВТО, реализуемым в телекоммуникационной отрасли, так как данные требования осуществля-

лись и до вступления Российской Федерации в данную международную организацию.

К числу возникших сложностей в области государственного регулирования [3, 4], над которыми Минкомсвязь ведет работу на данный момент, можно отнести:

1. Независимость регулятора от участников рынка. Возникла необходимость вывода государственных чиновников из советов правления телекоммуникационных компаний.

2. Обоснованность цен на услуги связи на основании себестоимости.

3. Распределение радиочастотного спектра. В данном вопросе должен присутствовать принцип справедливости, в связи с ограниченностью ресурсов.

4. Развитие межсетевого взаимодействия. На данный момент в Российской Федерации законодательно запрещено совместное использование базовых станций несколькими операторами. Тем не менее, наблюдается активная работа в данной области. Среди положительных тенденций в области межсетевого взаимодействия операторов, стоит отметить закон о переносе абонентского номера от оператора к оператору, позволивший повысить качество услуг связи, и сокративший рост абонентской базы.

Если рассматривать российский телекоммуникационный рынок с точки зрения последствий для его участников, последствия для поставщиков телекоммуникационных услуг оказались практически не ощущимы. Об этом свидетельствуют данные, приведенные в таблице 1.

ТАБЛИЦА 1. Инвестиции в телекоммуникационную отрасль до вступления в ВТО и после [5]

Наименование показателей	9 месяцев 2012 г.	9 месяцев 2013 г.	в % к 9 месяцам 2012 г.
<b>Капитальные вложения – всего, млн руб.</b>	<b>182 600,0</b>	<b>160 200,0</b>	<b>87,7</b>
<b>Инвестиции из-за рубежа в отрасль «Связь» (данные Росстата России) – всего, млн \$</b>	<b>2 225,0</b>	<b>1 672,0</b>	<b>75,1</b>
в том числе прямые инвестиции	79,0	432,0	546,8
портфельные	11,0	0,0	0,0
прочие инвестиции	2 135,0	1 240,0	58,1

Главным риском от вступления в ВТО для отрасли являлось появление иностранных компаний-операторов, способных конкурировать с операторами Большой тройки. Принцип либерализации торговли является основным принципом, реализуемым ВТО, тем не менее, его реализация в условиях российского телекоммуникационного рынка оказалась не воз-

можна. В Российской Федерации сложился стабильный рынок, попасть на который довольно сложно. Барьер для входа на рынок для новых иностранных компаний установлен не законодательно, а сложился естественным путем. Во-первых радиочастоты распределены между операторами Большой тройки, во-вторых в сравнении с телекоммуникационными рынками других стран, российский рынок не столь привлекателен из-за необходимости большого количества инвестиций в сооружение объектов связи, и относительно низкой окупаемостью инвестиций в связи с неравномерностью распределения населения на огромной территории, и неравномерно распределенным доходом населения. Зарубежных операторов пугает необходимость выполнения столь больших объемов работы за столь низкую прибыль. От вступления в ВТО российские операторы получают выгоду, хоть и сомнительную, в связи с тем, что стоимость иностранного оборудования для сооружения объектов связи существенно снижается благодаря либерализации таможенных ограничений. Обилие и дешевизна телекоммуникационного оборудования иностранных производителей отрицательно скажется на обеспечении государственной безопасности.

Одним из последствий вступления в ВТО является повышение себестоимости услуг связи за счет введения новых норм сертификации и лицензирования. Средства, потраченные на покупку требуемых лицензий, будут перенесены на стоимость услуг связи. Международные соглашения в сфере предоставления телекоммуникационных услуг затрагивают только сектор базовых услуг, дополнительные виды обслуживания, практически не затронуты, поэтому, можно спрогнозировать увеличение стоимости дополнительных видов обслуживания. Также, международные соглашения декларируют необходимость обоснования себестоимости услуги связи, что является не очень логичным. Потому, что рассматривать отдельную услугу связи не логично, так как используемый абонентом тарифный план сбалансирован с учетом взаимной выгоды потребителя и поставщика телекоммуникационных услуг. Например, практически все операторы реализуют в некоторых тарифных планах определенное количество бесплатных минут голосового трафика. С учетом того, что канал связи предоставляется абоненту бесплатно, оператор несет затраты, которые перенесены на стоимость остальных предоставляемых мобильных услуг. Проследить изменение доходов в отрасли можно в таблице 2. Таблица свидетельствует, что темпы роста дохода отрасли замедлились.

ТАБЛИЦА 2. Изменение экономических показателей отрасли  
с момента вступления в ВТО (в млн руб.) [5]

Наименование показателей	9 месяцев 2013 года	в % к 9 месяцам 2012 года
Доходы от услуг связи – всего	1 184 643,4	104,3
Объем реализации услуг связи населению – всего	662 934,8	105,7
От услуг по обеспечению регулирования использования радиочастотного спектра и радиоэлектронных средств (РЭС) – всего	2 720,3	113,0
От услуг по обеспечению регулирования использования радиочастотного спектра и радиоэлектронных средств (РЭС) от населения	1,2	47,8

Если рассматривать российский телекоммуникационный рынок с точки зрения потребителей, то на практике особых улучшений они пока что не почувствуют. Так как унификация требований ВТО и Минкомсвязи практически не нужна, и заданный вектор развития останется тем же.

Если рассматривать телекоммуникационный рынок с точки зрения поставщиков телекоммуникационного оборудования, то можно прийти к выводу, что сильный ущерб нанесен именно данному сектору. В связи с технологической отсталостью, сформированной экономическим спадом периода перестройки, отечественные производители не смогли занять достойное место на мировом рынке производителей. Оказывать государственную поддержку отечественным производителям можно благодаря соглашению о вступлении в ВТО, только в рамках государственных закупок.

Решением проблемы являются сами законодательные положения ВТО в данной области. Правила ВТО способствуют развитию систем сертификации и лицензирования оборудования. Помимо сертификации и лицензирования международными органами, ВТО поощряет развитие национальных систем лицензирования и сертификации. При внедрении сертифицированной системы управления качеством при производстве отечественного телекоммуникационного оборудования, основанной на требованиях регулятора можно снизить издержки отечественного производителя по сравнению с зарубежным, и дать ему некий «запас прочности» [6].

В свою очередь, необходимо очень тонкая юридическая проработка вопроса, в связи с тем, что вступив в ВТО Российская Федерация согласилась на применение принципов свободной торговли. Производимое за рубежом телекоммуникационное оборудование в большинстве своем не отвечает стандартам многих климатических зон Российской Федерации, не рассчитано на резкоконтинентальный климат Сибири и географический рельеф и климат Дальнего Востока.

Чтобы дать возможность для развития отечественному производителю необходимо создать новые ниши рынка телекоммуникационного оборудования. Необходимо ввести собственные, узкоспециализированные стандарты и требования к приемке телекоммуникационного оборудования в каждом субъекте Российской Федерации, с целью повышения эффективности и срока работы телекоммуникационного оборудования. Отечественный производитель сможет удовлетворить потребности рынка наиболее полно, так как основные мировые производители телекоммуникационного оборудования производят продукцию, изначально под потребности своей страны. Потребности Российской Федерации сложно сравнить с потребностями других стран. Сходные потребности в характеристиках оборудования испытывает Канада и США, но тем не менее в силу специфики отношения данных стран к производству телекоммуникационного оборудования, предлагаемое соотношение цены и качества импортной продукции будет не конкурентоспособно.

На данный момент российский телекоммуникационный рынок проходит через стадию приведения национальных стандартов к международным. Правильная политика Минкомсвязи и уникальность рыночных условий сделали процесс вступления в ВТО практически безболезненным для отрасли. Максимально сгладить все неприятные последствия от вступления в ВТО можно исключительно при помощи государственного регулирования отрасли.

### Список используемых источников

1. Управление инновациями и обеспечение качества в отрасли ИКТ : монография / В. В. Макаров. – СПб. : Издательство СПбГУТ, 2012. – 164 с.
2. Investment policies and telecommunications regimes //Trade, investment and competition policies in the global economy : the case of the international telecommunications regime Baden-Baden : Nomos, 2002, 80 р.
3. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 02.04.2014) «О связи» (с изм. и доп., вступ. в силу с 01.05.2014) [электронный ресурс]. – Режим доступа: [/http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=153866/](http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=153866/)
4. Телекоммуникации России: состояние, тенденции и пути развития / В. В. Макаров : монография. – М. : ИРИАС, 2007. – 296 с.
5. Сайт Минкомсвязи, статистика отрасли за 3 квартал 2013 года [Электронный ресурс]. – Режим доступа: <http://minsvyaz.ru/ru/directions/stat/stat/>
6. General Agreement on Trade in Services [Электронный ресурс]. – Режим доступа: [/http://www.wto.org/english/tratop\\_e/serv\\_e/serv\\_e.htm/](http://www.wto.org/english/tratop_e/serv_e/serv_e.htm/)

*Статья представлена научным руководителем  
д-ром экон. наук, профессором В. В. Макаровым.*

УДК 338.47

**Карпенко М. В. (студент 3 курса, СПбГУТ)**

## **РАЦИОНАЛЬНЫЕ СПОСОБЫ НАЧИСЛЕНИЯ ОПЛАТЫ ЗА УСЛУГУ ДОСТУПА К СЕТИ ИНТЕРНЕТ**

Всего за 20 с небольшим лет, с момента предложения Тимом Бернерсом-Ли в 1989 г. протокола HTTP, языка HTML и идентификаторов URL, Всемирная паутина (Интернет) получила широчайшее распространение и проникла практически в каждый уголок нашей планеты, что позволяет нам, потребителям, пользоваться услугами сети Интернет находясь на улице, в транспорте, в кинотеатрах, пунктах общественного питания и т. д. При этом актуальным остается понятие стоимости или цены потребления услуги как суммы цены приобретения и затрат до полного прекращения использования. При этом особый интерес представляет средняя цена потребления за определенный период: месяц (год). Что можно понимать под словом рациональная оплата? Вероятнее всего учет всех скидок и бонусов и оптимальный тарифный план, который позволит иметь идеальную (минимальную) цену потребления:

$$\text{ЦП}_i^S = \frac{1}{m} C_{np} + \sum_{i=0}^{i=n} C_i^o - \sum_{k=1}^{k=p} C_k^o$$

где ЦП<sub>i</sub><sup>S</sup> – цена потребления идеальная; абонента *s* ;

$\frac{1}{m} C_{np}$  – стоимость приобретения (*m* – число месяцев до прекращения использования);

$\sum_{i=0}^{i=n} C_i^o$  – стоимость всех соединений и сервисов, которые были осуществлены и получены через основного оператора;

$\sum_{k=1}^{k=p} C_k^o$  – стоимость всех бонусов и скидок [1].

Оптимальный тарифный план выбирается из набора, предоставляемого оператором с которым заключен договор. Имея ноутбук или карманный персональный компьютер с контроллером Wi-Fi, посетители кафе или ресторана (в зоне покрытия сети Wi-Fi) могут быстро соединиться с сетью Интернет. При этом использование Wi-Fi представляет собой бонус, исходящий не от основного провайдера, а от продавца других товаров или услуг. Кроме того, следует отметить тенденцию мнимого «обесценивания» Wi-Fi, а именно: предоставление клиентам доступа к сети Интернет бесплатно. На самом деле, затраты на установление и обслуживание беспроводного доступа к сети Интернет также приходится оплачивать потребителям. На данный момент наиболее распространенным способом начисления

оплаты за данную услугу в пунктах общественного питания является перенесение части стоимости подключения к сети Интернет на предоставляемую кулинарную продукцию, то есть повышение цен на продукцию в меню. Исходя из этого, можно сделать вывод, что в большинстве случаев интересы клиентов в части использования услуги доступа к сети Интернет не учитываются, что приводит к несправедливости в отношении оплаты услуг пунктов общественного питания. Для примера следует рассмотреть несколько групп клиентов, которые имеют различные потребности в отношении приобретения кулинарной продукции и использовании услуг доступа к сети Интернет:

Группа А – клиенты, которые посещают пункты общественного питания, чтобы приобрести кулинарную продукцию и воспользоваться услугой доступа к сети Интернет.

Группа Б – клиенты, которые посещают пункты общественного питания, чтобы приобрести кулинарную продукцию, а предоставляемые услуги доступа к сети Интернет для них не представляют интереса.

Группа В – клиенты, которые посещают пункты общественного питания, чтобы бесплатно воспользоваться услугами доступа к сети Интернет, не приобретая кулинарную продукцию.

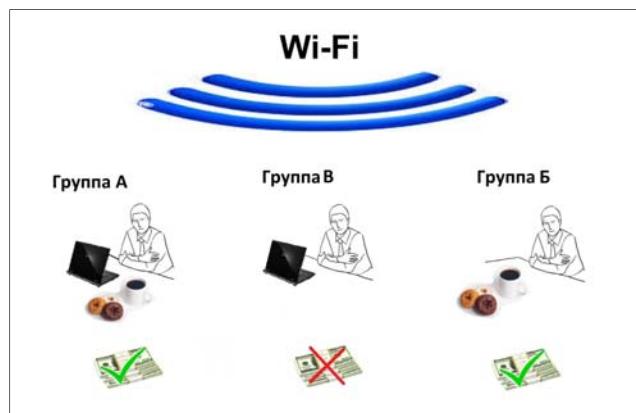


Рис. 1. Визуальное представление клиентов групп А и В

В данном случае несправедливость по отношению к группе А заключается в том, что они оплачивают доступ к сети Интернет не только для себя, но и для клиентов группы В.

Несправедливость по отношению к группе Б основывается на том, что они оплачивают доступ к сети Интернет клиентам из группы А и группы В, не пользуясь данной услугой.

Несправедливость по отношению к группе В заключается в том, что они хотели бы оплатить услуги доступа к сети Интернет, но при отсутствии желания потреблять кулинарную продукцию они не могут этого сделать.

Рациональный способ оплаты – это способ оплаты, организованный наиболее разумным образом, целесообразный. Используя это понятие, предлагается заменить традиционное разделение залов на «зал для курящих» и «зал для некурящих» на «зал с беспроводным доступом к сети Интернет» и «зал без беспроводного доступа к сети Интернет», более сокращенно данные залы можно назвать «с Wi-Fi» и «без Wi-Fi». Иными словами, помещения пунктов общественного питания предполагается разделить на помещения, оборудованные для предоставления услуги доступа к сети Интернет, и на помещения, в которых доступ к сети Интернет через Wi-Fi, предоставляемый пунктом общественного питания будет невозможен.

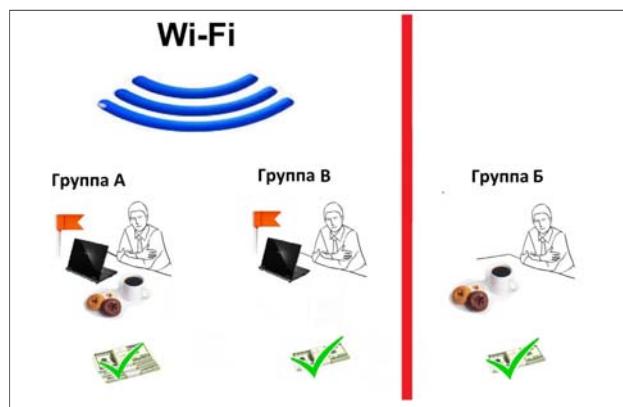


Рис. 2. Визуальное представление клиентов групп А, Б и В при разделении помещений пунктов общественного питания на залы с Wi-Fi и без Wi-Fi

Перейдем к понятию целесообразный, то есть достижение цели с наименьшими потерями. Рассмотрим замечания по поводу безопасности для здоровья человека использования ноутбука с включенным Wi-Fi. В 2011 г. были опубликованы результаты эксперимента по изучению влияния Wi-Fi, в ходе которого было установлено увеличение повреждений их ДНК в 2,5 раза при четырёхчасовой экспозиции на коленях ноутбука с включённым Wi-Fi. Следовательно, необходимо создать условия при которых место для ноутбука на столе всегда свободно, и никому не придет в голову положить его на колени. Такое размещение является достаточным по мнению одного из английских профессоров из университета Ноттингема (Nottingham University) для обеспечения безопасности [2].

Предлагаемая концепция основывается с одной стороны на личном выборе каждого клиента в каком зале он желает провести время, с другой прививает культуру использования Интернета, руководствуясь правилом: выключи, если не нужен. Это понятие перекликается с концепцией «умного дома», которая направлена на экономное рациональное использование всех ресурсов.

Если клиент (группа клиентов) выбирает зал с Wi-Fi, то ему (им) необходимо оплатить фиксированную стоимость за получение доступа к

сети Интернет. В этом случае клиенту (группе клиентов) выдается флагок, который можно поставить на стол, или любой другой знак отличия о том, что клиент (группа клиентов) приобрел (приобрела) услуги доступа к сети Интернет в данном пункте общественного питания.

При этом оплата производится для каждого устройства, которое будет использовано при подключении к сети Интернет, соответственно, флагок (другие знаки отличия) необходимо выдавать в количестве подобных устройств. Именно взимание платы за услугу доступа к сети Интернет за каждое устройство является наиболее рациональной мерой, в связи с тем, что:

1) Реализуется принцип справедливости в отношении оплаты услуги доступа к сети Интернет между клиентами, которые используют либо одно, либо несколько устройств одновременно.

2) Отсутствует несправедливое взимание платы с **группы** клиентов, которые используют одно устройство.

Одним из наиболее важных аспектов в этом случае является контроль за соблюдением клиентами условий использования услуги доступа к сети Интернет. Предполагается, что осуществление наблюдения и контроля возлагается на администратора зала через персональный компьютер и установленное на нем специализированное программное обеспечение.

Примером в данном случае может послужить программа **Wireless Network Watcher**. Данная программа служит для сканирования беспроводных сетей и визуального отображения всех устройств, которые подключены к сети. Использование данной программы обладает рядом преимуществ, таких как:

1) бесплатность использования;

2) визуальное отображение информации, которая включает в себя: IP-адрес устройства, его сетевое имя, MAC-адрес и производитель адаптера;

3) возможность мониторинга сети в фоновом режиме. Иными словами, при новом подключении к сети программой издается соответствующий звуковой сигнал, что обуславливает отсутствие необходимости постоянно присутствия перед персональным компьютером [3].

Таким образом, можно определить целый ряд конкурентных преимуществ при разделении помещений на залы с Wi-Fi и без, а именно:

1) устраняется несправедливость по отношению к клиентам с разными потребностями в части приобретения кулинарной продукции и использования услуг доступа к сети Интернет, а именно: предоставление возможности группе В оплатить услуги доступа к сети Интернет и снижение расходов для клиентов группы Б;

2) отсутствует необходимость изменять цены в меню для различных групп клиентов;

3) принципиально новый привлекаемый формат пунктов общественного питания;

- 4) возможность обеспечения клиентам более качественного Интернет-соединения путем прекращения предоставления услуги доступа к сети Интернет во всех залах;
- 5) широкие возможности применения различного программного обеспечения для мониторинга процесса предоставления услуг доступа к сети Интернет;
- 6) возможность оценки потребностей клиентов в доступе к сети Интернет с помощью различного программного обеспечения и принятия на этой основе решений о сокращении либо расширении площадей, в которых будет предоставляться услуга доступа к сети Интернет;
- 7) внедрение элементов системы поддержки ориентированного на клиента качества [4];
- 8) обеспечение возможности выбора правильной позы при работе с ноутбуком;
- 9) снижение вредного влияния на здоровье человека ноутбука с включенным Wi-Fi;
- 10) повышение культуры использования ресурсов Интернет.

#### **Список использованной литературы**

1. **Цена** потребления мобильной услуги связи / М. В. Карпенко //ХII студенческая международная научно-практическая конференция «Научное сообщество студентов XXI столетия» экономические науки: материалы конференции – Россия, г. Новосибирск 8 октября 2013 г.
2. **Wi-Fi** [Электронный ресурс] / Материалы из Википедии – свободной энциклопедии. – Режим доступа: <http://ru.wikipedia.org/wiki/Wi-Fi> (дата обращения 21.05.14).
3. **Как** узнать, кто подключен к моему Wi-Fi [Электронный ресурс] / Артем Аленин //Компьютеры и Интернет. Безопасность. – 05.11.2012. – Режим доступа: [http://www.freeadvice.ru/view\\_advice.php?id=173](http://www.freeadvice.ru/view_advice.php?id=173) (дата обращения 24.04.14).
4. **Управление** инновациями и обеспечение качества в отрасли ИКТ : монография / В. В. Макаров. – СПб.: Издательство СПбГУТ, 2012. – 164 с.

*Статья представлена научным руководителем  
старшим преподавателем кафедры «Экономика и управление в связи» Старковой Т. Н.*

УДК 374.3

**А. И. Копп (студентка магистратуры кафедры ИТЭ СПбГУТ)**

## **ИННОВАЦИОННЫЙ ПРОЕКТ: ТРЁХУРОВНЕВАЯ БИЗНЕС-МОДЕЛЬ ТЕЛЕКАНАЛА «МОЛОДЕЖНАЯ СРЕДА»**

Предприятия – это основные заказчики и потребители нового интеллектуального капитала. Они ожидают от выпускников высших и средних учебных заведений требуемой профессиональной компетенции. Не всегда теоретические знания студентов соответствуют требованиям производства, поэтому предприятия и учебные заведения реализуют программы сотрудничества [1]. Для школьников проводятся занятия по профориентации в целях расширения их знаний о профессиях, в том числе приоритетных для России, и снижения степени влияния на их выбор одностороннего влияния родителей.

Для решения проблемы низкой осведомленности молодёжи о требованиях производства и разнообразии видов деятельности в статье предлагается инновационный проект трёхуровневой бизнес-модели телеканала «Молодёжная среда».

*Первый уровень* – телестудии образовательных учреждений. Участниками рассматриваются не только российские, но и зарубежные образовательные учреждения. Как правило, между ними заключены программы международного сотрудничества в обучении. Например, зарубежными вузами-партнёрами СПбГУТ являются Telecom Ecole de Management (Эври, Франция), Lappeenranta University of Technology (Лаппеэнранта, Финляндия).

На межвузовской конференции «СМИ в современном мире. Современные исследователи» 3 марта 2010 г. было сообщено, что в том или ином виде университетское телевидение существует в 31 университете России [2]. Большинство университетов (77 %) для трансляции используют интернет (IP-TV). В других случаях (27 %) университетское телевидение выходит на региональных СМИ, например раз в неделю. Кабельное телевидение используют 20 % учебных заведений. Роль университетского телевидения, как одного из видов средств массовой информации, обсуждается на мероприятиях, посвящённых развитию научно-познавательного телевидения. Телеканал «Просвещение» организовал в Московском авиационном институте 17–18 июня 2012 г. первый российский форум пресс-служб и медиацентров вузов России [3]. Было предложено создание единой информационной программы о вузах на базе вещания телеканала «Просвещение» с целью повышения узнаваемости вузов. На форуме прозвучало предложение от представителей вузов предоставлять сюжеты не только

телеканалу «Просвещение», но и осуществлять обмен между университетами, как это делает Дальневосточный федеральный университет.

Накопленный опыт университетами позволяет им сотрудничать по созданию совместных телепередач.

Интернет воспринимается как механизм глобального распространения информации, объединения людей и их взаимодействия вне зависимости от расстояния, временных, государственных и иных ограничений [4, с. 493]

*Второй уровень бизнес-модели* телеканала «Молодёжная среда» заключается в работе интернет–телеканала. Его информационное содержание формируют транслируемые по расписанию программы, разработанные участниками первого уровня бизнес-модели. Предполагается разработка расписания по профилям учебных заведений. Телередакции выходят в прямой эфир или присылают подготовленный сюжет в телередакцию СПбГУТ.

Телеканал «Молодёжная среда» предоставляет интерактивность для зрителя: отправка и просмотр комментариев, оценка сюжета во время вещания, голосование за понравившийся сюжет и выбор будущей темы. Функционирование телеканала «Молодёжная среда» соответствует методике Web 2.0. Идея Web 2.0 состоит в том, что за информационное наполнение рассматриваемого ресурса «отвечают» сами пользователи, разработчики проекта лишь создают условия для размещения информации [5].

В таблице 1 указаны заинтересованные стороны с точки зрения спроса на информационное содержание телеканала «Молодёжная среда».

ТАБЛИЦА 1. Представители спроса на информационное содержание

Потребители	Сфера интересов
Преподаватели, учёные	<ul style="list-style-type: none"><li>• Достижения учебных заведений в научно-исследовательской деятельности</li></ul>
Студенты	<ul style="list-style-type: none"><li>• Получение информации о требованиях производства, лекции преподавателей, мастер-классы, новости учебного заведения, информация о вакансиях и возможности пройти производственную практику</li></ul>
Телеканалы	Показ зрителям передач о научных достижениях и инновационных идеях, заказ сюжетов определённой темы
Школьники, абитуриенты	<ul style="list-style-type: none"><li>• Выбор профессии и учебного заведения</li><li>• Интерес к научно-исследовательской деятельности</li></ul>
Родители	Просмотр мероприятий, новостей учебного заведения, в котором учится их ребёнок
Факультет повышения квалификации	Информация для разработки программ повышения квалификации

Новизна идеи телеканала «Молодёжная среда» заключается в создании распределённой редакции на основе работы телестудий и телередакций высших и средних учебных заведений, формировании информацион-

ного содержания на основе идей, потребностей молодёжи. Предполагается периодическая смена учебного заведения, телередакция которого будет отвечать за работу второго уровня бизнес-модели телеканала «Молодёжная среда».

Предполагаемая тематика сюжетов телеканала «Молодёжная среда»:

1. Новости вузов (спартакиада, Мисс университет, фестивали).
2. Студенческие конференции (полностью или подготовленные сюжеты о результатах, показ лучших выступлений).
3. «Быть в курсе событий» – вузы рассказывают о планируемых в течение месяца мероприятиях в своём городе (ярмарки вакансий, выставки, концерты, форумы, посвящённые проблемам и развитию образовательной сферы и др.).
4. Лекции преподавателей вузов.
5. Сюжеты о Дне открытых дверей вузов.
6. Мастер-классы (например, Тайм менеджмент, Как вести семейный бюджет?, Предпринимательство для студентов).
7. «Путь к успеху» – рассказ о предпринимательском опыте представителей предприятий.
8. «Моя профессия...» – интервью с работодателями, выпускниками вузов.
9. «Мир профессий» – ситуация на рынке труда, информирование о приоритетных профессиях России.
10. «Я люблю свой город...» – история, памятные даты, выдающиеся личности, события и достижения в социальной, культурной, экономической, политической сфере.
11. «Предприятие + вуз = союз» – результаты и программы сотрудничества вузов с предприятиями.
12. «От теории к практике» – предложения работодателей о возможностях прохождения производственной практики, отзывы студентов.
13. «Новости в сфере образования»: участие вузов в форумах, семинарах, законодательство, приоритетные профессии (сюжеты готовятся по очереди вузами, материалы могут предоставляться Министерством образования и науки России).
14. «Актуальные вопросы молодёжи»: поиск и приобретения жилья, трудоустройство, написание резюме, обучение за рубежом, армия, здоровье и другие темы, определяемые по результатам голосования студентов (подготавливаются вузами по очереди).
15. «Диалог»: интервью с деятелями науки, культуры, политики об образовании, карьере.
16. «КВН в вузе».
17. «Чего надо бояться», например, спама, грязных рук, испорченных продуктов.

18. «Иностранный язык в карьере и жизни» – изучение иностранного языка, передачу могут вести преподаватели, студенты, предполагается несколько выпусков в день для разных иностранных языков, являющихся наиболее интересными по результатам голосования.

19. И другие сюжеты, предложенные зрителями.

20. Реклама: фитнес-клубы, вакансии, приглашение на стажировку, конкурсы научно-исследовательских работ, объявляемые предприятиями, молодёжные газеты и журналы, косметика, социальная реклама.

Затраты на предоставление полноценных лекций для одного студента и для тысячи студентов равны за счёт экономии средств при увеличении потребителей образовательных услуг, что увеличивает образовательный уровень населения в целом, т. к. каждый желающий может воспользоваться образовательными услугами дистанционно [4, с. 588].

Финансирование является открытым. Одним из источников финансирования рассматриваются взносы предприятий-партнёров учебных заведений и организаций, желающих способствовать развитию телеканала. Рассматривается обращение к Министерству науки и образования РФ, фондам поддержки образования. Предполагается использовать заинтересованность в размещении рекламы на рассматриваемом телеканале от организаций, целевой аудиторией которых являются молодёжь, в частности студенты, например:

- фитнес-клубы, т. к. спорт, как компонент здорового образа жизни, популярен у молодёжи;
- издательства журналов, выпускающих впервые, имеющих сильную конкуренцию, а также с целью привлечения внимания к материалам с точки зрения профессиональных интересов студентов;
- горнолыжные курорты;
- производители косметики (предмет интереса девушек и женщин);
- организации, заинтересованные в размещении социальной рекламы, в частности для студентов, о пропаганде здорового образа жизни, соблюдении правил дорожного движения и др.

Организации, размещая рекламу на телеканале «Молодёжная среда» получают возможность привлечения молодёжи в рамках количества вузов-партнёров телеканала.

*Третий уровень бизнес – модели телеканала «Молодёжная среда»* заключается в сотрудничестве с каналами эфирного вещания, заинтересованными в транслировании по подписке сюжетов телеканала «Молодежная среда», покупке прав на вещание сюжетов. Например, предполагается интерес телеканалов Россия (программа «Вся Россия» о неизвестных участниках известных исторических событий, рассказы о повседневной жизни соотечественников), 24Техно (программа «Параллели» о мировых разработках в различных областях науки и техники – изобретениях, инновациях, стартапах).

Выводы:

Телеканал «Молодёжная среда»:

- способствует повышению эффективности телестудий ВУЗов, так как за счет рекламы и расширения аудитории будут привлекаться и абитуриенты и потребители рабочей силы;
- с помощью показа лекций преподавателей, семинаров, предоставляет возможность в одном средстве массовой информации объединить участников из разных учебных заведений, не требуя от них временных и финансовых затрат на приезд;
- позволяет реализовать интерактивное общение по актуальным проблемам, волнующим молодежь и не только;
- способствует развитию профессиональных компетенций молодежи, повышению качества образования, увеличению интеллектуального капитала общества, повышению узнаваемости учебных заведений;
- позволяет активно воздействовать на сознание людей в целях гуманизации общества;
- способствует созданию единого информационного пространства, как основы информационного и инновационного общества.

#### **Список используемых источников**

1. **Бизнес и ВУЗы: к проблеме кадрового голода** [Электронный ресурс] / Е. Лиховцева // Эксперт Северо-Запад. – 24.06.2013. – № 25 (622). – Режим доступа: <http://expert.ru/northwest/2013/25/biznes-i-vuzyi-k-probleme-kadrovogo-goloda/> (Дата обращения 31.03.2014).
2. **В 31 российском** вузе есть своё телевидение [Электронный ресурс]: Неделя – информационный портал об образовании. – 03.03.2010. – Режим доступа: <http://www.nedelya.ru/view/66827> (Дата обращения: 20.04.2014).
3. **Форум «Медиакарта высшей школы страны»** [Электронный ресурс] // Московский авиационный институт. – М., 1997–2014. – Режим доступа: <http://www.mai.ru/media/video/index.php?ID=32076> (дата обращения: 09.04.2014).
4. **Интеллектуальный капитал.** Материализация интеллектуальных ресурсов в глобальной экономике: монография / В. В. Макаров, М. В. Семёнова, А. С. Ястребов; под ред. В. В. Макарова. – СПб. : Политехника, 2012. – 688 с.
5. **Инновационные** подходы в управлении телевещанием [Электронный ресурс] / Т. Н. Старкова, А. В. Кудрин // Экономика и современный менеджмент: теория и практика: XXXIV Международная научно-практическая конференция; Новосибирск, 3 февраля 2014 г. – Режим доступа: <http://sibac.info/13229> (дата обращения 05.04.2014).

*Статья представлена научным руководителем,  
д-ром экон. наук, профессором В. В. Макаровым.*

УДК 65.012

**А. И. Копп (студентка магистратуры кафедры ИТЭ СПбГУТ)**

## **РАЗРАБОТКА МЕТОДА ФОРМАЛЬНОГО КОНСТРУИРОВАНИЯ СЕРВИСОВ ПРЕДПРИЯТИЯ НА ОСНОВЕ БИЗНЕС-ПРОЦЕССОВ**

В настоящее время широко распространён процессный подход к управлению предприятием, накапливается база процессных моделей, создаётся архитектура бизнес-процессов [1]. Реализация бизнес-процессов связана с взаимодействием сотрудников, подразделений предприятия, предприятий и их групп. Как правило, взаимодействие сотрудников рассматривается с точки зрения управления персоналом.

В статье взаимодействие сотрудников и подразделений предприятия рассматривается как реализация понятия сервис (услуга), подразумеваемого в качестве объекта управления.

Описание деятельности предприятия с помощью модели взаимосвязанных сервисов позволит провести анализ компетенций предприятия с точки зрения специфики отрасли, целесообразности реализации сервисов, конкурентоспособности. Задача определения наилучшего или приемлемого набора сервисов в структуре предприятия подобна поиску «идеальной» организационной структуры или необходимого набора бизнес-процессов.

Сервисы, как компоненты деятельности предприятия [2], по характеру взаимодействия участников классифицируются на:

- материальные сервисы (при материальном взаимодействии), например, цепочки поставок;
- нематериальные сервисы, которые в свою очередь делятся на:
  - информационные сервисы (например, обмен информацией и документами);
  - когнитивные сервисы (например, консультирование);
- комбинированные сервисы.

На основании накопленного опыта работы с моделями бизнес-процессов в статье рассматривается гипотеза о том, что графическое описание бизнес-процессов с использованием зон разделения ответственности (дорожек, swimlane) позволяет перейти к сервисной модели деятельности на основе формального метода. Визуальными признаками сервиса на процессной диаграмме с использованием зон разделения ответственности являются:

- взаимодействие участников близки во времени и множественны (предлагается в качестве условной единицы времени рассматривать действие – элемент «задача» или «решение»),

- пары взаимодействий могут идти вглубь, но локально замкнуты на одной роли (заказчике).

Процессная диаграмма является ориентированным графом.

Для выявления сервисов предприятия как компонентов его деятельности предлагается формализованный метод, основанный на графическом описании бизнес-процесса с разделением зон ответственности и анализа матриц смежности или инцидентности.

Матрица смежности (инцидентности) содержит информацию о соответствии вершин графа зонам ответственности для определения участников взаимодействия при анализе последовательности вершин и информацию о типе действия для определения постоянства сервиса.

#### *Анализ матрицы смежности для выявления сервисов*

Воспроизвести графическую цепочку связи вершин графа позволяет его матрица смежности. Выбор нумерации вершин влияет на расположение значений элементов в ней и, соответственно, зон ответственности.

Предлагается алгоритм нумерации вершин графа бизнес-процесса в рамках последовательного заполнения зон ответственности (дорожек):

1. Исследователь определяет удобный для себя способ расположения зон ответственности на процессной диаграмме и определяет последовательность заполнения «дорожек».

2. В каждой «дорожке» вершины нумеруются следующим образом:

2.1 в случае ветвления процесса вершины, расположенные горизонтально на одном уровне при вертикальном расположении «дорожек», нумеруются последовательно слева направо, в случае горизонтального расположения «дорожек» – нумеруются последовательно по выбору исследователя снизу вверх (или сверху вниз),

2.2 при отсутствии ветвлений (или объединения в один поток) вершины нумеруются последовательно.

Разработанный алгоритм нумерации вершин исключает сомнения исследователя и обеспечивает сортировку по ролям в строках и, соответственно, столбцах матрицы смежности. Произвольный выбор последовательности ролей для нумерации вершин не влияет на наглядность определения сервисов при предлагаемом способе нумерации вершин графа бизнес-процесса, т. к. обеспечивается сортировка и расположение действий по ролям (зонам ответственности).

Предлагаемый алгоритм нумерации вершин применён к упрощённому бизнес-процессу «Обслуживание авиапассажира после полёта» (рис. 1). Бизнес-процесс описан с точки зрения пассажира на уровне взаимодействия служб аэропорта от момента прибытия на аэровокзал до прохождения таможенного контроля.

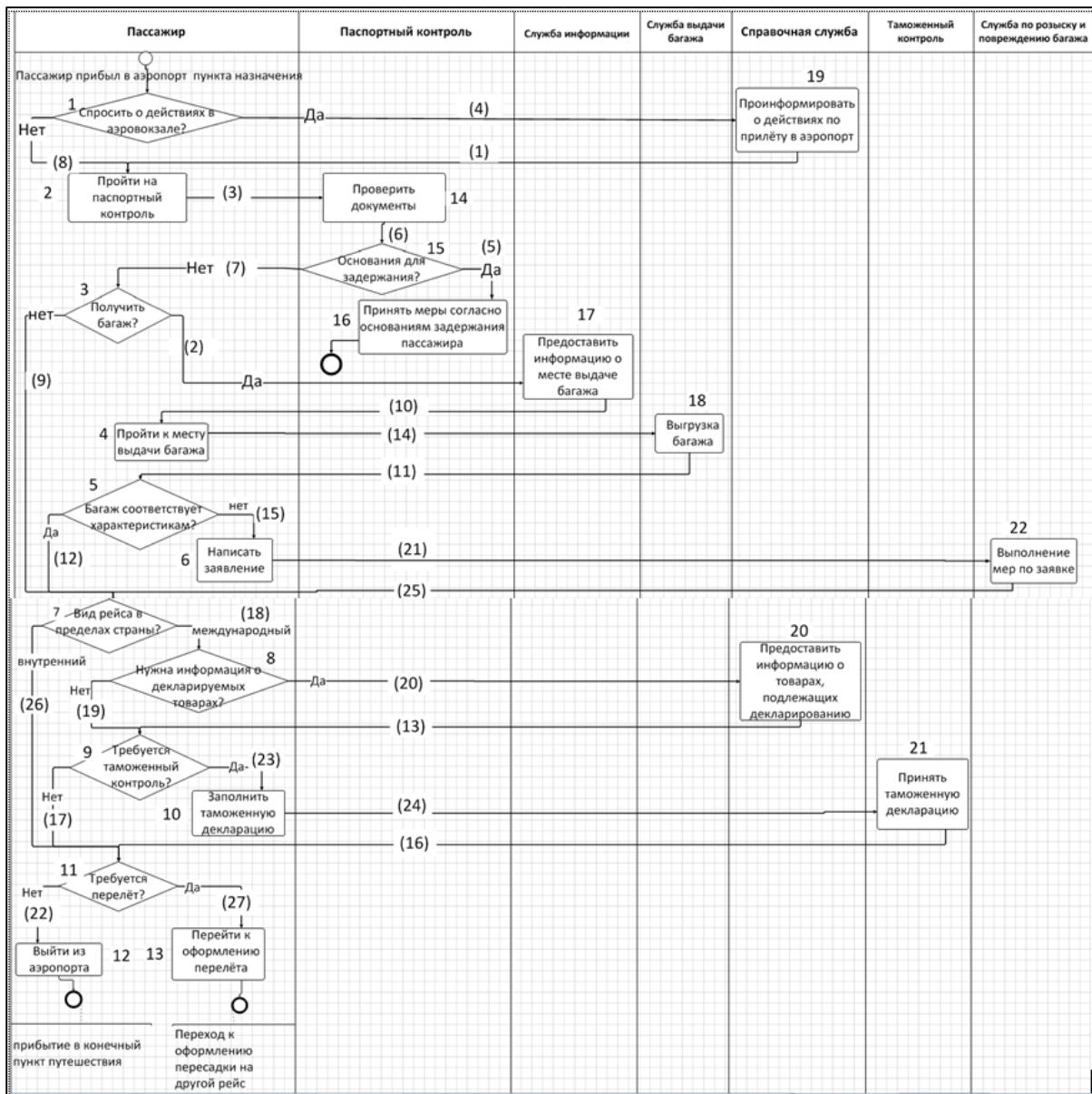


Рис. 1. Бизнес-процесс «Обслуживание авиапассажира после полёта»

Матрица смежности для рассматриваемого процессного графа приведена на рисунке 2. Если значение элемента матрицы смежности равно 1 и расположено на пересечении строки и столбца, принадлежащим разным ролям, то следует составить и проанализировать цепочку вершин, связанных и расположенных до и после, рассматриваемых вершин для выявления ролей исполнителя и заказчика сервиса. Смысловое содержание действий определяет название сервиса. В таблице 1 показаны выявленные на основе анализа последовательности вершин в матрице смежности (действий), образующие сервисы (в скобках указан возврат от номера столбца к аналогичному номеру строки). В выявленных сервисах рассматриваемого бизнес-процесса вершины начала и окончания принадлежат роли («дорожке») – пассажир, т. е. он является заказчиком сервисов.

Рис. 2. Матрица смежности бизнес-процесса (рис. 1)

ТАБЛИЦА 1. Сервисы, выявленные на основе анализа матрицы смежности (рис. 2)

Цепочка вершин	Название сервиса	Исполнитель
1-19-(19)-2	Информирование о действиях в аэровокзале после посадки самолёта	справочная служба
2-14-(14)-15-(15)-3	Проверка документов авиапассажира	паспортный контроль
3-17-(17)-4	Информирование о месте выдачи багажа	служба информации
4-18-(18)-5	Доставка багажа в аэровокзал	служба выдачи багажа
6-22-(22)-7	Принятие мер при получении заявления о несоответствующем состоянии багажа авиапассажира	служба по розыску и повреждению багажа
8-20-(20)-9	Информирование о товарах, подлежащих декларированию	справочная служба
10-21-(21)-11	Декларирование товаров	таможенный контроль

*Применение матрицы инцидентности для выявления сервисов.*

Вершина является началом ребра, если значение равно «-1», окончанием – «1». Столбец показывает связь между вершинами и может иметь только два ненулевых значения (ребро соединяет две вершины). Алгоритм нумерации рёбер и вершин не влияет на удобство определения сервисов при анализе матрицы инцидентности. На рисунке 1 для рассматриваемого графа бизнес-процесса приведена нумерация рёбер в произвольном порядке. Матрица инцидентности для такого графа бизнес-процесса приведена на [рисунке 3](#). Принадлежность ненулевых элементов столбца разным участникам бизнес-процесса и анализ последующих элементов относительно «-1» и предыдущих относительно «1» позволяет выявить действия, совокупность которых образует сервис. Например, ребро 14 содержит ненулевые элементы, относящиеся к разным участникам бизнес-процесса. Последовательность вершин 4-18-5 образует сервис, исполнитель которого – служба выдачи багажа, а заказчиком выступает пассажир. Предыдущей к вершине 4 является вершина 17 (служба информации), за вершиной 5 следуют вершины 6 или/и 7, т. е. действия пассажира, что требует уточнения типа решения.

Матрица инцидентности		ребра																											
роль	тип действия	вершины	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
пассажир	решение	1	0	0	0	-1	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
пассажир	задача	2	1	0	-1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
пассажир	решение	3	0	-1	0	0	0	0	1	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
пассажир	задача	4	0	0	0	0	0	0	0	0	1	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0
пассажир	решение	5	0	0	0	0	0	0	0	0	0	1	-1	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0
пассажир	задача	6	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	-1	0	0	0	0	0	0	0	0
пассажир	решение	7	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	-1	0	0	0	0	0	0	0	1	-1	0
пассажир	решение	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	-1	-1	0	0	0	0	0	0	0	0
пассажир	решение	9	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	-1	0	1	0	0	0	-1	0	0	0	0
пассажир	задача	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	-1	0	0	0
пассажир	решение	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	-1	0	0	0	0	1	-1	0
пассажир	задача	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
пассажир	задача	13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
паспортный контроль	задача	14	0	0	1	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
паспортный контроль	решение	15	0	0	0	0	-1	1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
паспортный контроль	задача	16	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
служба информации	задача	17	0	1	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
служба выдачи багажа	задача	18	0	0	0	0	0	0	0	0	0	-1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
справочная служба	задача	19	-1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
справочная служба	задача	20	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	1	0	0	0	0	0	0
таможенный контроль	задача	21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	1	0	0	0	0
служба по розыску и повреждению багажа	задача	22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	-1	0	0

Рис. 3. Матрица инцидентности бизнес-процесса ([рис. 1](#))

Анализ матрицы смежности и инцидентности с точки зрения чередования действий участников сервиса позволяет выявить:

- использование символа нотации описания бизнес-процесса не по назначению (например, обозначение в виде задачи «ожидание результата»);
- несоблюдение уровня детализации бизнес-процесса (например, переход от уровня подразделений на уровень функций на местах).

Таким образом, в статье предложены два варианта методики, которые позволяют при выполнении ряда несложных формальных действий получить перечень сервисов, обеспечивающий выполнение действий, определённых бизнес-процессом. Достоинствами предлагаемых методик является формирование математической модели деятельности в границах бизнес-процесса и возможность обнаружения ошибки в графическом описании бизнес-процессов при выявлении сервисов. Внимание на тип действия, инициирующего сервис, позволяет выделить в наборе сервисов две группы – постоянные и предоставляемые по требованию. Сервисы «по требованию» становятся объектом анализа с точки зрения целесообразности реализации. Перспективным представляется исследование внутренней структуры сервиса на основе объектно-ориентированной модели, что позволит автоматизировать предложенные процедуры.

#### **Список используемых источников**

1. The State of Business Process Management – 2014 [Электронный ресурс] / P. Harmon, C. Wolf // BPTrends. – 2014. – С. 54. – Режим доступа: <http://www.bptrends.com/bptrends-surveys> (Дата обращения: 19.04.2014).
2. Сервис-ориентированная модель описания информационно-функциональных взаимодействий предприятия [Электронный ресурс] / М. Ю. Арзуманян, А. Д. Сотников // Проблемы современной экономики. – 2009. – № 2 (30). – Режим доступа: <http://www.m-economy.ru/art.php?nArtId=2625> (Дата обращения: 15.03.2014).

*Статья представлена научным руководителем,  
д-ром техн. наук, профессором А. Д. Сотниковым*

УДК 338.47

**У. В. Мальцева (аспирант кафедры УЭС СПбГУТ)**

## **МЕТОДИКА ФОРМИРОВАНИЯ МНОГОМЕРНЫХ ЭТАЛОННЫХ ОПИСАНИЙ ПРЕДПРИЯТИЙ СВЯЗИ**

Каждая отрасль состоит из множества различных предприятий. Чтобы узнать растет предприятие или стагнирует, часто для анализа используют методы прогнозирования. Однако, они учитывают только внутренние характеристики предприятия. Но инвесторам и руководителям необходимо отслеживать изменения, всего разнообразия мира. Для исследования этого вопроса предлагается методика многомерных эталонных описаний.

Если у исследователей имеется множество различных факторов и их нужно объединить и проанализировать появляется необходимость в методах анализа. Для этого действия будет использован метод, который носит название «кластерный анализ», только он дает возможность разделения множества данных на обособленные группы по выбранному признаку.

Кластер-анализ – это способ группировки многомерных объектов, основанный на представлении результатов отдельных наблюдений точками подходящего геометрического пространства с последующим выделением групп как «сгустков» этих точек. Собственно, «кластер» (cluster) в английском языке и означает «сгусток», «гроздь (винограда)», «скопление (звезд)» и т. п. [1].

Одним из методов кластерного анализа, носит название алгоритм Форель, который позволяет решать задачу кластеризации заданной выборки векторных признаковых описаний объектов с помощью следующей схемы. Фиксируется положительное число некоторой метрики в пространстве признаковых описаний и произвольный этalon обучающей выборки. Определяется подмножество векторов, принадлежащих сфере с центром в заданном эталоне, и вычисляется средний вектор по данному множеству векторов. Данный средний вектор принимается за центр новой сферы. Найденные в итоге число кластеров (и сами кластеры) будут зависеть от выбора метрики, начальных эталонов, радиусов сфер [2].

Отмеченная на графике точка может содержать различную информацию. С помощью этого алгоритма будет проанализирована группа предприятий по определенному признаку.

Первым этапом является подготовка к анализу. Он состоит в необходимости выделения группы для анализа [3]. Например, предприятия отрасли связи гражданского назначения. Выбираются в идеале все предприятия. Направленность – радионавигация и радиосредства. Примерный список предприятий представлен в таблице 1.

ТАБЛИЦА 1. Близкие по параметрам предприятия

Электросигнал	Ангстрем	Электросигнал Дербент
ЧРД	Радиосвязь	КРЗ
ЯРД	Егорш. рдз	Супертел
Рязанский радиозавод	Иж. рдз.	

Второй этап – выделение необходимых характеристик. На основании изучения литературы [4, 5], можно выделить несколько характеристик, которые и будут анализироваться:

- среднесписочное количество работников, чел.;
- выручка от продажи товаров, продукции, работ, услуг, тыс. руб.;
- себестоимость продаж, тыс. руб.;
- объем проданной продукции, тыс. руб.;
- кредиторская задолженность на конец года, тыс. руб.;
- дебиторская задолженность на конец года, тыс. руб.;
- объем произведенной продукции, тыс. руб.;
- запасы, тыс. руб.

Третьим этапом будет являться анализ выбранных предприятий и характеристик. Последовательный анализ критерий даёт наглядно понять, как изменяются данные по каждому предприятию в рамках отдельной характеристики. На основании вариативного ряда, присваивается номер предприятию относительно характеристики.

ТАБЛИЦА 2. Присвоение вариативного номера  
для каждой выбранной характеристики

Обозначение предприятий	Среднесписочное количество работников
11	2035,00
10	1973,00
9	1862,00
8	1660,00
7	1658,00
6	1500,00
5	800,00
4	683,00
3	410,00
2	180,00
1	100,00

Четвертый этап – использование алгоритма Форель. На рисунке 2, представлены данные из таблице 2, ось х – номер предприятия, по ось у – значение характеристики.

На рисунке 2 так же, отмечены области с применением алгоритма. Каждая сфера объединила группу предприятий. Из него видно, что есть кластеры, которые находятся в верхнем правом углу и в нижнем левом. Самый верхний кластер предприятий, для данного критерия, назовем «предкризисные», вторую – «перспективные».

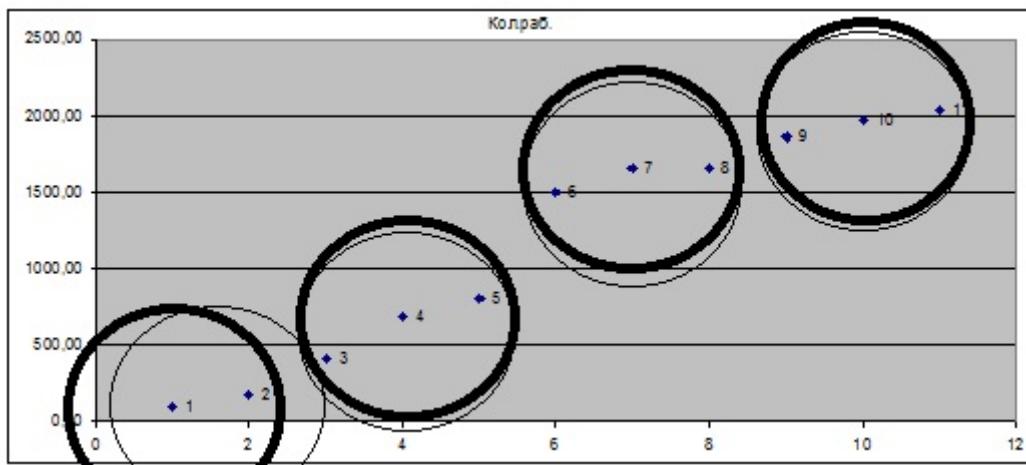


Рис. 2. Графическое представление результата использования алгоритма

Получив среднее значение в каждом кластере, и отметив новый центр, получаем среднее значение.

ТАБЛИЦА 3. Список предприятий и соответствующее среднее значение среднесписочного количества работников

Обозначение предприятий	Среднесписочное количество работников	Среднее значение
11	2035,00	1956,67
10	1973,00	
9	1862,00	
8	1660,00	1606,00
7	1658,00	
6	1500,00	
5	800,00	631,00
4	683,00	
3	410,00	
2	180,00	140,00
1	100,00	

Теперь можно записать частный критерий и на основе его, можно будет понять, относится ли предприятие к «перспективным» или к «неперспективным». Среднесписочное количество рабочих:

$$\Pi > 2000$$

$$H < 140$$

где  $\Pi$  – эталонное значение перспективные;  
 $H$  – эталонное значение неперспективные.

Данный критерий дает возможность анализировать другие предприятия. Например, можно сказать, что предприятие, имеющее работников меньше ста сорока, может находиться в предкризисном состоянии. А предприятие, имеющее более двух тысяч человек – перспективное. Однако стоит учитывать, что использование только одного критерия или неполного списка предприятий отрасли резко снижает объективность метода анализа.

Обработав, таким образом, все критерии получим обособленные группы предприятий. Сформированные многомерные эталоны помогут принять оптимальное решение, и показать в какую сторону двигается предприятие – в сторону обозначенную как «перспективные» или «предкризисные».

#### **Список используемых источников**

1. Кластерный анализ / И. Д. Мандель. – М. : Финансы и статистика, 1988. – 176 с.
2. Методы построения коллективных решений задачи кластерного анализа : дис. ... канд. физ.-мат. наук: 05.13.17 / Бирюков А. С. – Москва, 2005. – 100 с.
3. Предприятия отрасли связи в рыночной экономике / У. В. Мальцева // 67-я научно-техническая конференция студентов, аспирантов и молодых специалистов. 28–29 мая 2013 года : материалы. – СПб. : Издательство СПбГУТ, 2013.
4. Экономический анализ / В. Г. Когденко. – 2-е изд., перераб. и доп. – М. : 2011. – 399 с.
5. Интеллектуальный капитал. Материализация интеллектуальных ресурсов в глобальной экономике : монография / В. В. Макаров, М. В. Семёнова, А. С. Ястребов; под ред. В. В. Макарова. – СПб. : Политехника, 2012. – 688 с.

*Статья представлена научным руководителем,  
д-ром экон. наук, профессором В. В. Макаровым.*

## ГУМАНИТАРНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

**УДК 654.739**

**О. Н. Агеев (студент группы ИКТ-303 СПбГУТ)**

### **АКТУАЛЬНЫЕ ФИЛОСОФСКИЕ ПРОБЛЕМЫ СОВРЕМЕННОСТИ**

#### *Проблема Сущности Человека*

Раскрытие сущности входит в само определение любого предмета и без этого вообще невозможно вести разговор о его значении.

В истории развития науки рассматривали отличие человека от животного и объясняли его сущность, используя различные специфические качества человека. Действительно, человека можно отличать от животного: обладает мышлением и членораздельной речью, способен к сознательной целенаправленной творческой деятельности, а также отличие во внешнем виде.

Во всех этих случаях сущность человека определяется не из его самого, а как бы со стороны. С методологической точки зрения такой подход не совсем правомерен. Ибо сущность любого предмета определяется прежде всего внутренними законами его существования, субстанцией, выражющей его качество.

Такой субстанцией, составляющей сущность человека, как свидетельствует современная наука, является его трудовая деятельность. Человек занимается трудовой деятельностью, вступая прямо или опосредованно в общественные отношения, совокупность которых и образует общество. В процессе общественного производства и трудовой деятельности развиваются и общественные отношения людей. В той степени, в какой индивид реализует совокупность общественных отношений, происходит и его собственное развитие.

Человек – не только плод развития общества и общественных отношений, но он и сам творит их. Следовательно, человек и объект и субъект данных отношений.

Мы можем говорить о социально-деятельностной сущности человека, потому что вне социальных отношений и общения, человек не может стать человеком.

Аристотель в свое время отметил, что существо, неспособное вступать в общение или животное, или Бог.

На этой основе возникает и такая сущностная характеристика человека как разум (по Аристотелю – УМ), которая является в высшей степени человеческим свойством [1, 2].

### *Проблема смысла и цели жизни*

Дать логически обоснованный ответ об абсолютном смысле жизни человека невозможно. Дать абсолютный ответ – значит исчерпать саму жизнь, которая беспредельна в своем существовании и не исчерпывается рациональным объяснением.

Применительно к жизни отдельной личности данный вопрос имеет реальный смысл и значение. Если бы каждый не отвечал для самого себя на этот вопрос, то само существование человека было бы бессмысленным. Много глубокого смысла и мудрости содержат слова Ницше: « тот, кто имеет ЗАЧЕМ жить, может вынести любое КАК».

Если говорить про этот реальный, а не абсолютный смысл жизни, мы полагаем, что в общем плане можно сказать: смысл жизни состоит в развитии человека как самоцели, его всестороннем совершенствовании. Как писал Кант, существование человека «имеет в себе самом высшую цель, которой, насколько это в его силах, он может подчинить всю природу». Определить личностный смысл жизни – это значит осмыслить жизнь во всей ее сути и в большом плане; это значит объяснить, что в ней подлинное, а что – мнимое, определить не только основные задачи и цели жизни, но и реальные средства их осуществления.

Ценностную основу смысла жизни составляет «жизненно важная, эмоционально приемлемая цель, которая не только объективно целесообразна, но и субъективно утверждена, лично приемлема и признана в качестве таковой... Обретение смысла жизни предполагает свободное целеполагание индивида, поэтому его необходимым условием является свобода как человеческая форма самообусловливания бытия.

В истории социально-философской мысли, в зависимости от того, какие цели ставит перед собой человек, выделялись две различные установки в обретении индивидом смысла жизни: «быть» или «иметь»

Смысложизненная установка «иметь» уходит своими корнями в далёкое прошлое человечества, где данное требование было необходимым условием выживания человеческого рода. Присутствие данной установки является нормальным состоянием души и современного человека, так как жизнь требует обладания некоторыми вещами. Но в то же время установка «иметь» не должна стать самоцелью, обладание некоторыми вещами, объектами, предметами должно служить лишь средством достижения смысложизненных задач.

Установка «быть» означает реализацию более высокой программы, отвечающей духовным потребностям человека, его истинной сущности. По учению М. Экхарта: «... ничем не обладать и сделать свое существо открытым и «незаполненным», не позволить «я» встать на своем пути – есть условие обретения духовного богатства и духовной силы. По Марксу, роскошь – это такой же порок, как и нищета, цель человека – быть многим, а не обладать многим».

Смысложизненная программа «быть» предполагает отказ от эгоизма и эгоцентризма, активизацию и продуктивную реализацию природных данных человека, духовный рост, выход за рамки своего изолированного «я», стремление к «человеческому» в человеке – Добру, Истине, Красоте, Справедливости.

Ко всему сказанному следует добавить, что поскольку человек в своей сути существо общественное, поэтому и смысл его жизни может быть найден только на пути сопряжения интересов и целей общества и личности. Общность индивида и рода, личности и социума дает основание оптимистически смотреть на бытие человека в мире и смысл его жизни. Трагизм индивидуальной смерти преодолевается тем, что человек и после смерти остается в результатах своей деятельности, своего творчества в благородной памяти потомков [1, 3].

### *Сознание как философская проблема*

Проблема сознания всегда привлекала внимание философов, ибо определение места и роли человека в мире, специфики его взаимоотношений с окружающей его действительностью предполагает выяснение природы человеческого сознания. Для философии эта проблема важна и потому, что те или иные подходы к вопросу о сущности сознания, о характере его отношения к бытию затрагивают исходные мировоззренческие и методологические установки любого философского направления. Подходы бывают разные, но все они по существу имеют дело с единой проблемой. Анализом сознания как специфически человеческой формы регуляции и управления взаимодействием человека с действительностью.

Разрабатываемые сознанием идеальные планы деятельности, его программы и проекты предшествуют деятельности, но их осуществление обнажает новые слои реальности, открывает новую фактуру бытия, которая выходит за пределы исходных установок сознания. В этом смысле бытие человека постоянно выходит за пределы сознания как идеального плана, программы действия, оказывается богаче содержания исходных представлений сознания. Вместе с тем это расширение «бытийного горизонта» осуществляется в деятельности, стимулируемой и направляемой сознанием. Человек сознает при помощи мозга, но сознание – не функция мозга самого по себе, а функция определенного, специфического типа взаимоотношения общественно развитого человека с миром. возникает и развива-

ется в совместной деятельности людей, в процессе их труда и общения. Вовлекаясь в эти процессы, люди вырабатывают соответствующие представления, установки, нормы, которые вместе с их эмоциональной окраской составляют содержание сознания как специфической формы отражения. Это содержание и закрепляется в их индивидуальной психике.

С сознанием в широком смысле слова, конечно, следует связывать и представление о самосознании. Самосознание – это сознание человеком своих действий, чувств, мыслей, мотивов поведения, интересов, своего положения в обществе. В формировании самосознания существенную роль играют ощущения человеком своего собственного тела, движений, действий. Человек может стать самим собой лишь во взаимодействии с другими людьми, с миром через свою практическую деятельность, общение.

Сознание выступает, таким образом, как ключевое, исходное философское понятие для анализа всех форм проявления духовной и душевной жизни человека в их единстве и целостности, а также способов контроля и регуляции его взаимоотношений с действительностью, управления этими взаимоотношениями.

Сознание – это выевшая, свойственная только людям и связанная с речью функция мозга, заключающаяся в обобщенном и целенаправленном отражении действительности, в предварительном мысленном построении действий и предвидении их результатов, в разумном регулировании и самоконтроле поведения человека [1].

### *Проблема свободы человека*

Свобода – это специфический способ бытия человека, связанный с его способностью выбирать решение и совершать поступок в соответствии со своими целями (в рамках существующей необходимости). Абсолютной, безграничной свободы быть не может ни в физическом, ни в социальном аспекте существования человека. Полная свобода одного означала бы произвол в отношении другого.

Соотношение категорий свободы и необходимости можно рассмотреть посредством анализа работ Гегеля. Все в мире подчинено силам, действующим непреложно, неотвратимо. Эти силы подчиняют себе и деятельность человека. Если эта необходимость не осмысlena, не осознана человеком – он ее раб, если же она познана, то человек обретает «способность принимать решение со знанием дела». В этом выражается свобода воли человека.

Но какова природа «необходимости»? Необходимость, считает ряд философов, существует в природе и обществе в виде объективных, т. е. независимых от сознания человека, законов. Иначе говоря, необходимость есть выражение закономерного, объективно обусловленного хода развития событий. Сторонники этой позиции не считают, что все в мире, особенно в общественной жизни, жестко и однозначно определено, они не отрицают

наличие случайностей. Но общая закономерная линия развития, отклоняемая случайностями в ту или другую сторону, все равно пробует себе дорогу.

Ответственность – саморегулятор деятельности личности, показатель социальной и нравственной зрелости личности. Ответственность предполагает наличие у человека чувства долга и совести, умения осуществлять самоконтроль и самоуправление. Совесть выступает как контролер всех действий человека. Сделанный человеком выбор, принятое решение означают, что человек готов взять на себя всю полноту ответственности и даже за то, что он не смог предусмотреть. Неизбежность риска сделать "не то" или "не так", предполагает наличие у человека мужества, необходимого на всех этапах его деятельности: и при принятии решения, и в процессе его реализации, и, особенно в случае неудачи. Таким образом, свобода связана не только с необходимостью и ответственностью, но и с умением человека сделать правильный выбор, с его мужеством и с рядом других факторов [4].

#### **Список используемых источников**

1. **Философия:** учебн. для вузов / В. В. Миронов. – М. : Норма, 2005. – 928 с.
2. **Маркс К., Энгельс Ф.** Соч. Т. 42. – М. : Государственное издательство политической литературы, 1955–1981. – 530 с.
3. **В мире** причин и следствий. Смысл жизни: диалог мировоззрений. – М. : Знание, 1991. – 64 с.
4. **Экзистенция** как свобода / Н. Аббаньяно // Вопросы философии. – 1992. № 8. – 145–157 с.

*Статья представлена научным руководителем,  
канд. филос. наук, доцентом М. Р. Зобовой.*

**УДК 654.739**

**Д. Д. Алексеева (студентка группы ИКТ-307 СПбГУТ)**

#### **ЗОЛОТОЕ СЕЧЕНИЕ**

Что же такое «золотое сечение»? Золотое сечение – гармоническая пропорция, равенство двух отношений: всей длины какого – либо отрезка к большей его части, и большей части к меньшей.

Например, возьмем отрезок  $AB$ . На отрезке поставим точку  $C$ , при том, что  $AC$  будет больше  $CB$ . Если  $AB:AC = AC:CB$ , то точка  $C$  делит данный отрезок в «золотой» пропорции. Приблизительная величина золотого

сечения равна  $1,6180339887$  ( $1/\tau$ ). В процентном окружённом значении — это деление величины на 62 % и 38 % соответственно [1].

Интерес к золотому сечению в разное время то проявлялся, то угасал. Золотое сечение, (как её назвал Леонардо да Винчи, или божественная пропорция, золотое деление и другие названия в разных источниках), было известно еще в древнем Египте. И действительно, пропорции пирамиды Хеопса, храмов, барельефов, предметов быта и украшений из гробницы Тутанхамона свидетельствуют, что египетские мастера пользовались соотношениями золотого деления при их создании [2].

Божественные пропорции также присутствуют и в греческой архитектуре. Например, в фасаде древнегреческого храма Парфенона. В дошедшей до нас античной литературе золотое деление впервые упоминается в «Началах» Евклида. После Евклида исследованием золотого деления занимались Гипсикл (II в. до н.э.), Папп (III в. н.э.) и др.

В эпоху Возрождения золотое сечение вновь заинтересовало великие умы. В 1509 г. в Венеции была издана книга Луки Пачоли «Божественная пропорция» с блестяще выполненными иллюстрациями. Среди многих достоинств золотой пропорции монах Лука Пачоли не преминул назвать и ее «божественную суть» как выражение божественного единства бог сын, бог отец и бог дух святой.

Леонардо да Винчи также много внимания уделял изучению золотого деления. Он производил сечения стереометрического тела, образованного правильными пятиугольниками, и каждый раз получал прямоугольники с отношениями сторон в золотом делении. Именно он придумал называть божественную пропорцию золотым сечением. Так оно и держится до сих пор как самое популярное. Яркий пример работы Леонардо, а также золотого сечения в живописи, портрет Монны Лизы.

Отдали дань золотому сечению также композиторы и поэты. Известно, например, что в произведениях выдающегося австрийского композитора, представителя венской классической школы, Иозефа Гайдна, существует золотое сечение. Анализ стихотворений А.С. Пушкина показал, что поэт явно предпочитает количество строф в 5, 8, 13, 21 и 34 строк (числа Фибоначчи). Раковина улитки, подсолнух — во всем присутствует божественная пропорция [3].

Что же представляет собой «золотая пропорция» с позиций философской науки? Это некое отношение между какими-либо противоположными свойствами какого-либо объекта.

Напомним, что противоположности — две стороны одного и того предмета или явления, которые находятся постоянно в противоречии друг с другом из-за своей абсолютной полярности. Две противоположности образуют противоречие. Противоположности не могут существовать друг без друга по отдельности. Они существуют вместе, но только в рамках противоречия. Разве может добро существовать отдельно от зла? Ведь добрый

человек не может быть добрым, если нет злого, иначе кто же узнает, каким должен быть добрый.

Накопленные человечеством знания говорят о том, что и в природе, и в человеческом обществе бывают устойчивые образования, которые не изменяются, как с точки зрения пространственной, так и с временной, хотя и в этих образованьях идут количественные изменения.

На любую форму, либо динамический процесс, можно наложить числовые ряды золотого сечения для установления правильных гармоничных пропорций. Любое искажение – это негармоничные пропорции, или диспропорции. Если система находится в положении устойчивого динамического равновесия, то взаимосопряженные элементы такой системы должны находятся в отношениях золотого сечения. Нарушить эти пропорции – система придёт в движение и начинает перебирать возможные комбинации своих элементов до тех пор, пока не установится другое равновесное состояние.

Числовые ряды золотого сечения, таким образом, могут служить своеобразной матрицей гармоничного состояния, к которому должна стремиться любая система в своём движении и развитии.

Красота должна быть во всем. Человек, как творение природы, тоже входит в число обладателей золотой пропорции. В 1509 году в Германии Альбрехт Дюрер подробно разрабатывает теорию пропорций человеческого тела. Важное место в своей теории исследователь отводил золотому сечению.

В 1855 г. немецкий исследователь золотого сечения профессор Цейзинг опубликовал свой труд «Эстетические исследования». Он измерил около двух тысяч человеческих тел и пришел к выводу, что золотое сечение выражает средний статистический закон [4].

Подобно Цейзингу, мы решили измерить пару десятков человек в нашем университете и посмотреть, какое количество из них имеет золотые пропорции в лице. Мы измерили расстояние от подбородка до кончика носа и от подбородка до конца лба и выяснили, что у 40 % испытуемых существует золотая пропорция. Если вспомнить, что золотое сечение делит величину в пропорциях 62 % и 38 %, то можно утверждать, что проделанный нами опыт также доказывает справедливость теории золотого деления. Студенты с золотым сечением в лице и без него тоже находятся в правильном соотношении, или в гармонии.

Закономерности «золотой» симметрии проявляются в энергетических переходах элементарных частиц, в строении некоторых химических соединений, в планетарных и космических системах, в генных структурах живых организмов. Эти закономерности есть в строении отдельных органов человека и тела в целом, а также проявляются в биоритмах и функционировании головного мозга и зрительного восприятия. Золотое сечение определяет красоту, гармонию. Оно везде, к этому надо стремиться. Прин-

цип золотого сечения – высшее проявление структурного и функционального совершенства целого и его частей в искусстве, науке, технике и природе.

#### **Список используемых источников**

1. **Золотое сечение** / А. Д. Бендукидзе // Квант. –1973. – № 8.
2. «**Золотое сечение**» в архитектуре [Электронный ресурс] / С. А. Волков. – Режим доступа: [http://culture-people.com/index.php?option=com\\_content&task=view&id=131](http://culture-people.com/index.php?option=com_content&task=view&id=131) (Дата обращения 21.05.2014).
3. **Тайны золотого сечения** / А. Соколов // Техника – молодежи. – 1978. – № 5. – С. 41–42.
4. **Золотая пропорция** [Электронный ресурс] / Б. Б. Косенок. – Режим доступа: [http://borkos.narod.ru/Page\\_Gold\\_mid.htm](http://borkos.narod.ru/Page_Gold_mid.htm) (Дата обращения 21.05.2014).

*Статья представлена научным руководителем,  
канд. филос. наук, доцентом М. Р. Зобовой.*

**УДК 008:93**

**О. С. Барбир (студентка группы ЗР-32 СПбГУТ)**

#### **ДУХ БРИТАНСКИХ ЗАМКОВ В ЛИНГВОКУЛЬТУРОЛОГИЧЕСКОМ АСПЕКТЕ**

Данная работа посвящена описанию замков и их роли в истории и культуре Великобритании. На передний план будут выдвинуты основные черты замков, а так же особенности этих средневековых строений, которые подчёркивают уникальность и самобытность британской культуры. Кроме того, автор рассмотрит, насколько применим термин «дух» к архитектуре замков, и какой отпечаток на свое жилище оставляет его владелец.

В первую очередь, рассмотрим такой феномен, как «замок». В течение средних веков феодалы строили необычные укрепления, в которых можно было не только жить, но и успешно держать оборону, находить помощь. Очень часто вокруг укреплений после строились многочисленные дома, возводились стены. Со временем все это стали называть «Замком». Замки являлись одними из самых популярных построек не только в Средневековье, но и в последующее время. Сегодня насчитывается более 1000 замков только на территории современного Соединенного Королевства – в Англии, Уэльсе, Ирландии и Шотландии. Некоторые из них прекрасно сохранились, некоторые живы исключительно благодаря регулярным реконструкциям, а некоторые превратились в руины.

Хотя начало строительства замков в Великобритании в основном приходится на Нормандскую эпоху, первые замки, тем не менее, возникли накануне – в правление Эдуарда Исповедника, при дворе которого уже было много знати из Нормандии. Нормандские подданные возводили первые оборонительные укрепления на границе с Уэльсом для усмирения валлийцев. И если ранее крепости англо-саксонского происхождения возводились для защиты целых городов и поселений, то новый тип укрепления был личной защитой вассала.

Поэтому название таких укреплений *Castle*, которое восходит к латинскому *castellum* – пришло в английский язык уже как французское заимствование (*chastel*). Это относится также и к названиям отдельных частей замка: *motte* (мот, холм), *moat* (ров), *curtains* (куртины, стены), *donjon* (главная башня) и другие.

Следующие элементы свойственны практически любому замку, будь он в Великобритании, Франции, Германии или даже Японии [1, 2]:

– *Холм (motte, bailey)*. Это насыпной холм из земли, часто смешанной с гравием, торфом, известняком или хворостом.

– *Донжон*. Главная башня в европейских феодальных замках. В английском языке французское название *donjon* не прижилось, закрепился термин *keep* (хранить, держать). По одной из версий такое название возникло в силу того, что здесь содержались жилые покоя, часто здесь держали узников. Наряду с оборонительной функцией донжоны обычно выполняли функцию непосредственного жилища феодалов.

– *Крепостные стены (curtains)*. Это защитные стены вокруг внутреннего двора. Они должны были быть достаточно высокими, чтобы затруднить штурм.

– *Ров (moat)*. Как правило, рвы устраивались вокруг замков как часть оборонительной системы.

– *Городские ворота (gate)*. Их возводили, чтобы предоставить точку контролируемого входа и выхода людей, транспорта, товаров и животных из обнесенного стеной города.

Если мы присмотримся более внимательно к каждому замку, то обязательно увидим – каждый из них по-своему уникален. Если мы говорим конкретно о Соединенном Королевстве, то даже между отдельными его частями мы увидим некоторые принципиальные различия.

Обратимся к истории. Расцвет строительства замков начался после норманнского завоевания. Став хозяевами обширных владений в чужой стране, они поспешили утвердить свою власть. Исторические условия сформировали своеобразный, чисто английский тип замка – в Англии сложилась такая ситуация, что даже поместье небогатого рыцаря рассчитано было на серьёзную оборону.

Центром замков был огромный кубический донжон, часто с угловыми башнями. Вокруг него располагались хозяйственные постройки и допол-

нительные здания, которые росли с каждым годом. В XII-XIII веках крестоносцы привезли из Святой Земли новые веяния: круглые башни и концентрические крепости. В конце XIV века в Англии было построено несколько весьма специфических, т. н. «жилых» замков, например Бодиам и Болтон. Не меньше труда было положено на то, чтобы создать внутри большие и комфортабельные помещения для жизни. Идея концентрической крепости была привезена из Палестины.

Совсем другой была ситуация на кельтских территориях. Шотландский (кельтский) замок представляет совершенно другой тип крепости, чем в Англии. Всего несколько замков в Шотландии построены в норманнском стиле. Все остальные спроектированы иначе. Шотландский замок рассчитан не на долгую осаду, а на противостояние набегу соседей.

В Уэльсе с конца XI века началось строительство замков, собственниками которых были т. н. Лорды Границы, превратившие свою разовую победу над валлийцами в долговременное господство. В течение нескольких лет все владения Лордов Границы были укреплены дугой замков норманнского типа: от Честера на севере до Чепстоу на юге и на запад до Пембрука.

Замки активно строились в Англии с XI-го по XV век, особенно много их появилось в период с 1090 по 1200 года. Возникло также понятие *Castle mentality* (замковая ментальность), характерное для этого периода. Основное идея его является уверенность в том, что война может быть выиграна на пороге собственного дома.

Далее происходят серьезные исторические изменения. Война постепенно становится уделом короля и его многочисленного войска. В конце XV-го века, когда в стране установился относительный мир после Войны Роз, мелкие лорды перестали нуждаться в неприступных крепостях. Так появился тип «укреплённого манора». Такие поместья всё еще окружались стенами, но башни (если они были) играли уже декоративную роль, окна были широкими, а интерьеры содержали много дерева. Такие укрепления давали защиту от случайного набега или крестьянского бунта, которые и были самыми вероятными напастями в то время. Ко времени правления Генриха VIII элемент укреплённости полностью исчез из архитектуры и в таких дворцах, как Хэмптон-корт, Хэт菲尔д или Пэнхерст он присутствует только в виде стилизации.

Такие замки принято называть *doubtful castles* (не собственно замки). Впоследствии возник т. н. замковый стиль в британской архитектуре, когда использовались отдельные черты замков в целях украшения жилища, придания ему статуса богатого имения, подчеркивался социальный статус владельца. Так закрепился термин *The Country-house castle* (замок-поместье).

А в XVIII веке возникло понятие *picturesque ruins* (живописные руины), связанное с романтическими ассоциациями со славным прошлым. Ча-

сто землевладельцы сооружали такие руины в своем имении для придания ему изящного, романтичного вида.

Вы никогда не найдете двух абсолютно одинаковых замков. Как сказано ранее, это непосредственно связано с владельцами и жильцами этих строений. Каждый из них пытался обустроить свой дом по своему вкусу и согласно определенным целям. В течение долгого времени что-то изменялось, что-то достраивалось. Люди давно умерли, а их след в замках жив, и оживляет бездушный холодный камень. В данном ключе, можно рассматривать особую индивидуальность, неповторимость замков, обусловленную соединением разных эпох, культур, историй.

Хотелось бы привести два примера замков, демонстрирующих данное утверждение. Эти замки располагаются на одной территории, и, казалось бы, должны во многом походить друг на друга. Но это не так.

Замок *Castle Coch* или *The Red Castle*, что в переводе означает *Красный замок* своё название получил из-за оттенка камня, из которого построен. В XIX веке замок был реконструирован, воссоздан из руин предыдущего. Наверно, именно поэтому каждый гость замка приходит в недоумение – за неотесанными, грубыми стенами, скрывается хрупкая, великолепная архитектура. Прежде всего, это многоуровневость, необычный красный цвет деревянной части замка, небольшие, но декорированные витражами окна, изящные элементы, украшающие внутренние постройки [3]. Если зайти внутрь, то становиться трудно представить, что находишься в замке. Каждая комната украшена разнообразными орнаментами, тщательно прорисованными. Каждый фрагмент стены выглядит, как часть большой картины. Поражают восхитительные потолки – в главном зале он стилизован под звездное небо, в комнате принцессы – это украшенные различным орнаментом плиты. Кроме того, в каждой комнате немало скульптур и декоративных изделий. Комнат не так много, но заходя в каждую из них, оказываешься, как будто, в другом мире. Дизайнером этого замка (и нескольких других в Уэльсе) выступил Уильям Бёрджес (William Burges). Год назад автор работы провел в этом небольшом здании почти день, и оттуда совершенно не хотелось уходить.

Замок Карфили (*Caerphilly Castle*) построен в XIII веке. Как отмечалось выше, он располагается весьма недалеко от «Красного замка». Несмотря на этот факт, они совершенно разные. Снаружи строение выглядит достаточно привлекательно, несмотря на полуразрушенные стены. Милый, утопающий в цветах город окружает строение и придает яркость пейзажу. Но стоит нам зайти внутрь, как первые впечатления исчезают. Человек видит, что от внутренних стен замка осталось не так уж и мало, каждая деталь строения напоминает о боевых действиях, разрушениях, которые пережил этот замок. Что касается интерьера, мы не можем найти много интересных деталей в нём – от всего великолепия остались голые стены, едва украшенные символикой бывших обывателей. Сами стены имеют грязно-

серый оттенок. В главном зале одиноко стоит камин, который, скорее всего, больше никогда не зажгут.

Сложно не принять тот факт, что каждый замок имеет свою индивидуальность и носит след прошедших времен. Каждый уникален по-своему.

Замки стали неотъемлемой частью Британской культуры. Несмотря на то, что для самих британцев это обыденность, другие видят их значимость и неизменно ассоциируют их с культурой Соединенного Королевства. Ведь огромное количество преданий, сказок, легенд, рассказов, мифов и книг непосредственно связано со средневековыми строениями.

Беря во внимание всё вышесказанное, можно уверенно подвести итог, что замки играют значительную роль в культуре Британии. Они также стали важной составляющей частью нашего представления об этой стране.

#### **Список использованных источников**

1. **Castles. A very peculiar history** / J. Morley. – GB. : Book House, 2013. – 191 p.
2. **Дух Британских замков** / М Кук; пер. с англ. – Режим доступа: <http://velizariy.kiev.ua/avallon/stronghold/england.htm> (Дата обращения 20.05.2014).
3. **Castle Coch** / D. McLees. – GB. : CADW, Welsh Assembly Government, 2010. – 50 p.

*Статья представлена научным руководителем,  
канд. филол. наук, доцентом М. И. Парамоновой.*

#### **УДК 008**

**М. А. Беккер (студентка группы ЗР-31 СПбГУТ)**

#### **СПЕЦИФИКА СОВРЕМЕННОГО РОССИЙСКОГО ТЕЛЕВЕЩАНИЯ**

Роль современного телевидения в России как производителя информационного продукта для основной массы населения страны стала особенно велика в силу отсутствия достойной конкуренции со стороны других средств массовой информации (СМИ) и культурно-развлекательной индустрии. Телевидение как СМИ, предоставляя свои услуги и товары, влияет на мировоззрение, на систему ценностей человека, оказывает воздействие на политику, экономику, культуру [1].

Появление телевидения существенно снизило популярность печатных изданий и книг. Сейчас же невозможно отрицать тот факт, что развитие новых технологий, в частности всемирной сети Интернет, способствует перераспределению медийного потребления человека [2]. Телевещание се-

годня является сложной системой, формирование и преобразование которой зависит от множества факторов.

Для выявления специфики современного российского телевещания следует обратиться к фактической стороне вопроса. В этой связи целесообразно проанализировать современное российское телевещание для того, чтобы выявить его специфические черты.

Автором работы были выбраны пять телеканалов: Первый, Россия 1, НТВ, СТС, Россия К. Критериями отбора выступили популярность каналов, их доступность и неограниченность какой-либо тематикой. Днями для подсчета статистики стали 5 апреля (суббота) и 6 апреля (воскресенье) 2014 года. Именно в выходные контент телеканалов наиболее разнообразен, поскольку ориентирован на привлечение наибольшего числа телезрителей [3].

Данные исследования представлены на рисунках 1–5.

Рисунок 1 отображает информацию о количестве минут за двое суток вещания на определенный тип программ: новости, телепередачи, кино, сериалы, документальное кино, авторские программы, программы для детей, концерты. Из диаграммы следует, что наиболее обширно в выходные на телевидении представлены такие типы программ, как телепередачи и кино. Телеканал Россия 1, примерно половину контента которого в будние дни составляют сериалы, в выходные полностью исключает их показ, заменяя сериалы кино. Показ информационные программы в будние дни занимает примерно столько же пространства вещательной сетки, сколько и в будние дни (исключение – СТС, который, будучи телеканалом развлекательным, информационные программы не производит, т. к. их производство вызвало бы необходимость привлечения к этой работе высококвалифицированного персонала и использования, соответствующей оргструктуры). Документальное кино и концерты в выходные наиболее представлены на телеканале Россия К, авторские программы – на телеканале Россия 1. Программы для детей в выходные дни занимают большую часть вещательной сетки канала СТС (685 минут, что составляет 11 ч. 25 мин.), в то же время отсутствуют среди контента других телеканалов (исключение – Первый, 25 мин.).

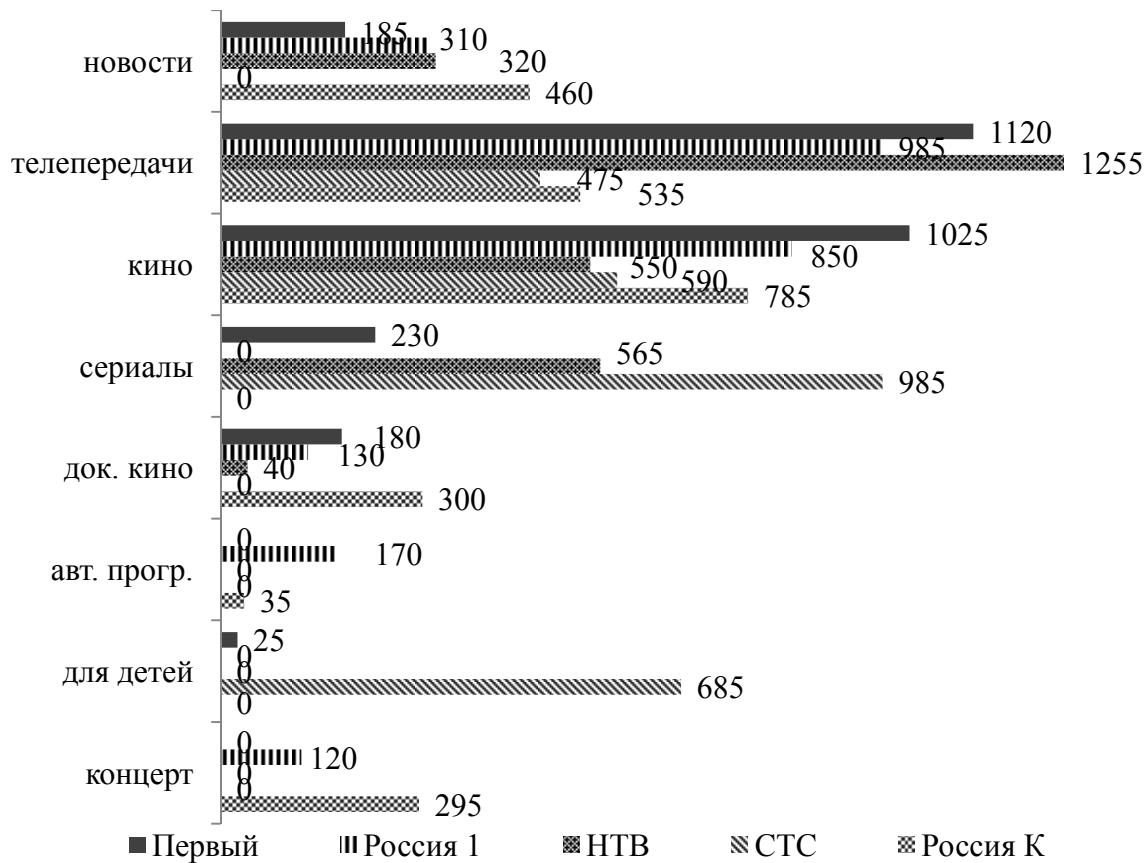


Рис. 1. Количество минут за двое суток вещания на определенный тип программ

Рисунок 2 содержит информацию о возрастных ограничениях за двое суток вещания по пяти телеканалам в сумме. Это такие ограничения, как 6+, 12+, 16+ и 18+. 56 % программ возрастные ограничения не имеют, 4 % программ имеют возрастное ограничение 6+, 8 % – 12+, 31 % – 16+, и меньше 1 % программ имеют возрастное ограничение 18+.

Рисунок 3 представляет данные о странах-производителях кино/сериалов за двое суток вещания по пяти каналам в сумме. 50 % показанных в выходные кино и сериалов были произведены в России, 26 % – в США, 14 % – в СССР, по 3 % – во Франции и Германии, по 1 % – в Японии, Украине и Канаде.

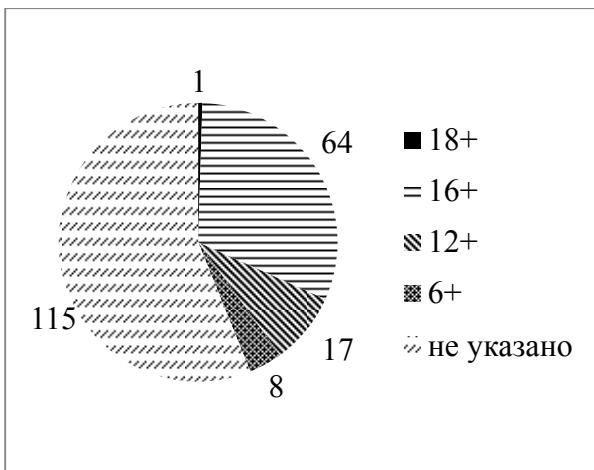


Рис. 2. Возрастные ограничения за двое суток вещания по пяти каналам в сумме

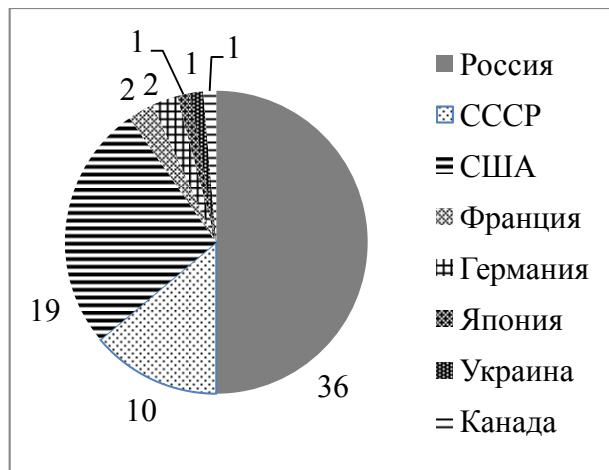


Рис. 3. Страны-производители кино/сериалов за двое суток вещания по пяти каналам в сумме

На рисунке 4 представлена информация о количестве фильмов/сериалов, выпущенных в различные десятилетия, за двое суток вещания по пяти каналам в сумме. Наибольшее количество показанного контента (69 %) было произведено в 2010-е годы, почти в пять раз меньшее количество (12 %) – в 2000-е.

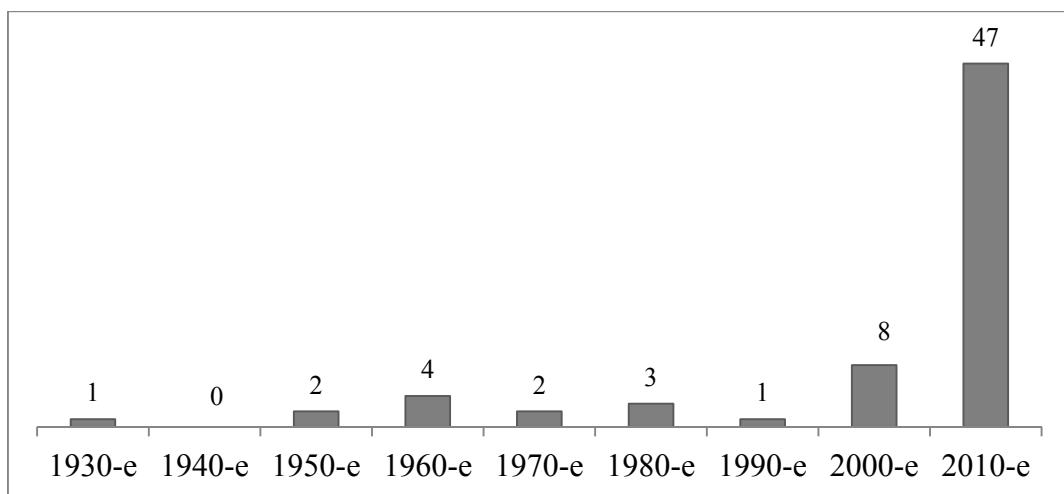


Рис. 4. Количество фильмов/сериалов, выпущенных в различные десятилетия, за двое суток вещания по пяти каналам в сумме

Рисунок 5 представляет данные о количестве фильмов/сериалов различных жанров за двое суток вещания по пяти каналам в сумме. Наиболее распространен в выходные дни такой жанр кино как комедия. Мало представлены жанры: вестерн, фильм-катастрофа, спектакль, фэнтези.

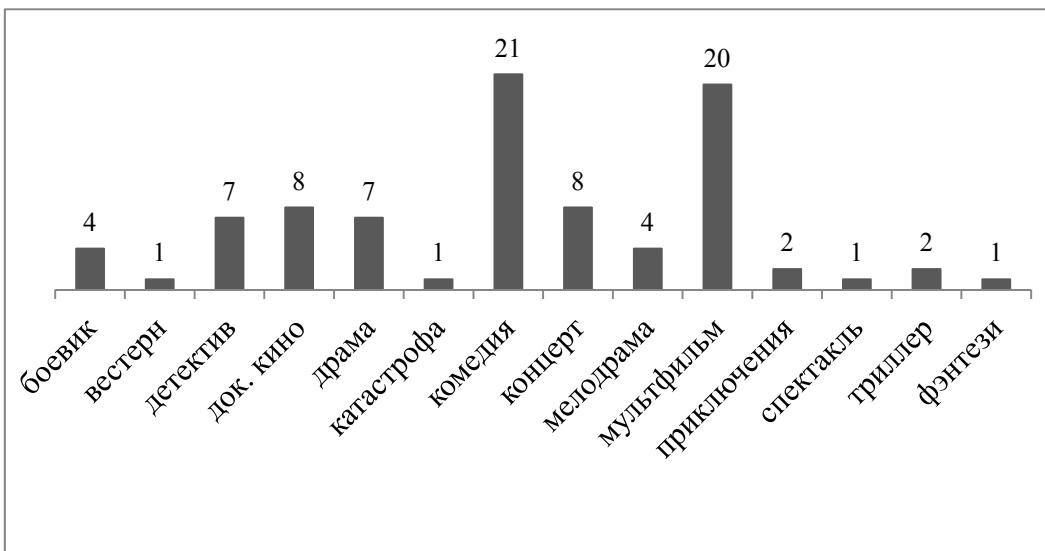


Рис. 5. Количество фильмов/сериалов различных жанров за двое суток вещания по пяти каналам в сумме

На основании проведенного исследования, можно вывести следующие специфические черты современного российского телевещания:

1. Контент телевизионных передач вышеупомянутых телеканалов ориентирован на молодежь или людей среднего возраста. Для детского возраста фактически отсутствует телевизионный продукт (исключение – телеканал СТС).
2. Среди кинофильмов иностранного производства лидером показа являются американские фильмы.
3. В выходные дни из сетки вещания исключаются сериалы, и происходит их замена фильмами (наиболее заметные изменения вносит телеканал Россия 1).
4. Из фильмов в выходные дни наиболее представлены комедии, произведенные в 2010-е годы.
5. В телевещательной сетке выходного дня авторские программы представлены в малом количестве.

Данные рекомендации могут быть использованы при создании новых телепередач с целью создания и поддержания их рейтинга. Это необходимо для получения телеканалами максимальной прибыли, которая напрямую зависит от численности аудитории.

#### Список используемых источников

1. Особенности организации производства телевизионных информационных программ / Т. Н. Парсаданова // Российское предпринимательство. – 2003. – № 5 (41). – С. 43–48.
2. Роль и место телевидения в современном медиапространстве / Д. Ю. Пащутин // Вестник Самарского государственного экономического университета. – 2010. – № 2. – С. 98–103.

3. **Тенденции** развития российского телевидения в условиях противостояния и взаимодействия мировых моделей вещания [Электронный ресурс] / А. Э. Литвинцев. – Режим доступа: <http://www.evartist.narod.ru/text16/021.htm> (Дата обращения 29.05.2014).

*Статья представлена научным руководителем, ассистентом Т. В. Молчановой.*

**УДК 316.722**

**И. А. Гель (студентка группы Э-01 СПбГУТ)**

## **СРАВНЕНИЕ РУССКОЙ И ФИНСКОЙ КУЛЬТУР: ВЛИЯНИЕ МЕЖКУЛЬТУРНЫХ РАЗЛИЧИЙ НА ВЕДЕНИЕ БИЗНЕСА**

В современном мире проблема межкультурного взаимодействия чрезвычайно актуальна, особенно в многонациональных компаниях, где руководящие и исполнительные должности занимают представители разных национальных культур. Для повышения эффективности подобного сотрудничества возникла необходимость выработать критерии для анализа межкультурных различий. В данной работе деловые культуры России и Финляндии рассматриваются в контексте теории голландского исследователя Герта Хоффстеде, который одним из первых использовал статистические данные для анализа культурных национальных ценностей, которые дали возможность сравнивать деловые культуры. В результате проведенного исследования, в котором приняли участие более 115 тысяч сотрудников компании *IBM* из 75 стран, Герт Хоффстеде выделил шесть параметров деловой культуры, построенных в виде бинарных оппозиций [1].

1. Дистанцированность от власти – степень готовности (добровольности) общества принимать неравенство распределения власти во взаимоотношениях и в организациях.

В культурах с высокой дистанцией власти сотрудники открыто не выражают несогласие с мнением начальства; разрыв в оплате труда сотрудников может превышать двадцатикратный уровень; наличие у руководителей привилегий распространено и считается нормальным.

В обществах с низкой дистанцией власти люди стремятся к уравнению распределения власти и требуют обоснования неравенства.

2. Соотношение индивидуализма и колLECTивизма – противопоставление общества со свободной/нежесткой социальной структурой обществу с жесткой/строгой социальной структурой, четким разделением на социальные группы.

В культурах с высокой степенью индивидуализма люди откровенно высказывают критические замечания; продвижение по службе связано с достоинствами работника; средний класс составляет солидную прослойку.

В культурах с высокой степенью коллективизма интересы коллектива выше личных; профессиональная зрелость – прерогатива возраста, что затрудняет карьерное продвижение.

3. Соотношение мускулинности и фемининности, или мужественности и женственности, как принято называть данный параметр в отечественной литературе [2], хотя речь не идёт о гендерном аспекте.

Мускулинность – приверженность таким ценностям, как рекорды, героизм, упорство в достижении цели, материальный успех и т. п.

Фемининность – приверженность таким ценностям, как выстраивание отношений, склонность к компромиссам, скромность, забота о ближнем, уют, качество жизни и т. п.

4. Избегание неопределенности – степень восприятия и реагирования на незнакомые ситуации или двусмысленности.

В культурах с высокой степенью избегания неопределенности обществу присущи напряженность и беспокойство. Проявление агрессивности и эмоций на работе и в быту – нормальное явление; люди испытывают потребность в четких правилах поведения; распространены негативно-критическое восприятие власти, раздражение по отношению к национальным меньшинствам; привязка карьеры к возрасту.

В культурах с низкой степенью избегания неопределенности считают, что всего предугадать нельзя; детальным контрактам предпочитают рамочные договоренности с возможностью корректировки по ходу дела.

5. Соотношение pragmatizma и нормативности. Параметр описывает отношение людей к тому, что многие вещи не могут быть объяснены.

В обществах с прагматической ориентацией большинство людей считают, что невозможно в полной мере понять всю сложность жизни. Допустимо существование одновременно нескольких верных точек зрения. Люди подстраиваются под ситуацию, имеют склонность к сбережению.

В обществах с нормативной ориентацией у большинства людей сильное желание объяснить все настолько, насколько это возможно; люди сильно обеспокоены установлением абсолютной истины, они нуждаются в личной стабильности, имеют небольшую склонность к сбережениям.

6. Соотношение стремления к удовольствиям и самоограничения.

В обществах с ориентацией на удовольствие людям важно удовлетворять свои потребности в развлечениях и наслаждении жизнью.

В обществах с ориентацией на самоограничение люди подавляют свои потребности в удовольствиях. Это регулируется социальными нормами.

Рисунок наглядно демонстрирует вышеуказанные параметры применительно к культурам России и Финляндии [3]. За 100 баллов принимается высшая степень первого параметра в каждой оппозиционной паре.

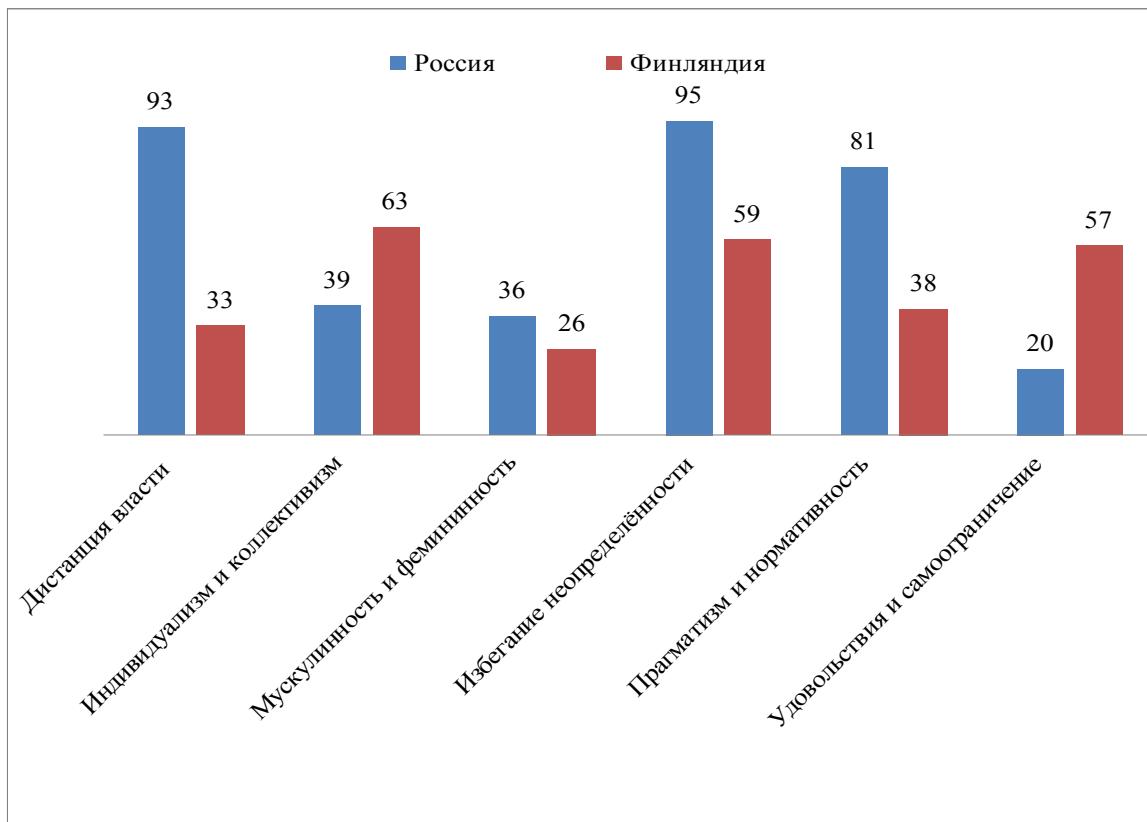


Рис. 1. Сравнение России и Финляндии по теории Г. Хофстеде

1. Дистанцированность от власти: Финляндия (33) и Россия (93).

У Финляндии относительно низкая оценка по этому параметру – 33. Это означает, что иерархическая структура не строгая. Отношения между людьми различных слоёв общества и различного статуса неформальные.

Россия имеет очень высокий балл по этому показателю – 93. Люди не равны между собой, и это является нормой для них. Здесь много правил, чёткая иерархическая структура, строго соблюдается субординация.

2. Индивидуализм/коллективизм: Финляндия (63) и Россия (39).

Финляндия – страна индивидуалистов. Здесь делают акцент на инициативность. Финны принимают решения самостоятельно.

В России низкий уровень индивидуализма. Для русских имеют большое значение хорошие взаимоотношения. В бизнесе для них важно хорошо знать человека, с которым они имеют дело. Управляющие чаще предпочитают принимать решения в группах, а не самостоятельно.

3. Мускульность/фемининность: Финляндия (26) и Россия (36).

Финляндия имеет низкий показатель по мускульности – это феминистская страна. Люди высоко ценят комфорт и свободу. Конфликты решаются компромиссом.

Оценка по мускулинности у России также довольно низкая. Люди всегда заботятся друг о друге, их волнуют проблемы всех знакомых. Управленцы часто заботятся о своих сотрудниках.

**4. Избегание неопределенности: Финляндия (59) и Россия (95).**

Данный показатель достаточно высокий у Финляндии. Люди придерживаются сложившихся обычаев и традиций. Они чувствуют себя неуверенно, если нет чётких указаний к каким-либо действиям.

В России чрезвычайно высокий уровень избегания неопределенности. Русские заботятся о завтрашнем дне и не могут быть уверены в будущем. Стабильность и безопасность важны и для менеджеров. Может быть, именно из-за этого высок и уровень коллективизма в России.

**5. Прагматизм/нормативность: Финляндия (38) и Россия (81).**

Финскую культуру можно отнести к нормативной культуре. У людей сильно развито чувство справедливости. Они проявляют уважение к традициям и небольшую склонность к сбережениям на будущее.

Россияне имеют прагматический склад ума. Они считают, что истина зависит от ситуации и времени; склонны к бережливости, инвестированию.

**6. Стремление к удовольствиям против самоограничения: Финляндия (57) и Россия (20).**

Финляндия имеет довольно высокую оценку по этому параметру. Финны склонны к оптимизму и имеют позитивный настрой. Они очень ценят своё свободное время, это важная часть их жизни.

По данному параметру Россия получает низкий балл. Это означает, что русские склонны к пессимизму. Они не делают акцент на развлечения и контролируют свои желания. Их сдерживают социальные нормы.

При рассмотрении параметров межкультурных различий, становится очевидным, что страны сильно отличаются друг от друга. Самый большой разрыв мы видим в параметре дистанцированности от власти. Фемининность – единственный параметр, по которому страны находятся примерно на одинаковом уровне.

В соответствии с вышеприведенным сравнительным анализом, можно разработать рекомендации для финских и российских менеджеров руководящего и исполнительного уровней, работающих соответственно в России и в Финляндии, которые приведены в таблицах 1 и 2.

ТАБЛИЦА 1. Рекомендации для руководящего звена

Финские менеджеры в России	Российские менеджеры в Финляндии
Будьте дружелюбными, но соблюдайте субординацию. Давайте прямые, недвусмысленные распоряжения	Больше сотрудничайте и активно участвуйте в работе с подчинёнными.
Знакомьтесь ближе, общайтесь с партнёрами. Это может занять некоторое время, но оно того стоит.	При ведении переговоров настройтесь на деловой подход. Можно поговорить на отвлеченные темы, но недолго. Финны будут

	разочарованы неэффективностью переговоров.
Устанавливайте чёткие временные границы. Будьте готовы к задержкам.	Соблюдайте временные рамки. От Вас этого ожидают.

ТАБЛИЦА 2. Рекомендации для исполнительного звена

Финские работники в России	Российские работники в Финляндии
Следуйте инструкциям старших по рангу. Не ставьте под сомнение планы их действий.	Старайтесь быть активными. Открыто высказывайте свои идеи по поводу проектов.
Спросите разрешения, прежде чем проявлять инициативу.	Не ждите, что распоряжения всегда будут чёткими и недвусмысленными.
Чтобы продвинуться по карьерной лестнице, старайтесь дружить с «нужными людьми» в компании.	Чтобы продвинуться по карьерной лестнице, старайтесь завершить работу в установленные сроки и сделать её хорошо. Результат не заставит себя ждать.

Различия в деловых культурах Финляндии и России являются следствием особенностей национальных культур. Несмотря на то, что стили управления со временем становятся похожими, различия всё же могут стать препятствием для эффективного взаимодействия. Взаимное понимание, основанное на изучении межкультурных различий, и открытое общение чрезвычайно важны для того, чтобы многонациональные компании успешно сотрудничали в современном мире бизнеса.

#### Список используемых источников

1. *Culture's Consequences: Comparing values, behaviors, institutions, and organizations across nations* / G. Hofstede. – Sage Publications, 2001. – 616 p.
2. **Межкультурная** коммуникация и корпоративная культура: учебное пособие / Т. Н. Персикова. – М. : Логос, 2002. – 224 с.
3. **National** cultural dimensions [Электронный ресурс] / The Hofstede Centre. Cultural tools. Country comparison. – Режим доступа: <http://geert-hofstede.com/national-culture.html> (Дата обращения 12.04.2014).

*Статья представлена научным руководителем, доцентом Н. В. Беспаловой.*

УДК 94

**А. Б. Гехт (аспирант кафедры Истории и регионоведения СПбГУТ)**

**АЛАНДСКИЙ ВОПРОС В ОТНОШЕНИЯХ ШВЕЦИИ  
И ФИНЛЯНДИИ В 1918–1921 гг. КАК ПРИМЕР РЕШЕНИЯ  
ЭТНОТЕРРИТОРИАЛЬНОГО КОНФЛИКТА  
В СЕВЕРНОЙ ЕВРОПЕ**

Практически все современные государства полиглоссичны, но степень полиглоссичности в различных регионах заметно различается. Представители различных этносов отличаются своим традиционным бытом и культурой. Однако, все члены полиглоссического общества, являются ли они представителями этнического большинства или меньшинства, должны иметь одинаковые права и обязательства перед государством. Поэтому важнейшими принципами современного международного права являются, с одной стороны, суверенитет государства, с другой – право на самоопределение народа, согласно которому все народы могут свободно определять, без вмешательства извне, свой политический статус и осуществлять свое экономическое, социальное и культурное развитие. В этой связи вопрос о положении этнических меньшинств, обеспечении их прав имеет особое значение. Защита прав национальных меньшинств должна обеспечить им равные с доминирующим этносом права во всех сферах жизни, но, с другой стороны, и создать благоприятные условия для сохранения их этнического своеобразия. Для стран Северной Европы подобное положение вещей является достигнутым результатом. Особенно показателен в этом отношении пример решения этнополитической проблемы в отношениях Швеции и Финляндии в период 1920–1930 гг. по определению политического статуса Аландских островов, преимущественно населенных шведами, но входивших в состав Финляндии.

Аландские острова (*швед. Åland, фин. Ahvenanmaa*) – архипелаг в Балтийском море, расположенный вблизи Ботнического залива. Исторически он был заселён шведами и входил в состав шведского королевства вплоть до начала XIX века. Но в соответствии с условиями Фридрихсгамского мирного договора от 17 сентября 1809 года между Россией и Швецией Аландские острова вместе с Финляндией вошли в состав Российской империи. Для России это было важное территориальное приобретение, прежде всего со стратегической точки зрения, поскольку обладание островами в значительной степени позволяло контролировать военные и торговые морские коммуникации в регионе Балтийского моря. В повседневной жизни жителей островов практически ничего не изменилось. Шведский язык по-прежнему был языком повседневного общения, делопроизводства и образования.

С 1830 года на архипелаге началось строительство российских военных укреплений. Но в ходе Крымской войны русская крепость Бомарсунд на Аландских островах была атакована, частично разрушена и захвачена англо-французскими силами. Крымская война завершилась подписанием Парижского мирного договора 18 (30) марта 1856 года. К тексту мирного договора была приложена конвенция об Аландских островах, в которой было зафиксировано обязательство со стороны России, согласно которому «Аландские острова не будут укрепляемы и что на оных не будет содержимо и вновь сооружено никакого военного или морского заведения». Таким образом, эта конвенция установила демилитаризованный статус Аландских островов [1]. Потеря возможности использовать Аланды в качестве укрепленной военно-морской базы отрицательно сказалась на стратегическом положении России регионе Балтийского моря. Более поздние попытки России пересмотреть соглашение 1856 г., предпринятые в 1907 г., не привели к успеху и вплоть до начала Первой мировой войны Россия не имела военного присутствия на Аландских островах. Только с началом боевых действий, когда возникла угроза захвата архипелага немецкими войсками, которые могли использовать его для дальнейшего продвижения на территорию Финляндии, на островах были размещены русские войска, что вызвало негативную реакцию со стороны Швеции, опасавшейся возможной военной угрозы со стороны России [2, С. 228–231].

На протяжении значительной части XIX века шведский язык продолжал оставаться официальным в системе государственного управления и образования на территории Финляндии, был языком элиты княжества, в то время как финский использовался большинством простого народа. Такое положение вещей стало причиной т. н. «фенномании», то есть стремления финнов, главным образом интеллигенции, к расширению использования финского языка и допуску его в сферу управления, в судопроизводство, в школы и университет. Однако это движение породило ответное стремление шведского меньшинства Финляндии к сохранению своих привилегированных позиций. Эти трения особенно ярко проявились в 1917 году, после обретения Финляндией независимости, в противостояние шведской общины Аландских островов и финского правительства.

В 1917 году Финляндия стала независимым государством. По условиям Брест-Литовского мирного договора, подписанного в марте 1918 года, предусматривался скорейший вывод российских сухопутных и военно-морских сил с территории Финляндии, в т. ч. и с Аландских островов. В дальнейшем вопрос о статусе Аландских островов решался уже без участия России вплоть до второй половины 1930 гг.

После провозглашения независимости Финляндии Швеция проявила заметный интерес к Аландскому архипелагу. В новых политических условиях шведская сторона высказала претензии на Аландские острова, опираясь на то, что Фридрихсгамский договор 1809 года утратил силу и что

население архипелага в подавляющем большинстве состояло из этнических шведов. Местное, преимущественно шведское население, негативно воспринимало свое нахождение в составе Финляндии, опасаясь вытеснения шведского языка и привычного образа жизни за счет насаждения финскими властями своего языка. 13 февраля 1918 года шведское правительство приняло решение отправить десант на Аланды под предлогом защиты местного населения. Сами жители Аландских островов также заявляли о своем желании войти в состав Швеции. Впервые это стремление было публично высказано еще до полного отделения Финляндии от России, 20 августа 1917 года. Это требование было повторено в начале 1918 года, когда аландская делегация посетила Стокгольм [3, S. 230].

Так в начале XX века вопрос о политическом и территориальном статусе Аландских островов приобрел особую актуальность для региона Балтийского моря. Он включал в себя две составляющие: стратегическую (важность архипелага с военной точки зрения) и национальную. Финская сторона негативно реагировала на шведские притязания и, в частности, на высадку шведского десанта на островах. Но в то же время в Хельсинки понимали необходимость определенных уступок, как шведской стороне, так и населению Аланд. 13 июня 1918 года Аландские острова были отделены от губернии Турку-Пори в отдельную губернию (лен в шведской традиции) с собственным провинциальным управлением. Тем не менее, сторонники выхода из состава Финляндии продолжали настаивать на дальнейших шагах по решению сложившейся ситуации. Ими был выдвинут лозунг: "Finland fritt – Åland svenska" («Свободная Финляндия – шведские Аланды») [4, S. 133].

В 1918–1920 годах Аландский архипелаг оставался предметом территориального спора между Финлядией и Швецией. Для решения сложившейся проблемы был создан Аландский комитет, сформированный в Хельсинки летом 1918 года из числа представителей умеренных шведоязычных общественных деятелей. Комитет, исходя из сохранения суверенитета Финляндии над Аландскими островами, разработал проект местного самоуправления для населения островов [4, S. 134]. Достаточно активно Аландский вопрос поднимался в ходе Парижской мирной конференции 1919 года, на которой обсуждались вопросы послевоенного устройства Европы. После обмена резкими нотами между финским и шведским правительствами конференция приняла предложение Великобритании о дальнейшем решении вопроса в ходе деятельности созданной Лиги Наций. 6 мая 1920 года финский парламент принял Акт об автономии Аландского архипелага. Этот документ провозгласил создание собственных учреждений автономии и установил их полномочия, которые приблизительно соответствуют существующим и в настоящее время. Но сторонники отделения Аландских островов от Финляндии продолжали отстаивать свою позицию и запросили у шведского правительства поддержки их требований о проведении пле-

биссита, который должен был решить судьбу региона. Ситуация особенно обострилась, когда лидеры движения за выход Аландского архипелага из состава Финляндии Ю. Сюнdblум и К. Бьёркман в июне 1920 года были арестованы. Шведское правительство направило запрос в Совет Лиги Наций, ходатайствуя о рассмотрении вопроса о статусе Аландских островов.

В финско-шведском споре за Аланды западные державы, в конечном счете, приняли сторону Финляндии: для них было важно сохранить позитивные отношения с Финляндией, которая непосредственно граничила с Советской Россией и рассматривалась как важный элемент создаваемой «версальской системы». 24 января 1921 года Лига Наций признала суверенитет Финляндии над Аландскими островами при условии, что аландская автономия будет подкреплена гарантиями сохранения шведского характера автономной территории [5, S. 535].

В 1921 году на 13-й сессии Совета Лиги Наций был представлен доклад Комиссии по решению Аландского вопроса, где указывалось, что Аландские острова должны оставаться под суверенитетом Финляндии. Комиссия отметила всеобщий характер пожеланий аландцев присоединиться к Швеции, но не сочла возможным их удовлетворить. 24 июня 1921 года Совет Лиги Наций утвердил резолюцию о суверенитете Финляндии над Аландскими островами. Финляндия обязывалась не вводить военные укрепления на островах и гарантировать преподавание шведского языка в аландских школах. Совет Лиги рекомендовал в целях гарантии автономии Аландов заключить договор между Финляндией и Швецией. 27 июня под эгидой Совета Лиги было подписано окончательное шведско-финское соглашение об условиях автономии Аландского архипелага, которое было включено в принятую 24 июня 1921 года резолюцию.

Решение Совета Лиги Наций не удовлетворило ни одну из сторон. Шведское правительство протестовало против финляндского суверенитета, а финское – недовольно предполагаемым контролем Лиги Наций над соглашением по вопросу о национальном меньшинстве. В октябре 1921 года под эгидой Лиги Наций в Женеве состоялась конференция, ставившая целью заключение международного договора о демилитаризации и нейтрализации Аландского архипелага. В подписанный 20 октября 1921 года международной конвенции о демилитаризации и нейтрализации Аландского архипелага Финляндия обязывалась не строить военных объектов на Аландских островах. Во время войны зона островов должна будет рассматриваться как нейтральная, а в случае военного конфликта на Балтийском море Финляндия получала право защиты нейтралитета Аландов. Суверенитет Финляндии над Аландскими островами сохранялся при условии предоставления дополнительных гарантий автономии для местного населения. Договаривающиеся стороны могли, когда сочтут необходимым, обращаться в Совет Лиги для определения мер соблюдения конвенции.

Более десяти лет вопрос о суверенитете Аландских островов не играл особой роли в международных отношениях в регионе Северной Европы, оставаясь второстепенным, в том числе и, в эволюции отношений между Швецией и Финляндией. Компромиссное решение проблемы, предложенное международным сообществом, остановило дальнейшее осложнение шведско-финских отношений, но не привело к окончательному упразднению противоречий, что проявилось в конце 1930 гг., в период роста международной напряженности в Европе. Незавершенное решение Аландского вопроса сказывалось на шведско-финских отношениях весь период между двумя мировыми войнами, негативно влияя на эволюцию отношений двух стран. Именно конфликт из-за статуса Аландских островов, в значительной степени препятствовал сближению Швеции и Финляндии в предвоенный период и, в конечном итоге, созданию совместного оборонительного союза. Тем не менее, противоречия между Швецией и Финляндией по вопросу суверенитета Аландских островов было разрешено мерным путём и не привело к вооруженному конфликту между двумя государствами.

#### **Список используемых источников**

1. Конвенция об Аландских островах от 18 (30) марта 1856 г. / Е. В. Тарле. Крымская война. – М., 2003. – Т. 2. – Приложение. – С. 703
2. Аланды в войнах и мире. Або-Аланды и их ненарушаемый нейтралитет в войнах XVIII–XX столетий по документам российских архивов и историческим изданиям / С. В. Тиркельтауб. – СПб., 2008.
3. Självstyrelsetanken i finlandssvensk politik // Svenskt i Finland. 1. Studier i språk och nationalitet efter 1860 / G. Von Bonsdorff. – Helsingfors, 1983.
4. Ålänningsarna och Ålandsfrågan // Väster om Skiftet. Uppsatser ur Ålands historia / G. Höglund. – Åbo, 1986.
5. Finlands svenskar / H. Dahl. – Helsingfors, 1954.

*Статья представлена научным руководителем,  
д-ром ист. наук, профессором С. Н. Полтораком.*

**УДК 821.111**

**О. С. Дерябина (студентка группы ЗР-22 СПбГУТ)**

#### **ПЕРСОНАЖИ ПЬЕС У. ШЕКСПИРА И ИСТОРИЧЕСКАЯ РЕАЛЬНОСТЬ**

Пьесы Уильяма Шекспира – поистине захватывающий феномен в литературе. Его сонеты, комедии, трагедии и исторические хроники одинаково любимы, не только в Британии, но и во многих других странах мира.

Его хроники доносят до нас истории о британских королях Средневековья, однако Шекспир никогда не стремился быть исторически достоверным: основной целью было развлечение публики. И тут напрашивается вопрос: насколько шекспировская интерпретация исторических событий отличается от реальных событий? Где находится эта грань между выдумкой и реальностью? Проведенное исследование поможет ответить на эти вопросы.

Уильям Шекспир – известный английский поэт и драматург конца XVI – начала XVII веков; он заслуженно называется достоянием Англии. Шекспир произвёл резонанс своими пьесами, однако шум вокруг него не утихает и по сей день – исследования его личности и произведений по-прежнему занимают умы лингвистов, литераторов и историков. Он родился 23 апреля 1564 года в Стратфорде-на-Эйвоне. О дальнейшей его жизни до 1582 года (когда он женился на Энн Хатауэй) известно достаточно мало, так как не сохранилось никаких источников, указывающих на его образование. Годы после рождения близнецов Гамнета и Джудит также не освещены никакими историческими записями, их называют «потерянными годами»; разве что из последующих источников нам известно, что он работал в Лондоне драматургом и позднее вместе со своей труппой построил театр «Глобус» на берегу Темзы.

Шекспир написал 38 пьес, 2 поэмы и 154 сонета. Авторство этих произведений окружено покровом тайны, ведь образование, которое, вероятно, получил Уильям, не могло бы дать ему столь огромный словарный запас и таких разносторонних знаний из весьма различных сфер современной ему жизни общества и дворянства. Существует множество теорий об авторстве шекспировских пьес. Считается, что «Шекспир» может быть своеобразным щитом для другого автора или группы авторов. Авторство приписывают таким личностям как Кристофер Марло, Эдвард-де-Вер, Френсис Бэкон, сэр Франсис Дрейк и даже самой королеве Елизавете I. Всего насчитывается около 84 претендентов на авторство. Был или не был Шекспир тем, за кого он себя выдавал, не исключает того факта, что работы его гениальны. И это приводит нас к основной теме работы – историческим хроникам.

Уильям Шекспир считается автором десяти исторических хроник и предположительно соавтором ещё одной хроники «Эдуард III».

- 1) Король Иоанн (1596-1597).
- 2) Ричард II (1595).
- 3) Генрих IV, две части (1590-е).
- 4) Генрих V (1599).
- 5) Генрих VI, три части (1590-1592).
- 6) Ричард III (1592-1593).
- 7) Генрих VIII.

Шекспир был ограничен в источниках, которые он мог использовать для своих хроник, и, в основном, он использовал одну или две книги. Из-

вестно, что он использовал «Жизнь Ричарда III» Томаса Мора, «Союз благородных и прославленных семей Ланкастеров и Йорков» Эдварда Халла и, как один из его наиболее доверенных источников, «Хроники Англии, Шотландии и Ирландии» Рафаэля Холишеда. Последний источник был наиболее предпочтителен Шекспиру, а так как границы между домыслами и реальностью достаточно туманны, то, если Холишед записал что-либо не так, Шекспир повторял эту ошибку [1].

Стоит заметить, что Шекспир был во многом достаточно точен. Тем не менее, многие события были выдуманы автором: они либо попросту не могли произойти, либо же у нас нет доказательств, что они имели место быть.

Во-первых, в хрониках Шекспир играет со временем, переставляя события по своему усмотрению. Либо мы можем наблюдать, как он виртуозно размещает период протяжённостью в 5–10 лет всего на паре десятков строк, либо то, как он совмещает несколько исторических баталий воедино, представляя нам одну яркую картину.

Во-вторых, Шекспир играет с именами. Иногда он может заменять персонажей по своему усмотрению, либо же он помещает в сцену человека, который просто не мог исторически находиться в ней, так как документально подтверждено, что эта персона в это время находилась в другой части страны. Например, принц Хал (будущий король Генрих V) не мог сражаться бок о бок со своим отцом в некоторых битвах шекспировских хроник, так как в это время он находился далеко на северо-западе Англии. Ка-сательно игры имён есть один яркий пример: персонаж, весьма полюбившийся людям – Фальстаф – был реально существующей личностью и действительно был компаньоном принца Хала. Однако игра состоит в том, что Шекспир взял лишь имя достопочтенного воина и героя – Джон Олдкасл – и превратил его в разгульного пьяницу и труса. Позднее автору пришлось сменить имя, так как потомки Олдкасла потребовали прекратить порочить имя их предка [1].

В-третьих, в интересах пьесы Шекспир играл ещё и с личностями своих героев. Пожалуй, пример с Фальстафом можно отнести и сюда. Однако есть и более яркие примеры. Портрет Ричарда II, написанный Шекспиром, был сильно омрачён по сравнению с тем, каким был король. Автор сконцентрировался на последних годах правления Ричарда и создал поэтически трагический персонаж, который всё же имеет мало общего с королём Ричардом.

Также и портрет Генриха V был весьма сильно преображен, хотя и в иную сторону. Он изображён юным, мятежным принцем, который затем становится зрелым мужчиной, отправляющимся на удачное покорение Франции. Шекспир делает его своеобразным символом великой Англии, только вот этот портрет Генриха V весьма сильно приукрашен [1].

В истории о Ричарде III многие факты, безусловно, являются реальными. Только вот портрет самого короля Шекспир снова исказил. Нам не известно, действительно ли король Ричард убил двух принцев в Тауэре – это всё ещё тайна, покрытая мраком. Также мы не знаем, действительно ли Ричард был угрюмым горбуном и отъявленным негодяем, который проснулся одним утром и решил стать злодеем. У нас попросту нет доказательств этого. Он был хорошим солдатом, и это говорит о том, что, скорее всего, он не был физически уродлив – Шекспир добавил это лишь для того, чтобы сделать историю более захватывающей [2].

Нужно не забывать быть осторожными, читая его хроники, ведь есть определённая грань, отделяющая реальность и вымысел. Тем более что Шекспир писал во время правления Елизаветы I, и он создал эти пьесы, показывая, как много крови и хаоса принесла династия Плантагенетов в Англию в сравнении с миром и покоем эпохи Тюдоров. Так что, пожалуй, хроники Шекспира отражают не столько эпоху Средневековых королей, сколько эру самого Уильяма.

Пьеса – это игра, и, создавая свои исторические хроники, Шекспир играет с историей. Он берёт что-то реальное и создаёт нечто новое и своё, слегка изменяя и украшая. Шекспиру нужно отдать должное за то, что он превратил сухие исторические хроники в нечто волшебное и захватывающее.

#### **Список использованной литературы**

1. **Shakespeare's English Kings: History, Chronicle, and Drama** / Peter Saccio. – Oxford University Press, 2000 – 296 c.
2. **Shakespeare's Kings: The Great Plays and the History of England in the Middle Ages: 1337–1485** /John Julius Norwich // Scribner. – 2001. – 432 c.

*Статья представлена научным руководителем,  
старшим преподавателем А. Б. Булатова.*

**УДК 338.242.2**

**Е. А. Дорохова (студентка группы РСО-11 СПбГУТ)**

## **ПРАКТИКИ ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ КОНКУРЕНТАМ: РЕКЛАМНЫЕ ВОЙНЫ**

Развязать войну на динамичном рынке рекламы – серьезный шаг. Несомненно, к нему нужно готовиться долго и тщательно. Для того чтобы война не являлась бессмысленной или, что еще хуже, негативно по-

влияла на имидж той или иной компании-бренда, необходимо грамотно выбрать или разработать стратегию поведения.

*Рекламная война* – это форма привлечения внимания к деятельности двух (и более) брендов-конкурентов посредством совместных рекламных кампаний, направленных на противоборство рекламных сообщений.

В рекламе, как таковой, идет привлечение внимания потребителей к компании-производителю, к ее деятельности и продукции. В случае же с рекламной войной речь идет не только о целевой аудитории «потребитель», но и о такой целевой аудитории, как «конкурент».

Под понятием «рекламная война» подразумевается не война между производителями, а война реклам. Такая война является совместной рекламной кампанией. При грамотном ведении подобной войны мнения потребителей должны разделиться: в этом случае они принимают одну из противоборствующих сторон. Отсюда вовлеченность клиента и потенциального клиента в «разборки» компаний-брендов, что, несомненно, увеличивает эффективность рекламных сообщений в войне по сравнению с обычными. Для удобства восприятия и возможности вовлечься в рекламную войну между брендами, а также для создания иллюзии «ответа» обе стороны выбирают один и тот же канал коммуникации. Чаще всего выбирают наружную рекламу и рекламу в сети Интернет.

Тщательная подготовка к рекламной войне, впрочем, как и в любой сфере, занимает больше времени, нежели сама реализация. В основе подготовке к подобным войнам всегда лежит *стратегия*.

Стратегии ведения рекламных войн выбираются в зависимости от занимаемых компанией и ее конкурентом позиций на рынке. Однако, при формировании стратегии необходимо помнить о следующих неформальных правилах [1]:

1. Нельзя нападать на конкурента, рыночные позиции которого слабее, чем Ваши.

2. Нападать на конкурента стоит только в том случае, когда есть за что «зацепиться».

3. Не стоит явно упоминать в своей рекламе имя конкурента.

4. Не стоит в рекламном сообщении зацикливаться на конкуренте.

Важнее то, что Вы скажете о себе.

5. Помните о деловой этике.

6. Если все-таки решились на контратаку, то ее лучше не откладывать, иначе целевая аудитория может потерять нить ведения войны между Вами и Вашим конкурентом.

7. Нападение на равных себе намного эффективнее нападения на конкурента слабее или сильнее Вас.

8. Практически все зависит от конкретных условий: Вашей силы, ресурсов, целей, позиции на рынке, действующей ситуации на рынке и от конкурента.

9. В случае рекламной войны чаще всего выигрывает лидирующий на данный момент бренд.

10. Эффект от ненужных конфликтов необходимо сводить на «нет».

11. Обычно тот, кто нападет, задает темп и стиль ведения всей рекламной войны.

*Стратегии поведения в рекламных войнах:*

*Стратегия атаки.* Заключается в нападении на слабые, уязвимые места более сильного или равного по силе соперника. Здесь важно про-считать атаку таким образом, чтобы контратака соперника не явила со-бой сильный, мощный ответ, который бы сокрушил атакующий бренд на уровне рекламы. В случае с сильным соперником стоит быть осторож-нее, т. к. чаще всего в открытой схватке побеждает та армия, у которой больше ресурсов и силы. Если все-таки решились нападать, то момент для такого нападения нужно выбирать таким образом, чтобы вы смогли извлечь победу и максимальную пользу от этой атаки.

*Стратегия обороны.* В случае атаки необходимо смотреть на ситу-ацию хладнокровно и рационально. Как говорится, лучшая защита – это нападение. Рекламная война не исключение. Если тот или иной бренд решил атаковать своего конкурента, то одним из самых лучших способов защитить себя и осадить нападающего будет *контратака*. Если все-таки решились на контратаку, то ответ конкуренту должен быть практически незамедлительным, в противном случае, это может затянуться надолго, тогда поздний ответ не принесет никакой эффективности, т. к. потреби-тель уже не вспомнит сложившуюся ситуацию.

Необходимо быть действительно сильным и компетентным брен-дом, чтобы иметь возможность атаковать любого противника и огор-дить себя от излишних нападений.

В свою очередь атака, как и оборона (контратака), делится на *пря-мую и косвенную*.

*Прямая атака* и контратака – это атака «лоб в лоб» с упоминанием названия или логотипа бренда конкурента, на которого мы нападаем или которому отвечаем. Как правило, такая атака дает наибольшие потери. Атакующий бренд рискует потерять доверие и уважение своего потреби-теля.

*Косвенная* стратегия атаки или контратаки – это упоминание в ре-кламе не самого конкурента, а его атрибутов, как бы намекая на него.

Далее прямая и косвенная атака или контратака может быть:

– *Односторонней* (применительно только к атаке) – война ведется одной стороной, а вторая предпочитает не реагировать на ее рекламные сообщения. Создается эффект ведения войны только лишь одной сторо-ной. Вторая сторона стремиться «мягко свести эффект ненужного скан-дала к нулю». Порой действительно лучше достояно промолчать. При-

мер с *Pepsi* и *Coca-Cola*. Нападает преимущественно *Pepsi*. Как таковая, *Coca Cola* не участвует в этой битве, эпизодически проводя незаметные рестайлинги своего столетнего логотипа и наблюдая за тем, как активна в этом смысле *Pepsi* [2].

– *Многосторонняя* – война ведется двумя и более противоборствующими сторонами. Чаще всего рекламная война ведется двумя сторонами. Двухсторонний вариант намного эффективнее, чем, если в войне появиться еще и третья сторона. При таком раскладе потребителю будет трудно отслеживать суть противоборства. Хотя, если рекламное сообщение разовое и «прямо в яблочко», то оно может быть весьма любопытным. Пример рекламной войны *Apple* и *Samsung*, но только добавим *Nokia*. В своей рекламе «*Nokia Lumia 920 Windows Phone*» *Nokia* позволила себе высмеять противоборство между *Samsung* и *Apple*, тем самым привлекла внимание потребителей и к своему бренду, уверив клиента, что она ничуть не хуже тех двоих. Пока *Apple* и *Samsung* тратили свои силы и ресурсы как в рекламной, так и в маркетинговой войне, *Nokia* зарабатывала на их сражении.

– *Одноканальная* – война, где затрагивается лишь один канал размещения рекламного сообщения. Как правило, популярностью в рекламной войне пользуются наружная реклама и реклама в Интернете.

– *Многоканальная* – рекламные сообщения противоборствующих сторон появляются на разных каналах размещения рекламы.

– *Кратковременная* – такая война предусматривает не более одного сообщения с каждой стороны.

– *Долговременная* – происходит долгая рекламная «перепалка» между конкурентами (более чем два рекламных сообщения с каждой стороны).

– *Однократная* – после окончания войны между сторонами следующая рекламная война между этими же брендами не возникает. Это свидетельствует либо о неэффективности рекламных кампаний конкурентов, либо война слишком быстро закончилась, поражением или победой одной из сторон.

– *Многократная* – рекламные атаки одних и тех же брендов то затихают, то возобновляются снова через определенное время. Наиболее эффективны, т.к. потребитель успевает проследить противоборство этих брендов, а, следовательно, запомнить их. Пример рекламной войны *Audi* и *BMW*. Их рекламные кампании направленные друг на друга начались с 2006 г. по 2007 г., затем возобновились в 2009 г. и т. д. Здесь нужно знать меру, чтобы не надоест своей аудитории.

Выше перечисленные стратегии не должны существовать в отдельности. Планируя стратегию нужно рассматривать комбинацию данных стратегий и выстраивать их в одну. Для создания ярких, привлекающих внимания рекламных сообщений можно выделить следующие стратегии:

– «*Насмешка*» – в рекламных сообщениях бренд придерживается насмешки над противником.

– «*Поздравление*» – атака и контратака происходит на основе саркастических замечаний (поздравлениях). Снова возвращаясь к рекламной войне *Audi* и *BMW*, невозможно пройти мимо взаимных «поздравлений» брендов. Ответом *Audi* на поздравление *BMW* с текстом «Поздравляем *Audi* с победой в конкурсе «Машина года–2006» в Южной Африке от победителя конкурса «Машина мира–2006» было «Поздравляем *BMW* с победой в конкурсе «Машина мира–2006». От шестикратного победителя гонок *Consecutive Le Mans 24 Hour (2000–2006)*».

– «*Провокация*» – провокационные рекламные сообщения, требующие ответной реакции.

– «*Унижение*» – реклама, так или иначе унижающая бренд конкурируента. Примером является рекламная война между крупными автопроизводителями *BMW* и *Mercedes*. *BMW* в одном из своих атакующих рекламных постов был представлен, как леопард, то есть хищник, который в природе – мощный, сильный, агрессивный. *Mercedes* предстал потребителю в образе зебры, которая в природе никогда не выдержит противостояния с леопардом и всегда будет жертвой» [3].

– *Реклама УТП* – суть реклам конкурентов в войне сводиться к демонстрации своих уникальных торговых предложений (УТП). *BMW* на рекламу о русифицированной системе навигации *GPS* от *Audi* сделали следующее рекламное сообщение, выделив свое УТП: «Пока другие переводили навигацию, мы сделали лучший в мире двигатель. Настоящий шедевр современного искусства. 6-цилиндровый 3-литровый двигатель *Twin Turbo* – лучший двигатель 2007 года».

– *Ценовая аргументация* – атака или контратака с использованием ценовых аргументов.

– «*Селебрити*» (от англ. *celebrity* – «знаменитость», «звезда») – использование в рекламных сообщениях войны обращения знаменитостей, медиаперсон, *VIP* и т. д.

Как правило, если один бренд в своей атаке использует, к примеру, стратегию косвенной «насмешки», то контратакующий (защищающий себя) бренд тоже придерживается этой стратегии, как бы в отместку. Таким образом, чаще всего атакующий бренд задает стратегию поведения всем участникам рекламной войны.

Однако, что касается рекламных войн в России, прямое сравнение рекламируемого товара с товарами другого бренда считается недобросовестной рекламой, в отличие от других стран [4].

### **Список используемых источников**

1. **Стоит** ли начинать рекламную войну [Электронный ресурс] // Advsmile.ru: портал рекламы и PR. – URL: <http://www.advsmile.ru/istorii-na-advsmile/rasskazhem-o-reklamnyih-voynah/stoit-li-nachinat-reklamnyu-voynu.html> (Дата обращения: 27.11.2013).
2. **Война** брендов [Электронный ресурс] // Adme.ru: сайт о творчестве. – URL: <http://www.adme.ru/kreativnyj-obzor/vojna-brendov-261055> (дата обращения: 28.11.2013).
3. **Рекламная** война как эффективная стратегия продвижения бренда [Электронный ресурс] / Г. А/ Мирошниченко // Kafedramk.ru: сайт каф. масс. коммуникаций Российского университета дружбы народов. – Москва, 2012. – URL: <http://www.kafedramk.ru/content/reklamnaya-vojna-kak-effektivnaya-strategiya-prodvizheniya-brenda> (дата обращения: 27.11.2013).
4. **Федеральный** закон от 13 марта 2006 г. № 38-ФЗ «О рекламе» // Собрание законодательства Российской Федерации. – 2006. – № 12. – Ст. 1232.

*Статья представлена научным руководителем,  
канд. полит. наук, доцентом И. Г. Чередовым.*

**УДК 811.111**

**М. М. Заливина (студентка группы СР-12 СПбГУТ)**

## **СЛОВА-ПАРАЗИТЫ В СОВРЕМЕННОМ АНГЛИЙСКОМ ЯЗЫКЕ**

Данная работа посвящена изменениям в современном английском языке. Она акцентирует внимание на словах, которые являются очень популярными не только в Соединенных Штатах Америки (США) и Великобритании, но и во всем мире. То, как они используются в современном языке, отличается от нормы. Основная цель этой статьи – показать на примерах из современной художественной литературы такие метаморфозы.

Начнем с одного из самых популярных слов в мире – О'К. Существует много теорий о его возникновении. Согласно одной из них, выражение О'К появилось как аббревиатура в бостонской газете в 1839 году. Оно означало “all correct”, но было написано как “oll correct”, т. е. неправильно написанное «всё правильно».

С усилением роли современных технологий в нашей жизни оно распространилось по всему миру с помощью программного обеспечения корпорации Microsoft и Apple Inc., так как в большинстве программ слово “OK” используется для подтверждения операции. Кроме того, общение в Интернете и переписка с помощью мобильного телефона заставляют людей использовать сокращения для упрощения набора сообщения и уменьшения его размера.

Говоря о применении слова «OK», следует заметить, что носители английского языка часто используют его неправильно и неуместно, зачастую злоупотребляя им. Аббревиатура «OK» является очевидным символом американского «позитивного мышления», она часть их национального самосознания, поэтому США, вероятно, является единственным местом, где оно используется по назначению [1].

Когда же использование данного слова уместно?

Во-первых, это ответ на вопрос “How are you?” – Как дела? В значении «нормально», «хорошо», «неплохо».

– ““But you’re *okay*, Ginny”, said Ron, beaming at her. ‘It’s over now...’” (Harry Potter and the Chamber of Secrets. J. K. Rowling.)

Во-вторых, вы можете ответить OK, чтобы подтвердить уже заранее согласованную договоренность.

– ““*OK*,” Ron sighed, as though resigned to the worst, ‘I’m ready. Let’s go.’”

– ““*It’s OK*, Hermione,” said Harry quickly. ‘We’ll take you up to the hospital wing.’”

– ‘*OK*, we’ll just have to check on it every half an hour or so.’

(Harry Potter and the Chamber of Secrets. J. K. Rowling.)

В-третьих, OK используется, когда говорящий задает вопрос или обращается с просьбой, ожидая положительного ответа.

Более того, OK может также означать согласие, но при наличии каких-либо обстоятельств или ограничений, которые должны непременно учитываться.

– ‘All right, we’ll do it. But not toenails, *OK*?’ (Harry Potter and the Chamber of Secrets. J. K. Rowling.) [2].

Иногда OK выражает раздражение или неудовольствие говорящего тем, что собеседник морочит ему голову. В этом случае это слово-паразит повторяется несколько раз.

Кроме того, OK как вопрос может быть использован со значением «Вы меня поняли?», «Вам все ясно?».

И, наконец, американцы обращаются к человеку, у которого возникли проблемы, не так, как русские: «Вам нужна помощь?», а, в соответствии с американским «позитивным мышлением», они спрашивают: «Все ли с вами хорошо?» – “Are you OK?”.

– ““Are you *OK*? Harry said urgently.” (Harry Potter and the Chamber of Secrets. J. K. Rowling.) [2].

Еще одно очень популярное слово-паразит – это слово “like”, его значение схоже с русским «как бы». В основном оно используется, чтобы смягчить суждение, показать неопределенность, неуверенность.

– I was *like*, exhausted, *like* really, really tired.

Кроме того, его можно услышать, когда говорящий преднамеренно не желает передавать точную информацию, подчеркивая приблизительность приводимых им данных.

- He was *like*, 50 years old.

Более того, “like” служит чем-то вроде устных кавычек, помогает передать разговор, как при косвенной речи. Но есть проблема, связанная с тем, что like порождает неясность в разговоре, так как неясно, является ли реплика словами или мыслями самого говорящего.

- She's *like*, so where are you going on vacation? And I'm *like*, well, we're probably going to California [3].

Представляется очевидным, что “like” используется для замены современных разговорных конструкций и выражений и является явным показателем низкого уровня образования и безграмотности говорящего.

Еще одно слово-паразит, которое используется для неточного выражения мысли, – это “whatever”. В прошлом значение этого слова было совершенно ясным и определенным. “Whatever” означало только «все, что бы то ни было». Но в последнее время оно приобрело несколько новых значений, которые полностью отличаются от первоначального.

Например, “whatever” показывает отказ лица продолжать свою речь, это синоним «Все. Я все сказал», оно ставит точку в разговоре.

- So we're going to cut taxes and everything will be fine. *Whatever*.

Другая ситуация, когда человек не хочет вдаваться в детали, хочет побыстрее сказать самое важное, оставляя в стороне то, что является неважным и неактуальным.

- He talked about his plans for national health care, including insurance, the hospital system, outpatient clinics, *whatever*.

Последнее новое значение слова “whatever”, но не реже используемое – «мне абсолютно все равно», «какая разница». В этом случае говорящий показывает, что он совершенно равнодушен к происходящему.

- He says all kinds of things with which I really disagree. It doesn't really matter, *whatever*.

Стоит также добавить, что слово “whatever”, когда оно используется в одном из современных значений, ставится в конце предложения [2].

Еще одно очень популярное слово-паразит, которое использовалось в основном среди подростков и людей с низким уровнем образования, – “you know”. Оно появлялось везде и не имело никакого особого значения.

Но теперь оно используется также среди высокообразованных людей, даже политиков. Эта тенденция вызывает довольно отрицательную реакцию у американской публики, включая избирателей, потому что это признак слабости, неуверенности и уязвимости говорящего.

- ‘Well, I'll be off, plenty to do, you know.’
- ‘Father's got a lot of influence, you know.’

– ‘But – Professor, my aunt and uncle – you know, they’re Muggles’  
(Harry Potter and the Prisoner of Azkaban. J. K. Rowling.) [4].

Стоит упомянуть и фразу “kind of”, которая, помимо своего традиционного значения, приобрела еще несколько новых. Использование ее смягчает высказывание, делает его менее категоричным, иногда снижая ответственность говорящего за свои слова.

– ‘Well, when it works correctly, it conjures up a Patronus,’ said Lupin,  
‘which is a kind of Anti-Dementor – a guardian which acts as a shield between  
you and the Dementor.’

– ‘I suppose there must be some kind of mouth under there, because they  
clamp their jaws upon the mouth of the victim and – and suck out his soul.’  
(Harry Potter and the Prisoner of Azkaban. J. K. Rowling.) [4].

Однако, фраза “kind of” также часто заполняет «пустоту», когда человек попросту не может подобрать правильные слова, чтобы объяснить что-то. Оно переводится как «что-то типа», «в этом роде», «что-то похожее».

Следует заметить, что современные англоязычные культуры отличает достаточно высокая терпимость к сквернословию, причем, среди образованных носителей английского языка. Как полагает Т. В. Ларина «Это явилось следствием демократизации общества, что нашло отражение в демократизации речи. То, что сейчас происходит в современном английском языке, можно охарактеризовать как изменение языкового престижа», то есть изменения в коммуникации происходят снизу вверх. Часто ненормативная лексика также используется как слова-паразиты, заполняя паузы, а не только выступает в эмоционально-экспрессивной функции. Одно из «мягких» выражений – “damn it”, которое можно услышать даже из уст ребенка [5].

Еще одной особенностью сегодняшнего английского языка является стратегия переоценки, т. е. частое использование оценочной лексики в гиперболизированном значении. Это некоторым образом повлияло и на расширение спектра слов-паразитов. Так, слово *absolutely* часто встречается в речи американцев совсем не в истинном своем значении и может служить даже фразой согласия или для заполнения паузы, когда коммуникант попросту не может определиться с ответом.

В заключение хотелось бы повторить, что упомянутые слова и фразы являются не только показателем некатегоричности, столь характерной для английского языка, но часто выступают как слова-паразиты, что является показателем низкого уровня образования, неумения точно выразить мысль, нерешительности и неуверенности. Таким образом, следует избегать использования таких слов в своей речи, стараться выражать свои мысли точно и ясно.

### Список используемых источников

1. Русские проблемы в английской речи. Слова и фразы в контексте двух культур / Линн Виссон; пер. с англ. Изд. 6-е, стереотипное. – М. : Р. Валент, 2013. – 192 с.
2. Harry Potter and the Chamber of Secrets / J. K. Rowling. – London : Bloomsbury, 2010. – 366 р.
3. Слова – хамелеоны и метаморфозы в современном английском языке / Линн Виссон. – М. : Р. Валент, 2010. – 160 с.
4. Harry Potter and the Prisoner of Azkaban / J. K. Rowling. – London : Bloomsbury, 2010. – 468 р.
5. Англичане и русские: язык, культура, коммуникация / Т. В. Ларина. – М. : Языки славянских культур, 2013. – 360 с.

*Статья представлена научным руководителем, доцентом Т. П. Савельевой.*

**УДК-94**

**Т. А. Захаренко (студентка группы СР-01 СПбГУТ)**

### **НЕЙТРАЛИТЕТ КАК ИНСТРУМЕНТ ШВЕДСКОЙ ВНЕШНЕЙ ПОЛИТИКИ В ПЕРИОД «ХОЛОДНОЙ ВОЙНЫ» с 1949 по 1969 гг.**

В работе рассматриваются понятие «нейтралитет», его виды и особенности шведского нейтралитета на фоне общепризнанных международно-правовых стандартов прав и обязанностей государства с нейтральным статусом. Приводятся примеры уклонения от провозглашенной политики, как в военное, так и в мирное время. Представлены мнения различных правящих партий Швеции по вопросу о необходимости сохранения и соблюдения нейтралитета.

Ключевые слова: нейтралитет, Швеция, свобода от альянсов, «холодная война», НАТО, план Marshalla.

Шведский нейтралитет был и остается довольно популярной темой для обсуждения. Историки, занимающиеся изучением данного вопроса, не могут прийти к единому мнению. Можно ли назвать внешнеполитический курс Швеции нейтральным или он все же не вписывается в критерии понятия нейтрального государства в международном праве. К сожалению, среди наших соотечественников мало историков, которые посвятили свою деятельность теме Шведского нейтралитета. Но нельзя не отметить труды Александра Сергеевича Кана, которого называют мэтром отечественной скандинавистики. Он является автором сотен статей и нескольких монографий по истории и историографии стран Северной Европы и советско-скандинавских отношений XX в. И Олега Ивановича Тиунова, доктора юридических наук, профессора, который в своих трудах «Нейтралитет в

международном праве» и «Принцип соблюдения международных обязательств» очень подробно исследует предмет нейтралитета, его виды, а также права и обязанности нейтрального государства, соответственно виду его нейтрального статуса (временный, постоянный или позитивный).

Целью данной работы является изучение особенностей шведского нейтралитета на фоне общепризнанных международно-правовых стандартов прав и обязанностей государства с нейтральным статусом.

Понятие нейтралитета в рамках международного права включает в себя такой вид внешней политики государства, при котором оно не принимает чью-либо сторону в случае вооруженных конфликтов между другими государствами или военными противоборствующими блоками. Отношения между воюющими и нейтральными государствами регламентируются пунктами 5 и 13 Гаагской конвенции 1907 года [1].

Принято выделять два вида нейтралитета: временный (нейтралитет во время войны) и постоянный. Но иногда встречается определение третьего вида – позитивный нейтралитет.

Главной обязанностью временно нейтрального государства является его безоговорочное неучастие в войне. Оно должно применять одинаковые запретные или ограничительные меры к обеим сторонам конфликта. Отсюда следует вся трудность положения и ответственность такого государства, так как «даже малейшее с его стороны пренебрежение своими обязанностями не может сработать в пользу одного из воюющих».

Значительную роль в поддержании мира играет постоянный нейтралитет, при котором государство, принявшее такой статус, обязано не только не участвовать в военных конфликтах, но и в мирное время проводить соответствующую политику, препятствующую вовлечению его в междоусобицы других государств, а именно: «Не вступать в военные союзы, не разрешать размещения на своей территории иностранных баз, не оснащать свою армию оружием массового уничтожения, а также бороться за мир и мирное сосуществование государств» [2]. Швейцария стала первым государством со статусом постоянно нейтральной державы.

Под позитивным нейтралитетом принято понимать внешнеполитический курс государства, основанный на стремлении сохранить мир и национальный суверенитет. Позитивный нейтралитет существует только в мирное время, поэтому государства, которые проводят такую политику, не обязаны оставаться нейтральными в случае начала войны.

Шведский нейтралитет. История и особенности.

Вот уже 200 лет Швеция не принимала участия в военных конфликтах. Иногда этот успех в избегании войн приписывают длительной и целеустремленной политике нейтралитета, основу которой заложил король Карл XIV Юхан еще в первой трети XIX века. Но это объяснение неполно. В некоторых случаях скорее геополитические обстоятельства или счастливая случайность позволили Швеции остаться в стороне от военных собы-

тий. Только после Второй мировой войны Швеция официально провозгласила нейтралитет в качестве официальной линии своей политики безопасности. Это решение стало важной частью национальной шведской идентичности в послевоенный период.

В «идентичности» шведского нейтралитета сомневаться не приходится. Главной его особенностью является его неоднозначность.

В период Второй мировой войны Швеция объявила себя нейтральным государством, что в военное время предполагало обязанность правительства никоим образом не оказывать содействие какой-либо из сторон. При этом шведское государство проводило плохо прикрытую прогерманскую политику, которая выражалась, например, в экспорте железной руды и шарикоподшипников для немецких оружейных заводов [3].

Неоднозначность шведского нейтралитета проявлялась впоследствии и в период «холодной войны».

После Второй мировой войны ситуация на международной арене изменилась. В связи с победой Союза Советских социалистических Республик (СССР) над Германией, союзники, в том числе и Соединенные Штаты Америки (США) боялись усиления коммунистического влияния на другие страны, а, следовательно, еще большей значимости Советского Союза на международной арене. Даже на шведских послевоенных выборах в парламент коммунисты добились лучшего результата за всю историю, получив 10 % голосов.

И все же в Швеции с ее признанным социально-демократическим режимом с осторожностью относились к приверженцам советских коммунистических взглядов и предпочитали держаться поближе к США, которые находили поддержку в сфере шведской экономики, а также в консервативных и либеральных партиях.

Согласно официальной политике Швеции, она должна была придерживаться курса неприсоединения к силовым альянсам сверхдержав. Шведский девиз можно сформулировать так: «Свобода от альянсов, нацеленная на нейтралитет в войне». Свобода от альянса – политика неприсоединения государства к силовым блокам с целью сохранения нейтрального статуса в случае войны [4]. Это понятие следует отличать от определения «нейтралитет», поскольку «нейтралитет» в контексте международного права не может существовать отдельно от конкретной конфликтной ситуации. Тем не менее, в экономическом и культурном отношении Швеция все же принадлежала к западной сфере влияния США. А также наравне с официальной политикой нейтралитета Швеция вступила в тайное сотрудничество с НАТО и одобрила американский план Marshalla. Это означало, что теперь она была привязана к системе рыночной экономики США.

На самом деле нет ничего удивительного в том, что Швеция сблизилась с Западом. Они были схожи как в идеологическом, так и в культурном плане. СССР же они наоборот опасались, частично из-за коммунистиче-

ской идеологии, частично из-за старой вражды с Россией, вызванной многовековым противостоянием в регионе Балтийского моря. А за счет тесного сотрудничества с НАТО государство могло рассчитывать на его помощь в случае захвата Швеции Советским Союзом, не имея при этом обязательств перед НАТО в обратной ситуации.

Тот факт, что Швеция экономически, идеологически и культурно была близка с НАТО и в отношении политики безопасности рассчитывала на поддержку Североатлантического альянса, не мешало ей высказывать критику в адрес действий США. Премьер-министр Улоф Пальме открыто критиковал деятельность США в войне во Вьетнаме в конце 1960 – начале 1970 годов. В то же время он продолжал сотрудничество с НАТО. Таким образом, можно прийти к выводу, что внешняя политика для Швеции была одним делом, а политика безопасности – совсем другим.

И даже сейчас у политиков нет единого мнения по вопросу о нейтральной политике Швеции. Можно выделить, по меньшей мере, три различных точки зрения по поводу того, как Швеция должна вести себя в случае возможного кризиса или войны.

Партия «левых», партия «зеленых» и партия «центра» считают, что шведский нейтралитет в любой подобной ситуации должен оставаться неколебимым.

В дебатах по поводу шведской политики безопасности стремление к нейтралитету зачастую сопоставляют с безразличием к развивающимся в мире событиям. Партия «умеренных» и «народная» партия считают, что Швеция должна иметь возможность выбирать в зависимости от ситуации, придерживаться ли ей политики невмешательства или нет. Представители этих партий уверены, что в случае военной угрозы одной из стран Европейского Союза (ЕС), Швеция вряд ли сможет остаться безучастной. «Умеренные» в противном случае сочли бы нейтралитет проявлением трусости, изолированности и уклонением от ответственности [5].

Тем временем социал-демократы утверждают, что нейтралитет – это самый вероятный выбор для Швеции в случае войны. Социал-демократы не согласны с мнением, что нейтралитет равносителен безразличию. Они уверены, что в случае военных конфликтов одной из стран ЕС с другим государством, Швеция сможет оказать содействие, например, пропагандой, посредничеством или политической поддержкой миротворческих сил как внутри, так и за пределами зоны конфликта, не выходя при этом за рамки нейтрального статуса. Согласно мнению социал-демократической партии Швеции, нейтралитет вполне возможно комбинировать с интернационализмом и операциями по поддержанию мира.

Едва ли возможно объединить все три позиции по данному вопросу. Швеция не может с одной стороны утверждать, что страна сохранит нейтральный статус в случае войны, а с другой стороны, что политика нейтралитета – это всего лишь один из возможных вариантов. Лишь одна

точка зрения должна стать официальным направлением шведской внешней политики.

#### **Список используемых источников**

1. **The Hague**, 18 October 1907. Convention (V) relative to the Rights and Duties of Neutral Powers and Persons in case of War on Land. Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War.
2. **Нейтралитет в международном праве** / О. И. Тиунов. – Пермь, 1986 – С. 4.
3. **Mein Lieber Reichskanzler!** / Staffan Thorsell. – Bonnierförlagen Press, 2007 – S. 7.
4. **Sveriges säkerhetspolitik** [Электронный ресурс]. – Режим доступа: <http://www.sakerhetspolitik.se> (Дата обращения: 25.03. 2014).
5. **Urikespolitiken** som slagfält. De svenska partierna och utrikesfrågorna / Ulf Bjereld och Marie Demker. – Stockholm : Nerenius&Santerus, 1995 – S. 237.

*Статья представлена научным руководителем, ассистент А. Б. Гехт.*

**УДК 159.9**

**Т. Б. Золотова (студентка группы ИКТ 304 СПбГУТ)**

## **ВЛИЯНИЕ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА НА СТАНОВЛЕНИЕ И РАЗВИТИЕ ЛИЧНОСТИ**

Существует множество определений информационного пространства. Но одна из самых доступных и точных формулировок такова: «Информационное пространство представляет собой совокупность объектов, вступающих друг с другом в информационное взаимодействие, а также сами технологии, обеспечивающие это взаимодействие» [1].

Информационное пространство образуется информационными ресурсами, средствами информационного взаимодействия и информационной инфраструктурой. Оно имеет своим центром субъект, который в процессе своей деятельности создает информацию, присваивает ее, накапливает и передает. Таким субъектом может выступать человек или социальная группа, а также компания, орган государственного управления – любой, кто в ходе осуществления деятельности использует возможности современных информационных технологий. В любом случае информационное пространство не может существовать без деятельности человека, то есть без личности, на которую должно влиять современное информационное пространство.

Рассмотрим, как это происходит.

В век компьютеризации ребенок быстро осваивает работу гаджетов, благодаря их простому интерфейсу дошкольник может спокойно включить компьютер или запустить игру на телефоне. Но наибольшее количество времени дети проводят у телевизора. Долгое пребывание у телеэкрана, нередко в полном спокойствии, объясняется тем, что ребенок полностью сконцентрирован на быстро меняющейся картинке, ему сложнее, чем взрослым, воспринимать смену кадров и информацию, заключенную в них. Столь сильное напряжение может послужить причиной к раздражительности, быстрой утомляемости, в некоторых случаях неупорядоченной разрядке неизрасходованной активности. Многие врачи и психологи советуют допускать ребенка к просмотру телевидения не более чем на 20 минут в день [2]. Давайте рассмотрим актуальность этой рекомендации. Мы живем в век современных технологий, в котором кинофильмы и мультипликация являются важной составляющей жизни. Дети воспитываются с их помощью, что нередко дает положительные результаты. Благодаря познавательным программам ребенок получает интересную информацию в доступной форме, из мультфильмов узнает сценарии жизненных ситуаций, поведенческие нормы и так далее. На данный момент существует множество фильмов (игровых, мультипликационных, научно-популярных), снятых с учетом особенностей детской психики в разном возрасте. Из всего вышесказанного можно сделать заключение: совет психологов не актуален и трудновыполним в наше время, нужно искать пути эффективного использования современных технологий в вопросе воспитания ребенка. Для положительного влияния телевидения на ребенка стоит отбирать фильмы, которые будет смотреть ребёнок в младшем возрасте, договариваться о времени просмотра кинокартин с подросшими людьми, делать перерывы, гимнастику для глаз, чаще гулять...

В 6–7 лет ребенок идет в школу. Идя первый раз первый класс, будущие ученики, как правило, уже имеют представление о том, что такое школа. Это представление зачастую сформировано под влиянием мультфильмов, что является причиной нередкого разочарования в учебном процессе. В фильмах, как известно, используют самые яркие моменты. Как говорил американский кинорежиссер Альфред Хичкок, «Кино – это жизнь, из которой вырезано всё скучное».

И вот шести-семи летние люди идут в храм знаний, куда они так мечтали попасть, где, как им кажется, их ждут совсем небольшие уроки (мелькнувшие лишь на пару секунд на экране) и, главное, бесконечные перемены, на которых и будет происходить все самое интересное, а учителя непременно будут либо очень злыми и враждебными, либо добрыми и во всём помогающими наставниками, где без сомнений будут звезды класса и неудачники... Все это чётко вырисовывается в воображении. И вот они видят таких же детей, отсиживают долгие уроки, а потом еще и домашнее задание, да и учителя оказываются какими-то «неправильными». У всех по-

разному, но в среднем первоклассник разочаровывается в школе на втором-третьем месяце обучения [3]. Бессспорно, причиной этому служат не только обманутые ожидания, но они, как правило, являются основой.

Проблема «обманутого ожидания» не покидает человека и в более зрелом возрасте. Конечно, со временем индивидуум осознает, что сюжеты историй с экрана и страниц книги крайне редко материализуются в нашем мире, но подсознание никак не хочет забывать сказки про Емеля и Ивана-дурака.

Важнейшими проблемами, возникающими благодаря современному информационному пространству, являются стремление к несуществующим идеалам и множественные комплексы. Эти два понятия недаром стоят рядом, ведь одно прямо вытекает из другого. Средства массовой информации настойчиво внушают нам, что всегда нужно быть победителем, нужно делать все идеально, быть идеальным: «Посмотри, ведь это так несложно! Мы покажем, что красиво, а что нет, каким быть правильно, а каким просто непозволительно». Наглядным примером является всем известная кукла Барби с ее неестественными параметрами лица и тела, которые фиксируются в качестве эталона красоты уже в детском подсознании. Девочки с малого возраста пытаются соответствовать своему «кумиру», в результате чего в современном западном обществе остро всталась проблема борьбы с анорексией. Школьницам постоянно кажется, что они страдают избыточным весом, они стараются ограничивать себя в еде, а то и вовсе отказываются от пищи и попадают в клиники с серьезными физическими и психическими нарушениями. Психологи полагают, что кукла Барби способствует формированию у подрастающего поколения девочек комплекса неполноценности в целом (лицо и тело реальной живой женщины не могут соответствовать «стандартам Барби») [4]. Не так давно поднялась волна возмущений по поводу того, что американские мультфильмы некоторой мультипликационной компании показывают матерей пожилыми, тем самым пропагандируя позднее деторождение. И уже в нашем обществе нередко суждение, что появление ребенка – это крест на карьере и хорошей жизни. Ребенок часто воспринимается как помеха, фактор, который мешает добиться успеха. Давление средств массовой информации и других источников мешают чувствовать себя полноценным, слушать свой внутренний голос, заниматься тем, что любишь, ведь это может пошатнуть твой будущий социальный статус, понизить в глазах общества, отдалить от идеала, от совершенства. В итоге возникает проблема, которую нередко ставят рядом с ленью, – прокрастинация. Ведь за хроническим «я сделаю это завтра» стоят страх неуспеха, боязнь оценки и сложность выбора.

Таким образом, выше были перечислены некоторые из отрицательных последствий влияния современного информационного пространства на становление и развитие личности, но это лишь одна, отрицательная, сторо-

на, не стоит забывать и о положительной. Интернет подарил людям возможность получать самые свежие новости и информацию.

С помощью видеоконференций люди могут решать важные вопросы, не меняя своего рабочего места и экономя как свои средства, так и время.

В интернете или газете можно найти информацию о работе, которая будет высоко оплачиваться и приносить удовольствие. Можно узнать последние новости, высказать свое мнение по волнующему вопросу.

Глобальная сеть позволяет лучше узнать мир и дает возможность людям сблизиться.

Не стоит забывать и об инвалидах, людях, которые не имеют возможности реального контакта с другими людьми. Интернет позволяет общаться с соотечественниками и людьми, живущими в других странах, что даёт возможность изучить культуру, нравы, историю других государств.

Интернет дает огромные возможности для образования, ведь в нем можно оперативно найти информацию, которой нет в библиотеках.

Можно долго перечислять положительные и отрицательные стороны влияния современного информационного пространства. Эра компьютерных технологий дает нам огромные возможности, доступ к терабайтам информации, задаёт новые тенденции. Вместе с этим идёт пропаганда ложных жизненных ценностей. У людей возникает зависимость от интернета, прокрастинация и многое другое. Таким образом, информационное пространство имеет как положительную, так и отрицательную сторону. Необходимо, не подпадая под его негативное влияние, стараться получать максимальную пользу из поступающей извне информации.

### **Список используемых источников**

1. **Информационное** пространство полиглоссических регионов России: Векторы развития [Электронный ресурс] / Я. В. Кудашкин, С. Ш. Маринова. – URL: <http://lomonosov-msu.ru/rus/event/1087> (Дата обращения 20.04.2014).
2. **Оттащите** ребенка от телевизора [Электронный ресурс] / Е. В. Чиркова. – URL: [http://missus.ru/articles/family/kids/25-02-2011/tv\\_kid\\_danger/](http://missus.ru/articles/family/kids/25-02-2011/tv_kid_danger/) 5867 (Дата обращения 20.04.2014).
3. **Трудности** первоклассника – первые месяцы в школе [Электронный ресурс] / М. Б. Серед. – URL: <http://sosed-domosed.ru/trudnosti-pervoklassnika/> (Дата обращения 20.04.2014).
4. **Глобализация** идеалов красоты и этнокультурная специфика / Л. Бунтовская. – М. : Век 2. Серия: Наука для всех. 2004г., Scan&Read "Русколань". – 230 с.

*Статья представлена научным руководителем,  
канд. филос. наук, доцентом М. Р. Зобовой.*

УДК 37.032

**А. С. Крылов (студент группы МТ-01 СПбГУТ)**

## **ШАХМАТЫ КАК СРЕДСТВО ВОСПИТАНИЯ ИНЖЕНЕРНОЙ МЫСЛИ**

Взаимоотношения науки и шахмат сложны и не совсем однозначны. Особенности логики рассуждений, творческих поисков, интуиции в подготовке решения в шахматах и науке близки. Попробуем разобраться подробнее. Начнем с качеств шахматиста: смелость в принятии решений, самодисциплина, точность расчета, хорошая память, трудолюбие, самоконтроль, умение признавать свои ошибки и недостатки, делать из этого выводы и самосовершенствоваться... Данные качества развиваются при игре и занятиях шахматами. Ведь шахматы не только игра. Еще в начале двадцатого века мудрый Эммануил Ласкер сказал, что «если бы шахматы были просто игрой, то они никогда не пережили бы тех серьезных испытаний, которым отчасти подвергались за долгое время своего существования» [1, 11].

Вопреки распространенному мнению для хорошей игры в шахматы не обязательно иметь математический склад ума или рвение лишь к точным наукам, поскольку «логика шахмат не математического свойства» – Э. Ласкер [1, 180], но для развития в себе инженерной мысли, в частности это касается научных и теоретических аспектов, очень помогут качества присущие хорошему игроку в шахматы. Академик Иван Матвеевич Виноградов – крупнейший специалист в области аналитической теории чисел считал, что «ученому и вообще человеку умственного труда шахматы просто необходимы» [2, 77].

Современный инженер (инженер связи) должен быть эрудирован, причем не только в своей области, он должен быстро и точно принимать решения по поставленным задачам, иметь хорошие нервы. Помимо этого, инженер должен творчески подходить к своему делу.

Рассмотрим наиболее важные аспекты в области пересечения качеств инженера и шахматиста: а) точность мышления и расчетов; б) самоанализ и самокритичность; с) эрудиция и хорошая память; д) смелость в принятии решений; е) творческая составляющая. Теперь попробуем установить связь шахматист – инженер между данными качествами.

Точность расчета и мышление в шахматах не может напрямую влиять на решение каких-либо инженерных задач, так как окончательные цели здесь различны. Но по словам великого шахматного игрока и мыслителя Эммануила Ласкера: «Главное – это постичь метод» [1, 25], и тут шахматная и инженерная мысли совпадают. Путем решения шахматных задач (хочется напомнить, что в данном случае нас интересует метод, а не

конечная цель) можно натренировать свой мозг, который будет быстро и точно рассчитывать различные возможности при любых видах деятельности, в том числе и при расчетах инженерных задач и моделей. Тринадцатый чемпион мира по шахматам Гарри Кимович Каспаров: «Если вы спросите гроссмейстера, художника или компьютерного специалиста, что характерно для хорошего шахматиста, то поймете, почему шахматы являются идеальной лабораторией для отработки процесса принятия решений» [3, 27].

В жизни и в любой деятельности человек не добьется успеха, если не будет самокритичен к себе, не будет анализировать свои действия и поступки. Добросовестный инженер должен знать свои недостатки и устранять их по мере возможности, чтобы они не отражались на качестве его работы. Важно делать правильные выводы и уметь направить свои силы для самосовершенствования, стремясь нивелировать свои слабые стороны. Именно шахматы помогают развивать в себе данные качества, ведь в шахматах винить кого-либо в своих поражениях бессмысленно. По мнению Г. К. Каспарова: «Путь к наивысшим достижениям лежит через самопознание и глубокое постижение смысла и значения всего достигнутого ранее. Лишь это дает возможность осмысленно принимать ответственные решения и наилучшим образом использовать свои знания, опыт и талант» [3, 20].

Шахматная эрудиция как таковая не может влиять на эрудицию инженера, поскольку области знаний слишком различны, но шахматная эрудиция не возможна без хорошей тренированной памяти, которая в свою очередь является основой для расширения объема знаний и длительного запоминания. В данном случае шахматы косвенно влияют на эрудицию инженера посредством развития памяти. Международный гроссмейстер, доктор психологических наук Николай Владимирович Крогиус: «Шахматы требуют хорошей памяти и активно стимулируют ее развитие. Однако бытует ошибочное представление о том, что шахматист, в основном, опирается на буквальное запоминание вариантов или позиций. Эксперименты, проведенные А. Бинэ (Франция) и П. Рудиком, а также другими учеными, убедительно продемонстрировали, что у шахматистов превалирует не механическое, буквальное запоминание, а логическое, смысловое. Итак – память шахматиста рассудочна. И шахматы прежде всего стимулируют развитие этого качества» [4, 272]. Можно сделать вывод, что влияние шахматной эрудиции на эрудицию инженера хоть и косвенное, но очень продуктивное.

Грамотный инженер должен принимать правильные и точные решения, причем зачастую это необходимо делать в условиях недостатка времени, когда каждая секунда на счету. Шахматы наглядно демонстрируют отрицательные последствия неверного планирования затрат времени, запаздывания и несвоевременности действий. «Очень

важна ясность цели в постановке задачи, умение найти короткий и рациональный путь решения» – Михаил Моисеевич Ботвинник [5, 197]. Эстетические ценности шахмат близки эстетике научных достижений: логичность, экономичность, оригинальность решений, поэтому шахматная игра прекрасно помогает логично решать проблемы, воспитывает смелость в принятии решений, учит быстрому и точному расчету различных вариантов и альтернатив. Шахматы дают возможность делать правильные выводы после всех проведенных операций, таким образом минимизируется возможность ошибочного решения той или иной задачи. По словам Н. В. Крогиуса, «результаты научных исследований и данные из практики обучения шахматам убедительно свидетельствуют о полезном влиянии шахмат на развитие интеллектуальных функций» [4, 270].

Тяжело представить работу инженера без творческой составляющей, поскольку необходимо привносить что-то новое в свою работу, нельзя стоять на месте. Умение нестандартно и разносторонне мыслить, умение применять свою фантазию – все это необходимо для инженера, стремящегося к развитию, и не желающего оставаться на определенном этапе своей деятельности. Шахматы лучше всего помогут в этом, ведь они оказывают самое благотворное влияние на умственную деятельность не перегружая ее, стимулируют развитие воображения, способность к предвидению и фантазии, но излишнее фантазирование и легкомыслие недопустимы: необходимо принимать решения, исходя из реальной обстановки. Петр Леонидович Капица говорил, что «Игра в шахматы как бы прочищает мозги от всех мыслей, накопившихся за день» [2, 68]. Шахматы никогда не дадут стоять на месте, а всегда помогут росту мышления. Но для этого тоже необходимо приложить усилия, нужно перебороть свои слабые стороны и еще больше совершенствовать сильные качества и шахматы будут лучшим помощником для вас. Гроссмейстер Крогиус писал, что «шахматы допустимо рассматривать в качестве своеобразного тренажера творческих способностей человека» [4, 280].

Общее значение шахмат для жизни и познания удачно выразил доктор филологических наук, профессор Владислав Антонович Ковалев: «И, наконец, шахматы – очень хороший вид отдыха. С шахматами не страшно одиночество. Любое общение с ними доставляет большую радость интеллектуального обогащения» [2, 59].

#### Список используемых источников

1. Здравый смысл в шахматах / Э. Ласкер. – М. : Современные проблемы, 1925. – 186 с.
2. Шахматы в жизни ученых / С. Я. Гродзенский. – М. : Наука, 1983. – 168 с.
3. Шахматы как модель жизни / Г. К. Каспаров. – М. : Эксмо, 2007. – 184 с.
4. Шахматы. Игра и жизнь / Н. В. Крогиус. – Ростов-на-Дону: Феникс, 2011. – 375 с.

5. Полвека в шахматах / М. М. Ботвинник. – М. : Физкультура и спорт. – 1978. – 272 с.

*Статья представлена научным руководителем  
канд. филос. наук, доцентом П. Ю. Нешитовым.*

**УДК 654.739**

**Ю. А. Попова (студентка группы ИКТ-307 СПбГУТ)**

## **ПРИМЕНЕНИЕ МЕТОДОВ МОТИВАЦИИ В УПРАВЛЕНИИ ОРГАНИЗАЦИЕЙ**

Управление персоналом включает многие составляющие. Среди них: кадровая политика, взаимоотношения в коллективе, социально-психологические аспекты управления. Ключевое же место занимает определение способов повышения производительности, путей роста творческой инициативы, а также стимулирование и мотивация работников.

Ни одна система управления не станет эффективно функционировать, если не будет разработана эффективная модель мотивации, так как мотивация побуждает конкретного индивида и коллектив в целом к достижению личных и коллективных целей.

Мотивация персонала – это стимулирование к деятельности, процесс побуждения к работе, воздействие на поведение человека для достижения личных, коллективных и общественных целей [1].

Рассмотрим виды мотивов к труду [1]:

а) мотив социальности (потребность быть в коллективе);  
б) мотив самоутверждения характерен для значительного числа работников, преимущественно молодого и среднего возраста. По мнению Герцберга, он является собственно мотивирующим фактором для сотрудников высокой квалификации;

в) мотив самостоятельности;  
г) мотив надежности (стабильности);  
д) мотив приобретения нового (знаний, вещей и т. д.);  
е) мотив справедливости;  
ж) мотив состязательности как основа организации.

Наиболее часто встречающаяся модель мотивации имеет три элемента [2].

1) Потребности, стремление к определенным результатам. Люди испытывают потребность в таких вещах как одежда, дом, личная машина и

т. д., но также и в «неосозаемых» вещах как чувство уважения, возможность профессионального роста и т. д.

2) Целенаправленное поведение. Люди, стремясь удовлетворить свои потребности, люди выбирают свою линию целенаправленного поведения. Работа в организации – один из способов целенаправленного поведения. Попытки продвинуться на руководящую должность – еще один тип целенаправленного поведения, устремленного на удовлетворение потребностей в признании.

3) Удовлетворение потребностей – отражает позитивное чувство облегчения и комфортного состояния, которое ощущает человек, когда его потребности реализуются.

Мотивацию персонала, анализируемую как процесс, можно представить в виде ряда последовательных этапов (рис. 1).

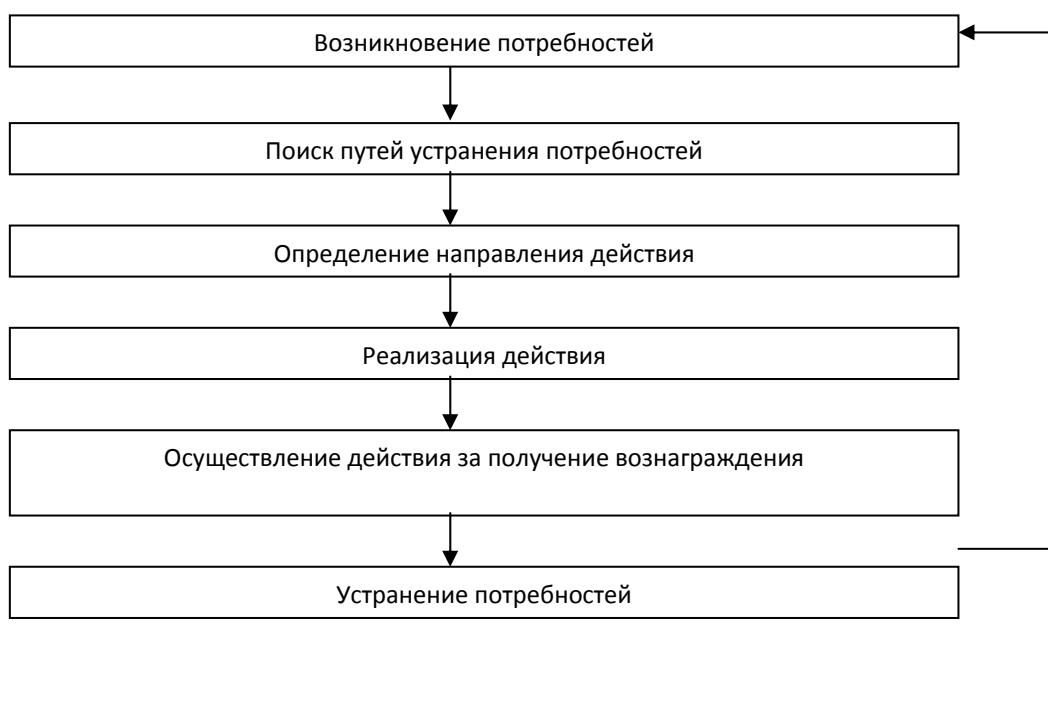


Рис. 1. Схема мотивационного процесса

- 1 этап – человек ощущает, что ему чего-то не хватает, он решает предпринять какие-то действия;
- 2 этап – определение направлений действий, как именно и какими средствами можно удовлетворить потребность;
- 3 этап – определяется, что именно и какими средствами нужно обеспечить потребность;
- 4 этап – затраты усилий для осуществления действия, позволяющего осуществить потребность. При этом может происходить корректировка целей, поскольку цели и потребности могут претерпеть изменение в процессе осуществления действий;

– 5 этап – проделав необходимую работу, человек получает то, что он может использовать для удовлетворения потребности, либо то, что он может обменять на желаемое для него;

– 6 этап – человек или прекращает деятельность до возникновения новой потребности, или продолжает искать возможности и осуществлять действия по устранению потребности.

Существуют следующие методы мотивирования эффективного трудового поведения [3]:

- материальное поощрение (зарплата, премии, гранты);
- организационные методы (перспектива приобрести новые знания и навыки);
- морально-психологические (атмосфера взаимного уважение, личное и публичное признание).

В современном обществе существуют различные модели распределения рабочего времени. В России на данный момент большинство организаций работают 5 дней по 8 часов, но также гибкий график является одним из предпочтительных методов.

1) 5 дней по 8 часов и 2 выходных.

2) 4 дня по 10 часов и 3 выходных («Сжатая неделя»).

3) «9–80» (4 дня по 9 часов и через неделю 4 дня по 9 часов и один день 8 часов).

4) Гибкий график.

5) Разделение рабочего задания (одно задание распределяется на несколько человек с целью разгрузить одного специалиста).

6) Дистанционное присутствие на рабочем месте (при наличие интернета можно работать, не выходя из дома).

В МОУ «СОШ № 21» г. Ухты был проведён опрос, в котором приняло участие 10 человек. Тестирование показало, что в данном учреждении наблюдается тенденция избежание неудач.

Так как организация некоммерческая, то бюджетом управляет государство. И в данном случае советы будут даны Министерству образования.

1. Увеличение выплаты надтарифного фонда.

2. Повышение оклада.

3. Увеличение разницы окладов у разных разрядов.

4. Дальнейшая поддержка конкурса «Учитель года».

5. Оставить без изменения процесс награждения.

6. Проведение различных семинаров.

#### **Список используемых источников**

1. **Основы** управления персоналом / А. Я. Кибанов. – М. : ИНФРА-М, 2005. – 102 с.
2. **Основы** менеджмента / А. В. Игнатьева. – М. : Эконом. Образование, 2003. – 38 с.

3. **Мотивация** и стимулирование труда в управлении персоналом: монография / Е. Е. Егоров. – Н. Новгород : Волж. гос. инж.-пед. акад., 2004. – 42 с.

*Статья представлена научным руководителем,  
канд. филос. наук, доцентом М. Р. Зобовой.*

**УДК 654.739**

**А. А. Тарабаев (студент группы ИКТ-303 СПбГУТ)**

## **ФИЛОСОФСКИЕ ПРОБЛЕМЫ ПОСТМОДЕРНА**

ПОСТМОДЕРН – обозначение специфики мировоззренческих установок новейшей, «постсовременной» культуры в целом, связанной прежде всего с поливариантным восприятием мира, а также с акцентированной проблемой самоидентификации культуры.

Жан Лиотар определил постмодерн как кризис метасценариев (великих проектов), и в своей работе «Состояние Постмодерна» он замечает, что в наше время существует скептицизм к мета – нарративам. Что есть мета – нарратив? По Лиотару это некие крупные доктрины (например, исторический прогресс, познаваемость всего наукой, возможность абсолютной свободы). Современные люди стали больше понимать несовместимость стремлений, разнообразие жизни, поэтому макро – нарративы как бы распадаются на множество микро – нарративов. Нарративы характеризуют вполне определенный тип дискурса в данную эпоху. Нарративы бывают: легитимирующие (обосновывают политический строй и законы), языческие (обыденная жизнь, коллективы, семья). Дискурс – мета – нарратация, его роль заключается в создании и поддержании «социальной мифологии» для удобства управления. Утрата легитимности макро – нарративами есть основная особенность времени постмодерна.

В третьей главе Лиотар вспоминает теорию языковых игр Людвига Витгенштейна, который под языковыми играми понимал модели работы языка, методики анализа его в действии, это более простые способы употребления знаков. «Когда Витгенштейн, начиная с изучения языка, сосредоточивает свое внимание на эффектах дискурса, он называет различные виды высказываний, которые он отмечает в языковых играх. Этим термином он обозначает, что различные категории высказываний должны поддаваться наименованию по правилам, определяющим их свойства и соответствующее им употребление, точно также как в шахматной игре существует группа правил, определяющих свойства фигур и соответствующий способ их передвижения» [1].

Данный вид взаимодействия с единицами языка наводит на мысль о существовании следующих трех видов явлений. Прежде всего, во внутренних закономерностях, правилах этих игр существует некий предмет явного или неявного соглашения между игроками. Кроме того, если изменить эти правила, то меняется и природа этой игры. Таким образом, в основе всего метода лежит сопоставление процесса говорения с борьбой, подразумевающей игровой акт, при котором словесные действия противостоят друг другу [1].

Понятие «хаос» сейчас широко используется представителями естественнонаучного знания.

Конечно, это невежественная позиция. Понятие «хаос» имеет длительную историю концептуализации в рамках философского знания. И эта история насчитывает многие сотни лет. Несложно объяснить причины того, что данный факт пока что находится на периферии научного знания.

Мне представляется актуальным и важным изучение наличествующих в истории философии стратегий взаимодействия с хаосом. Они способны помочь современному обществу выработать должное отношение к хаосу, который, по утверждению современных учёных, пронизывает многие уровни нашей действительности.

На протяжении тысячелетий философы разрабатывали стратегии отношения к хаотическим феноменам. Конечно, не всё из этого арсенала имеет смысл в современном обществе. В данном контексте сейчас неуместны те философские учения, которые призывают нас закрывать глаза на то, что является действительностью.

Безусловно, феномен хаоса был известен человечеству задолго до открытий учёных XX века. Господствующая идеология, популярные в ту или иную эпоху картины мира могли запрещать называть хаосом явления, которые не вписывались в бытовавшие представления о гармонии, но это не означает, что не велась рефлексия в отношении таковых явлений и не выдвигались предложения по отношению человека к ним. Человечество во все времена имело свои стратегии отношения к феноменам хаотичности и непредсказуемости, и эти стратегии позволили ему выжить.

Впрочем, в поисках философских стратегий взаимодействия человека с хаосом не нужно устремлять взгляд исключительно вглубь веков.

В вопросе взаимодействия с хаосом философия способна очертить стратегические направления. Тактику такого рода взаимодействия должны разработать прикладные науки. Стратегическое видение в этом вопросе необходимо – человек не может действовать эффективно, не зная, как следует относиться к тому, с чем он взаимодействует. Он должен иметь целостную и сущностную картину перед глазами, а не только выполнять какие-то алгоритмы.

Исаия Берлин говорит о необходимости относиться к хаосу как к тому, от чего человек призван себя обезопасить. Он пишет в связи с хаосом о

страхе, который требует, чтобы человек прежде всего обеспечил себе гарантии безопасности [2].

Итак, по-моему, историко-философские исследования проблемы хаоса могут иметь ощутимое теоретическое и практическое значение. Они дополняют существующие исследования материалом, который познакомит с наработанными подходами к проблеме отношения человека к хаосу.

Постмодернизм переосмыслил возможности и границы человеческой индивидуальности. При таком видении действительности, когда предметом осмыслиния становятся одна лишь нестабильность, хаос, фрагментарность, нелепость симуляций, когда мир раздвигается от макромира Вселенной до микромира夸ков, само существование целостной личности носит проблематичный характер [3].

В постмодернистской интерпретации человек превращается, с одной стороны, в «негативное пространство», «случайный механизм», «фрагментарного человека», «человека в минусовой системе координат» и т. д. Ролан Барт, например, вообще разработал постулат о смерти субъекта [3].

Такое переосмысление роли, возможностей человека, «места человека на координатах Вселенной», как в свое время выразился Л. М. Леонов, привело к философии антропологического пессимизма [3].

Может быть, одним из первых основные свойства человеческой личности в XX веке, веке социально-исторических катастроф и гуманистического кризиса мировой цивилизации, определил Роберт Музиль в «Человеке без свойств». В таком герое доведены до крайности все полярные категории, уничтожена бинарность, все сведено к явлениям медиативного ряда, а в итоге – духовная аннигиляция и нравственный коллапс [3, 4].

1) Истины не существует, существует лишь множество мнений (или, говоря языком постмодернизма, множество текстов) [5].

2) По любому вопросу ничье мнение не весит больше, чем мнение кого-то иного. Девочка-пятиклассница имеет мнение, что Дарвин неправ, и хороший тон состоит в том, чтобы подавать этот факт, как серьезный вызов биологической науке [5].

Это поветрие характерно не только для России, но и для западного мира. Действительно, существуют аспекты мироустройства, где истина скрыта и, быть может, недостижима; – действительно, бывают случаи, когда непрофессионал оказывается прав, а все профессионалы заблуждаются. И огромной силы стимулом к их принятию и уверованию в них служит их психологическая выгодность. Если все мнения равноправны, то я могу сесть и немедленно отправить и мое мнение в Интернет, не затрудня себя многолетним учением и трудоемким знакомством с тем, что уже знают по данному поводу те, кто посвятил этому долгие годы исследования. Психологическая выгодность здесь не только для пишущего, но также и для значительной части читающих: это освобождает их от ощущения собственной недостаточной образованности, в один ход ставит их выше тех, кто долго

корпел над освоением традиционной премудрости, которая, как они теперь узнают, ничего не стоит [5].

От признания того, что не существует истины в некоем глубоком философском вопросе, совершается переход к тому, что не существует истины ни в чем, скажем, в том, что в 1914 году началась Первая мировая война. И вот мы уже читаем, например, что никогда не было Ивана Грозного или что Батый – это Иван Калита. И что много страшнее, прискорбно большое количество людей принимает подобные новости охотно [5].

А нынешние средства массовой информации, увы, оказываются первыми союзниками в распространении подобной информации, потому что они говорят и пишут то, что должно производить впечатление на массового зрителя и слушателя и импонировать ему, следовательно, самое сенсационное, а отнюдь не самое серьезное и надежное [5].

#### **Список используемых источников**

1. **Состояние постмодерна** / Ж. Ф. Лиотар: пер. с фран. Н. А. Шматко. – М. : Институт экспериментальной социологии; СПб. : Алетейя, 1998. – 160 с.
2. **Европейское единство и превратности его судьбы** / И. Берлин // Неприкосновенный запас. Дебаты о политике и культуре. – 2002. – № 1. – С. 5–23.
3. **Актуальные** проблемы современной русской литературы (постмодернизм): учебн. пособие / Н. Е. Лихина. – Калининград : Калининградский ун-т, 1997. – 59 с. – ISBN 5-88874-085-3.
4. **Человек** без свойств / Р. Мизуиль: пер. с нем. С. Апт. – М. : Ладомир. 1994. – ISBN 5-86218-142-3, 5-86218-141-5.
5. **Истина** существует, и целью науки является ее поиск [Электронный ресурс] / А. А. Зализняк. – Режим доступа: <http://elementy.ru/lib/430463/430465> (Дата обращения 05.05.2014).

*Статья представлена научным руководителем,  
канд. филос. наук, доцентом М. Р. Зобовой.*

**УДК 339**

**Е. И. Фатькина (студентка группы СР-91 СПбГУТ)**

#### **РОЛЬ ШВЕЦИИ В РАЗВИТИИ ТРАНСАНГЛАНТИЧЕСКОЙ ЗОНЫ СВОБОДНОЙ ТОРГОВЛИ**

Начав активно развиваться во второй половине XX века, международная экономическая интеграция не теряет своей значимости и на современном этапе развития. Сегодня в мире можно заметить увеличение объема движения товаров, услуг, капитала, идей, людей. Этот процесс называется

глобализацией. Важным аспектом глобализации является международная торговля. Соединенные Штаты Америки (США) и Европейский Союз (ЕС) являются крупнейшими центрами мировой экономики и, следовательно, способны значительно влиять как на мировое хозяйство в целом, так и на экономики отдельных стран [1]. В 2013 году президент США Барак Обама, председатель Европейского совета Херман ван Ромпей и председатель Европейской комиссии Жозе Мануэль Баррозу, на основании рекомендаций Рабочей группы высокого уровня США–ЕС по вопросам занятости и экономического роста, заявили о начале переговоров по созданию трансатлантической зоны свободной торговли между США и Евросоюзом [2].

Для того чтобы понять, насколько значима роль Швеции в инициативе создания соглашения о свободной торговле между ЕС и США, целесообразно рассмотреть, насколько плотно сотрудничают государства, каковы основные направления сотрудничества. Особое внимание следует уделить взаимодействию в сфере торговли.

2013 год был отмечен важной датой для Шведско-Американских отношений – 230 лет со дня подписания первого соглашения о свободной торговле между государствами. Договор о дружбе и торговле между США и Королевством Швеция был подписан в 1783 году. Именно эта дата и ознаменовала начало дипломатических отношений между государствами.

Сегодня торговый поток между государствами достаточно велик. США являются важнейшим экспортным рынком для Швеции после ЕС и 11-м импортером на шведском рынке. Таким образом, для Швеции заключение трансатлантического соглашения о свободной торговле принесет большие выгоды: снижение торговых пошлин и нетарифных ограничений между двумя сторонами, значительное снижение стоимости торговых операций с США и увеличение их объема. Несмотря на то, что сегодня между США и государствами ЕС, в частности Швецией, торговые пошлины не так высоки, но при таких объемах торговли они все же весьма значимы.

Укрепление сотрудничества между США и ЕС в области свободной торговли стало одной из тем обсуждения на встрече шведского министра торговли Эвы Бьерлинг и американского торгового посла Рона Кирка в мае 2012 г. в Вашингтоне. Шведский министр торговли подчеркнула значимость такого сотрудничества для создания новых рабочих мест и экономического роста [3]. В том же году Шведским национальным советом по торговле (Kommerskollegium) было опубликовано исследование «Возможные эффекты соглашения о свободной торговле между ЕС и США. Швеция в фокусе» [4], в котором авторы предлагают различные сценарии развития соглашения и возможные выгоды для обеих сторон.

При рассмотрении торгово-экономических отношений между ЕС и США особое внимание необходимо уделить Шведско-Американской торговой палате – некоммерческой организации, основным направлением деятельности которой является содействие торговле между Швецией и Север-

ной Калифорнией. Шведско-Американская торговая палата является ярким примером тесного сотрудничества государств в сфере бизнеса, что в определенной степени служит доказательством нацеленности на дальнейшее укрепление связей между шведскими и американскими компаниями, взаимной открытости рынков. Подобное сотрудничество можно рассматривать как еще один шаг в укреплении отношений между государствами и, в перспективе, как еще один шаг на пути к подписанию трансатлантического соглашения о свободной торговле.

Активную позицию за создание трансантлантической зоны свободной торговли занимает шведский министр торговли, Эва Бьёрлинг. Она была одной из первых, кто предложил идею создания трансатлантической зоны свободной торговли, на семинаре в Вашингтоне, в 2009 году [5]. Кроме того, на сайте правительства Эвой Бьёрлинг была опубликована стратегия увеличения выгоды от подписания трансатлантического соглашения о свободной торговле. В ней не только поддерживается идея создания зоны свободной торговли между ЕС и США, но также говорится об активном участии Швеции в переговорах, организации встреч стран-членов ЕС с целью ускорения процесса подписания соглашения.

В целом, шведско-американские отношения имеют влияние на становление трансатлантической зоны свободной торговли. Государства сотрудничают в различных областях, таких как: защита окружающей среды, устойчивое развитие, предоставление помощи странам третьего мира [6] и т. д. В области торговли государства сотрудничают в рамках ряда проектов и организаций. Одной из данных организаций является Шведско-Американская торговая палата.

Таким образом, активное взаимодействие между США и Швецией в торгово-экономической и других областях можно рассматривать как своего рода катализатор в развитии трансатлантической зоны свободной торговли. Именно такой комплексный подход, когда сотрудничество осуществляется по достаточно большому количеству направлений, может оказаться наиболее действенным.

### **Список используемых источников**

1. Торговая политика Европейского Союза / Т. М. Исаченко. – М. : Государственный Университет, Высшая Школа Экономики, 2010. – С. 270.
2. Лидеры ЕС и США о трансатлантическом торговом и инвестиционном партнерстве (февраль 2013) [Электронный ресурс]. – URL: <http://iipdigital.usembassy.gov/st/russian/texttrans/2013/02/20130214142570.html#axzz2puG9Dxce> (Дата обращения 30.01.2014).
3. Regeringskansliet Ewa Björling till USA – fördjupathandelssamarbetepåagendan (май 2012) [Электронный ресурс]. – URL: <http://www.regeringen.se/sb/d/16164/a/193084> (Дата обращения 30.01.2014).

4. **Potential Effects from an EU-US Free Trade Agreement – Sweden in Focus / S. Kinnman, T. Hagberg // Kommerskollegium National board of trade Utrikesdepartementet.** – 2012.

5. **Regeringskansliet** Frihandelnstår Sverigesfokus 2014 zydfhm 2014 [Электронный ресурс]. – URL: <http://www.regeringen.se/sb/d/18334/a/231416> (Дата обращения 30.01.2014).

6. **Regeringskansliet** Utrikesdepartementet Mer innovation och nytänk inombiståndet (ноябрь 2013) [Электронный ресурс]. – URL: <http://blogg.ud.se/utvecklingspolitik/2013/11/19/mer-innovation-och-nytank-inom-bistandet> (Дата обращения 30.01.2014).

*Статья представлена научным руководителем,  
канд. ист. наук, доцентом Е. В. Драгуновой.*

## УДК 32.019.5

**А. А. Шарамыгина (студентка группы РСО-31М СПбГУТ)**

### **ОБЩЕСТВЕННОЕ МНЕНИЕ В СОЦИАЛЬНЫХ СЕТЯХ: МОТИВАЦИОННО-ЦЕННОСТНЫЕ КОМПОНЕНТЫ**

Для формирования современного государства необходимо уделять внимание развитию молодежи, что подразумевает не только создание развивающей образовательной среды, но и развивающего культурного фона, а также трансляцию заложенных с детства гуманистических ценностей. В современной информационной эпохе, в которой формируется сознание молодых людей, интерес вызывает такой особый тип коммуникаций, как массовые коммуникации. Российское общество находится на том этапе развития, когда Интернет для молодого поколения является ведущим источником информации об окружающем мире, формирующим в сознании молодежи особую информационную картину реальности. При этом сфера отношений между людьми в сети Интернет мало контролируется государством, что создает благоприятную почву для распространения искаженной информации и формирования неверных представлений об окружающем мире у молодых людей. Современное поколение, переставшее ценить знание как объективное отражение реальности, готово принять на веру любое высказывание, замаскированное под мнение большинства или научно доказанные факты.

Как показывает анализ литературных данных, определение понятия «общественное мнение» является дискуссионным вопросом. Б. А. Грушин характеризует общественное мнение как форму массового сознания, в котором проявляется отношение (скрытое или явное) различных групп лю-

дей к событиям и процессам действительной жизни, затрагивающим их интересы и потребности [1].

Понятию «мнение» можно дать и более узкое определение: мнение – это субъективное убеждение человека, основанное на интерпретации фактов и личных эмоциях. Важно отметить, что существует множество факторов, влияющих на формирование мнения индивида – это особенности воспитания и культуры, образование, интеллектуальный стиль, религиозные верования, ценности, потребности. Данные параметры, характеризующие индивидуальность человека, служат определенным информационным фильтром при восприятии фактов реальности и формировании субъективного мнения.

Можно предположить, что общественное мнение, выраженное в социальных сетях, обладает специфическим влиянием на процесс формирования представлений, мотивов и ценностей подрастающего поколения.

Согласно определениям, данным в работе Д. В. Кухарчука [2], социологи отмечают три необходимых условия функционирования и развития общественного мнения: общественная значимость, актуальность проблемы, темы или события; дискуссионность обсуждаемых вопросов; необходимый уровень компетентности группы. Важно отметить, что в виртуальной среде последний компонент далеко не всегда является обязательным.

Более того, сама «дискуссионность» общественного мнения в виртуальном пространстве предстает в искаженной форме. Специфика среды виртуального пространства размывает чувство ответственности и создает иллюзию анонимности. При этом обмен огромным массивом плохо структурированной информации среди множества активных участников социальной сети происходит мгновенно. Реакция на определенное явление, факт или процесс может быстро находить свое выражение в активных действиях людей.

Таким образом, уже само определение понятия «общественное мнение» включает идею о том, что в его основе лежат субъективные, личностные, психологические характеристики субъектов общественного мнения. При этом, средства массовых коммуникаций могут оказывать целенаправленное воздействие на мнения, оценки и, следовательно, поведение людей. Таким образом, общественное мнение может быть сформировано не только спонтанно, но и намеренно.

Обобщая исследования, проведенные Всероссийским Центром Изучения Общественного Мнения (ВЦИОМ) 31 марта – 1 апреля 2012 года, можно утверждать, что сетевые коммуникации пользуются наибольшим успехом именно у молодежи. При этом 96 % типичных пользователей социальных медиа – это люди в возрасте 18–24 лет.

Следует отметить, что именно в данный период ранней взрослости происходит активное формирование жизненных ценностей, собственных взглядов, системы идеалов и убеждений [3]. При этом в рунете самыми по-

сещаемыми интернет-ресурсами являются: социальная сеть Вконтакте ([vk.com](http://vk.com)) – 67 % от общего объема посещений Рунета; социальная сеть Одноклассники.ру – 64 % интернет трафика.

На основе приведенных выше статистических данных, можно утверждать, что наибольшее влияние на современную молодежь оказывает именно информация, полученная через социальные сети. С момента их появления (т. е. с 2006 года) данное влияние растет, потому растет и связь между социокультурными ценностями группы и воздействием на них информации, циркулирующей внутри данных социальных сетей.

В последние годы исследователями было проведено множество социальных опросов (региональных и общенациональных), направленных на выявление векторов ценностных ориентаций современной молодежи и их приоритетность. За последние четыре года результаты по ним совпадают, поэтому в качестве примера мы взяли опрос специалистов Фонда «Общественное Мнение» (ФОМ), проводившийся в июле 2011 года. Данные этого опроса позволяют нам выстроить определенную иерархию приоритетов, во главе которой находятся такие ценности как: семья и друзья, безопасность, достаток, личная выгода, стабильность.

Обобщив результаты опроса, можно прийти к выводу о том, что основные ценности современной молодежи, считающиеся приоритетными, являются достаточно узкими и находящимися на низком и среднем уровне иерархии потребностей А. Маслоу. При этом сам перечень ведущих ценностей отличается специфической направленностью: отображением важности лишь тех событий и фактов, которые затрагивают интересы конкретной личности или малой группы (близких людей).

Можно предположить, что среди причин, приведших современное поколение к подобным ценностным установкам – это и исторические, и экономические факторы развития страны, и социокультурные изменения, и прогресс информационного общества, а также влияние на подрастающее поколение средств массовых коммуникаций, одновременно транслирующих и отражающих данные ценности, мотивы, цели, интересы и модели поведения молодежи.

Проведенный нами опрос отражает основные ценности молодых людей в самых многочисленных и популярных группах социальной сети. Согласно статистике, средний возраст посетителей сети Вконтакте составляет 18–24 года, что соответствует характеристикам генеральной совокупности.

Контент-анализ 50 топ пабликсов, постов и параметров обратной связи (кликов (лайков), комментариев, репостов, упоминаний сообщества), а также количественный анализ подписчиков и охвата аудитории (пользователей, которые увидели предложенную новость в определенный день, в том числе с репостов) позволили выявить самые часто обсуждаемые темы, дискуссионные вопросы и волнующие проблемы, характеризующие данное сообщество.

Проведенное исследование позволяет прийти к следующим выводам: во-первых, приоритетными ценностями современной молодежи являются социальные ценности дружбы, любви и семьи. Во-вторых, самым дискуссионным вопросом в группах является вопрос честности. Внушительное количество постов посвящены именно теме предательства и недоверия к людям, страха быть обманутыми. В-третьих, широко одобряется стремление владеть материальными благами и ценностями, а также часто поднимаются вопросы о самообеспечении, быстром обогащении (зачастую с помощью других людей), важности власти в условиях социального неравенства. В-четвертых, достаточно важной стала тема личного спокойствия и комфорта, обеспокоенность нестабильностью общества, неуверенность в органах государственной власти, потребность «спрятаться, сбежать из этой реальности».

Исходя из полученных в ходе теоретического и эмпирического исследований данных, можно сделать вывод о том, что результаты прошлых опросов подростков и результаты недавнего собственного опроса самой популярной среди молодежи социальной сети во многом схожи. Это можно объяснить тем, что ценности личности начинают формироваться задолго до ранней взрослости. Стоит отметить, что проведенное эмпирическое исследование также показало, что в выражении ценностей в виртуальной реальности (за исключением самых главных базовых установок на любовь, семью и друзей) четко прослеживается осознание участниками сообществ нестабильности ситуации и чувство неопределенности.

Данный вопрос, а также вопрос о характере влияния общественного мнения, выраженного в социальных сетях, на мотивационно-ценостные компоненты личности молодежи требует дальнейших исследований.

Таким образом, информационное пространство социальных сетей является в современном обществе одним из самых значимых факторов формирования когнитивной картины мира молодежи. При этом до конца остается неизученным вопрос о характере связи общественного мнения в социальных сетях и мотивации, интересов, ценностей и убеждений участников данных групп.

Массовая виртуальная культура весьма противоречива: поток разнообразной, неструктурированной информации, попадающейся подросткам или даже детям в Интернете, не позволяет человеку, не имеющему стойких моральных внутренних фильтров, сформировать независимые, индивидуальные ценности. Данная особенность коммуникаций в Интернете делает каждого участника коммуникаций открытым для манипулятивного воздействия. В связи с этим постоянный мониторинг общественного мнения в социальных сетях позволит не только определить текущие ценности групп и спрогнозировать их поведение, но и описать ценностные установки нового поколения, образы мира, а также ценностные ориентиры страны, общества и каждой личности.

**Список используемых источников**

1. **Мнения** о мире и мир мнений / Б. А. Грушин. – М. : Изд-во полит. лит-ры, 1967. – 400 с.
2. **Социология.** Конспект лекций / Д. В. Кухарчук. – М. : ЮРАЙТ-ИЗДАТ, 2010. – 192с.
3. **Ценностные** ориентации и механизмы социальной регуляции поведения. Методологические проблемы социальной психологии / О. И. Зотова, М. И. Бобнева. – М. : Наука, 1975. – С. 27–34.

*Статья представлена научным руководителем,  
канд. психол. наук, доцентом Е. В. Беловой.*

## СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

УДК 623.486

А. А. Асеев (студент группы ИКТВ-31 СПбГУТ)

А. Н. Дробяскин (начальник учебной части – заместитель начальника отдела УВЦ ИВО СПбГУТ)

А. Н. Музыкантов (заместитель начальника УВЦ ИВО СПбГУТ)

### СБОР И ИСПОЛЬЗОВАНИЕ ТРОФЕЙНОЙ ТЕХНИКИ СВЯЗИ И ВОЕННО-ТЕХНИЧЕСКОГО ИМУЩЕСТВА. ЭВАКУАЦИЯ ТЕХНИКИ СВЯЗИ И ВООРУЖЕНИЯ. ОРГАНИЗАЦИЯ УЧЕТА ИМУЩЕСТВА СВЯЗИ

К началу Великой Отечественной Войны Советская Армия не имела самостоятельной трофейной службы. Лишь только после реорганизации тыла Советской Армии (август 1941 г.) была сделана первая попытка объединения трофейного дела в руках единого органа. В центре таким органом стал отдел эвакуации штаба Тыла, а во фронтах – эвакоотделы в управлении тыла и уполномоченные по сбору трофейного и негодного имущества при командующих родами войск и начальниках довольствующих служб. В армиях создавались эвакоотделения в управлениях тыла, назначались уполномоченные по сбору трофейного и негодного имущества, имелись армейские склады негодного имущества. Непосредственно в войсках вводились трофейно-эвакуационные отделения при штабах дивизий и уполномоченные по сбору трофейного и негодного имущества в полках. В конце 1941 г. в стрелковых и артиллерийских частях стали создаваться рабочие команды по сбору военного имущества<sup>1</sup>.

Такая структура оправдала себя при осуществлении эвакуации техники, но оказалась не приспособленной к решению таких задач, как сбор трофейного вооружения, имущества и металлом. Особо это выявилось в ходе наступательных операций зимней кампании 1941–1942 гг.

Весной 1942 г. были созданы две постоянно действующие комиссии – Центральная комиссия по сбору трофейного вооружения и имущества под председательством Маршала Советского Союза С. М. Буденного и Центральная комиссия по сбору черных и цветных металлов в прифронтовой

---

<sup>1</sup> Бурчин, А. Г. и др Техническое обеспечение войск связи в годы Великой отечественной войны. – Л. : ВАС, 1990. – 131 с.

полосе под председательством Н. М. Шверника. В составе Главного управления Тыла Советской Армии было сформировано Управление по сбору и использованию трофейного вооружения, имущества и металлолома, а во фронтах и общевойсковых армиях – аналогичные отделы со следующими задачами:

- сбор трофейного и другого войскового имущества, оставленного на поле боя;
- сортировка данного имущества;
- разделка техники и снаряжения;
- организация вывоза имущества из тыловой полосы фронта (армии);
- учет трофейного имущества;
- организация охраны освобожденных предприятий и объектов;
- очистка железнодорожных станций, дорог, предприятий и полей от взрывоопасных предметов.

В дивизиях трофейно-эвакуационные отделения были реорганизованы в отделения по сбору трофейного имущества, в том числе и имущества связи, и металлолома.

В полках за организацию сбора трофейного имущества и металлолома продолжали отвечать уполномоченные. Кроме того, в каждой армии по мере необходимости формировалось по одной трофейной роте численностью до 200 человек.

Зимой 1942–1943 гг. размах и темпы наступательных операций еще более возросли, что потребовало дальнейшего укрепления трофейных органов, повышения их маневренности. Ведь только за период зимнего наступления Советской Армии (ноябрь 1942 г. – 31 марта 1943 г.) нашими войсками было захвачено 1490 самолетов, 4679 танков, 15800 орудий различного калибра, 9835 минометов, 30705 пулеметов, свыше 500 тыс. винтовок, 17 млн. снарядов, 123 тыс. автомашин, 890 паровозов, 22 тыс. вагонов, 1875 складов и большое количество средств связи.

Весной 1943 г. при ГКО вместо двух существовавших комиссий был создан Трофейный комитет во главе с Маршалом Советского Союза К. Е. Ворошиловым. Кроме того, управление по сбору и использованию трофейного вооружения, имущества и металлолома было реорганизовано в Главное трофейное управление, имевшее в своем составе отдел связи. В армиях и соединениях вопросами использования трофейного имущества связи занимались помощники начальников связи по снабжению. Командирам соединений и частей разрешалось формировать по мере необходимости дополнительные нештатные команды.

Одновременно с реорганизацией органов управления трофейной службы началось формирование новых трофейных частей. Приказом Народного комиссара обороны СССР от 5 января 1943 г. был введен институт комендантских постов во главе с штатными комендантом с задачей своевременного выявления, учета, сбора, хранения и вывоза трофейно-

го и оставленного войсками отечественного оружия, имущества и продовольствия в освобожденных от противника населенных пунктах.

В 1944 г. танковым, механизированным и кавалерийским объединениям, которые, как правило, первыми входили в тыл противника и раньше других войск обнаруживали трофеиные объекты, были переданы трофеевые роты, демонтажные взводы и трофеевые склады.

Новые задачи, возникшие перед трофеейной службой на заключительном этапе войны, обусловили необходимость ее дальнейшего усиления. Приказом НКО СССР от 19 января 1945 г. во фронтах и армиях была введена должность заместителя начальника тыла по трофеям, в штабах тыла организованы отделы по учету и использованию трофеевого народнохозяйственного имущества, а в городах и крупных населенных пунктах учреждены помощники военных комендантов по хозяйственным вопросам. Несколько позже для руководства ликвидацией военно-экономического потенциала фашистской Германии был создан специальный комитет при Совете Министров СССР.

Сбор трофеевого имущества связи в годы ВОВ производился:

- в районе участка военной дороги этапными комендантами с привлечением местного населения;
- в дивизионном и полковом тылу – комендантскими взводами дивизии и полка, а также временными нештатными командами с дальнейшей передачей собранного имущества в армейские трофеевые органы;
- в армейском тылу – трофеевыми ротами, батальонами и демонтажными взводами;
- во фронтовом тылу – фронтовыми трофеевыми бригадами;
- в районах расположения и работы частей и подразделений связи – силами этих частей и подразделений.

Одновременно со сбором трофеевого имущества производился также сбор воинского имущества, оставленного по разным причинам на полях сражений нашими войсками или оставленного у местного населения. У последнего воинское имущество собиралось в принудительном порядке.

На армейских и фронтовых складах трофеевое имущество сортировалось, ремонтировалось и приводилось в состояние, пригодное для дальнейшего использования. Полученными деталями покрывалось до 50 % потребностей ремонтных органов в запасных частях. Особо ценные экземпляры трофеевого имущества направлялись в распоряжение ГУСКА на центральные склады, откуда оно поступало для изучения в научно-исследовательские институты и в Военную академию связи.

В годы войны эвакуации подлежало все имущество связи, в том числе трофеевое, и имущество, принадлежащее гражданским министерствам и ведомствам, но оставленное последними и даже требующее среднего и капитального ремонта. Все имущество, пришедшее в негодность, а также из-

лишнее и то, которое не могла быть использовано на фронте, направлялось на центральные склады НКО.

Общее руководство эвакуацией войскового имущества осуществлялось начальниками тыла дивизий, армий и фронтов. Непосредственное руководство и контроль за своевременной эвакуацией имущества связи было возложено на начальников связи дивизий и фронтов и их помощников.

В годы ВОВ учет имущества связи в частях и подразделениях велся согласно «Наставлению по войсковому хозяйству», введенному в действие приказом НКО № 180 летом 1942 г.

В отношении качественного состояния имущество делилось на 5 категорий:

1-я категория – новое имущество, не бывшее в эксплуатации и годное к использованию;

2-я категория – имущество, бывшее или находящееся в эксплуатации, либо требующее мелкого ремонта;

3-я категория – имущество, требующее среднего ремонта;

4-я категория – имущество, требующее капитального ремонта;

5-я категория – имущество, непригодное для дальнейшей эксплуатации.

Перевод имущества из одной категории в другую осуществлялся актами комиссий, назначенных командирами частей. На имущество, переведимое из 1-й во 2-ю категорию, при выдаче его в подразделения акты не составлялись – основанием являлись расходные документы.

Все случаи утраты и повреждения техники связи немедленно расследовались, а виновные привлекались к строгой ответственности. Основанием для производства расследования являлся приказ командира части. Этот приказ отдавался командиром согласно инструкции органам дознания на основании сведений о недостаче имущества. Материал расследования вместе с ходатайством о выдаче инспекторского свидетельства высыпался в штаб вышестоящего соединения (объединения) связи. В необходимых случаях вышестоящие начальники связи назначали дополнительное расследование, экспертизу и проверку. Выдача инспекторских свидетельств по делам, по которым виновные преданы суду, производились на основании судебного решения, вступившего в силу.

Исключительно важное внимание в годы ВОВ уделялось учету имущества связи. Учет осуществлялся по формам обычного материального учета: на складах применялась форма карточного учета; в штабах и в подразделениях записи учета производились в книгах.

В ходе перевозки имущество связи также обязательно учитывалось. Независимо от вида транспорта на все перевозимые грузы выдавались с места отправления «открытые листы», в которых обозначалось, какое имущество перевозится, в каком количестве, адрес отправителя и адрес назначения, фамилия и имя сопровождающего, ответственного за груз.

«Открытые листы» служили документом, по которому проверялось наличие имущества в ходе транспортировки и по прибытию на место получения.

В подразделениях имущество связи хранилось в таком же порядке, как и боевое оружие. Основные табельные средства связи закреплялись за определенными лицами с таким расчетом, чтобы каждый аппарат, каждый метр кабеля имел своего хозяина, отвечающего за постоянное исправное состояния имущества связи.

Своевременный учет, правильная организация хранения, охрана имущества и «открытые листы» в основном обеспечивали бережение техники связи. На это же было нацелено правильное ведение документов по учету имущества связи. Таких документов было несколько.

В подразделенияхвойской части велись: учетные карточки, формуляры (паспорта), описи комплектов имущества, книги сдачи имущества в ремонт.

На складах войсковой части велись: учетные карточки, формуляры (паспорта), описи комплектов имущества, книги сдачи имущества в ремонт, реестр учетных карточек.

В штабах отдельных частей велись: книга имущества войсковой части, книга учета боевых и вспомогательных машин, формуляры (паспорта), описи комплектов имущества, ведомость неукомплектованности, книга недостач и излишков, наряды, накладные, доверенности на получение имущества, извещения о получении имущества, акты на прибывшее имущество, инспекторские свидетельства, реестр учетных карточек.

Контроль за состоянием имущества связи и за ведением учета осуществлялся как по линии непосредственного командования, так и по линии вышестоящего начальника связи, путем периодических проверок имущества и ведения учета. Проверки были годовые, квартальные, месячные и внезапные. Они производились назначенными отдельными лицами или комиссиями. Часто проверка бережения имущества и техники связи и ведение учета осуществлялось в ходе комплексной проверки части связи. Так было, например, в июле 1942 г. в ходе проверок боевой готовности узла связи Генерального штаба. Во всех случаях по результатам проверки комиссии составлялись акты, в которых указывалось: состояние проверенного имущества, состояние учета, правильность хранения учетных документов. Выявленные при проверке дефекты немедленно устранялись. При необходимости назначались повторные комиссии. В случаях установления недостач или излишков командование части назначало расследование для привлечения виновных к ответственности. Материалы расследования служили основанием для выдачи соответствующими начальниками инспекторских свидетельств для перечисления имущества в 4-ю или 5-ю категорию, или списания утраченного или испорченного имущества.

УДК 621.395

**Л. В. Воробьев (начальник цикла ВК ИВО СПбГУТ)****А. А. Темуров (студент группы СК-02 СПбГУТ)****О. И. Федоровских (студент группы СК-02 СПбГУТ)**

## ПРИМЕНЕНИЕ ОБОРУДОВАНИЯ NGN НА СЕТЯХ ВОЕННОЙ СВЯЗИ

*«...В ряде отраслей (телекоммуникационные системы и др.) именно гражданские технологии являются движущей силой бурного развития военной техники...»*

B. Путин [1]

Во всем мире развитие телекоммуникационных систем осуществляется эволюционно, вне зависимости от тех революционных преобразований, которые происходят в научно-технической области (рис. 1).

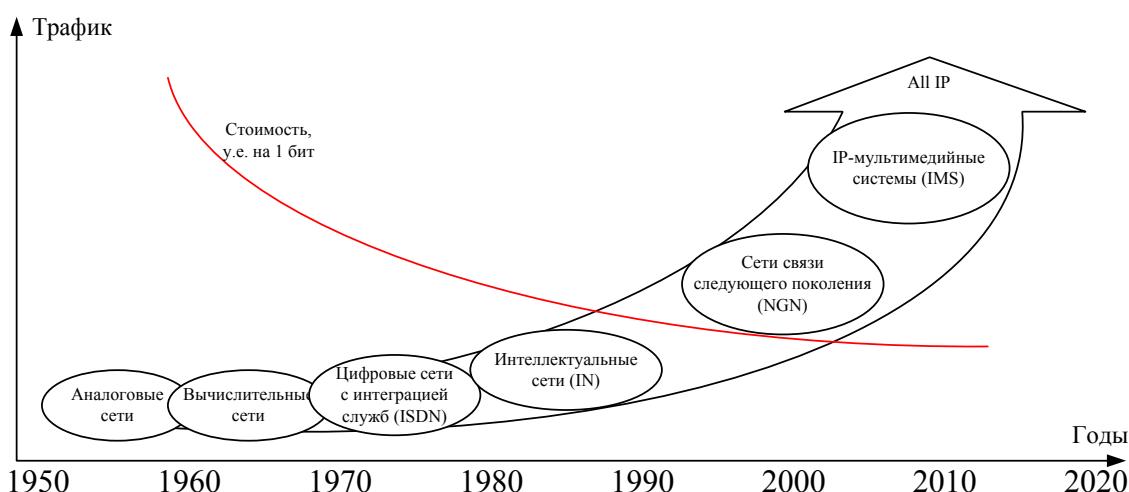


Рис. 1. Этапы развития сетей связи

В конце прошлого столетия было принято решение о необходимости скорейшего перехода на цифровое оборудование, но еще сегодня, например, на телефонных сетях связи, особенно ведомственных, можно встретить декадно-шаговые, координатные и тем более квазиэлектронные АТС.

Тем временем повсеместно начинается активное внедрение так называемых сетей связи следующего поколения (NGN – *Next Generation Network*), основанных на пакетной передаче всех видов сообщений, распределенной коммутации и использовании единого транспортного ресурса [2].

Переход к NGN должен обеспечить:

- расширение номенклатуры и качества услуг связи (телефония, электронный обмен документами, электронная почта, видео связь и др.);

- повышение эффективности использования пропускной способности трактов связи (по оценкам экспертов экономия при строительстве и эксплуатации NGN по сравнению с традиционной сетью – до 40 %.).

Соответственно должен измениться и облик сетей связи. Если до последнего времени существовали разрозненные сети, построенные по своим принципам и правилам, то в концепции NGN заложена идея как интеграции услуг, т. е. объединение различных видов связи (телефонной, телеграфной, передачи данных, видеинформации), так и конвергенции существующих сетей и технологий: фиксированных сетей общего пользования, сетей мобильной связи и IP-сетей [2].

Уровневая архитектура сети нового поколения приведена на рисунке 2. В состав NGN входят сети доступа и транспортная сеть [3].

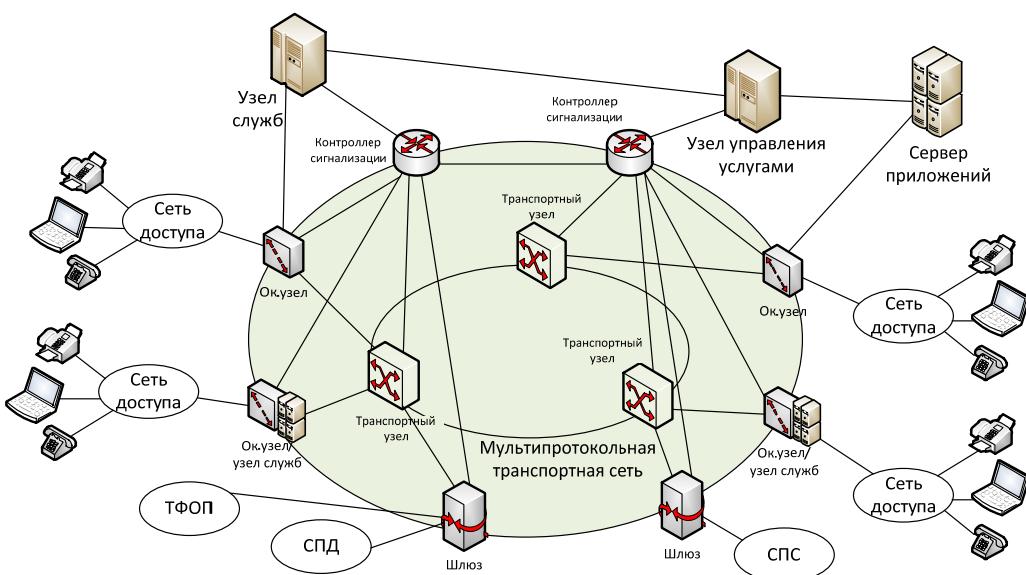


Рис. 2. Архитектура сети связи нового поколения

Транспортная сеть (*Transport Network*) – это часть сети электросвязи, обеспечивающая доставку информационных и служебных сигналов по заданным адресам и состоящая из ряда подсетей с возможно различными принципами их организации и принадлежности к различным операторам.

На уровне доступа осуществляется подключение терминалов пользователей к сети на основе применения разнообразных средств и преобразование исходного формата данных в соответствующий формат, используемый для передачи в данной сети. На уровне доступа используются следующие устройства [3]:

- медиашлюзы доступа (*AGW*);
- медиашлюзы сигнализации (*SGW*);
- устройства интегрированного доступа (*IAD*);
- медиашлюзы соединительных линий (*TGW*).

При построении NGN учитывается обязательность преемственности в предоставлении услуг связи от старых сетей (например, должны подключаться имеющиеся у пользователей терминальные устройства), должен обеспечиваться выход на существующие сети (рис. 3), которые не исчезнут в один момент.

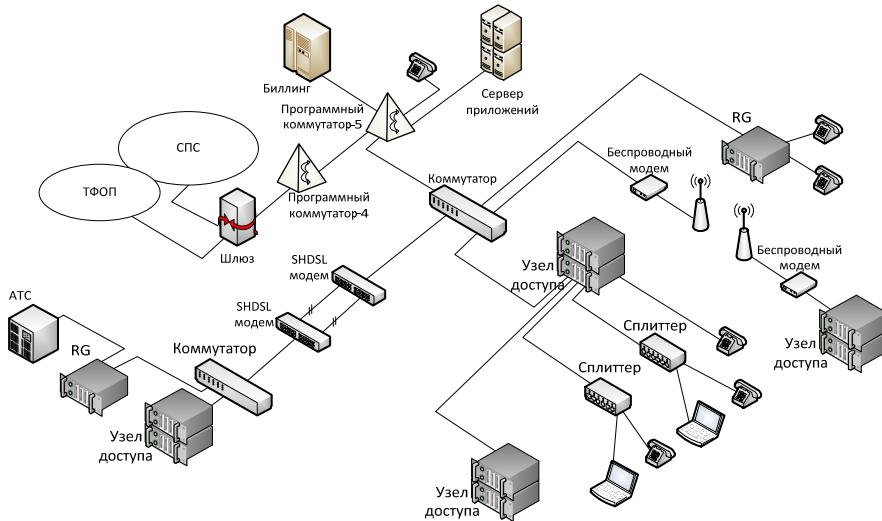


Рис. 3. Состав сети доступа (вариант)

Ситуация с развитием сетей связи Вооруженных Сил Российской Федерации (ВС РФ) отличается от задач, решаемых сетями связи других министерств и ведомств. Так, если для телефонной связи во всем мире использовались автоматически коммутируемые сети связи, то сети связи ВС РФ строились на принципах прямых связей с долговременной коммутацией на опорных узлах связи или с применением ручных телефонных станций. Подтверждением сказанного может служить то, что до последнего времени на вооружении имелась лишь одна аппаратная АТС – П-178-1(2). Данная АТС обеспечивала лишь внутреннюю автоматическую связь.

Тем самым на данном этапе ВС РФ оказались в уникальном положении. Определяя путь развития телекоммуникационных сетей, можно, не оглядываясь на прошлое, осуществлять построение современной сети связи опираясь на все последние достижения науки и техники, с учетом всех требований, предъявляемых как к системе связи, так и системе управления войсками в целом.

Комплекс технических средств для УС МО нового облика фактически уже определен. Оборудование разделяется на открытый и зарытый сегменты сети.

В состав оборудования открытого сегмента входят:

- пограничный маршрутизатор;
- шлюз VOIP телефонии, выполняющий также роль сервера управления вызовами и коммутатора открытого сегмента сети;

- цифровая АТС открытого сегмента (с рабочим местом телефониста);
- сервер и рабочее место технологического управления открытым сегментом сети.

В состав оборудования закрытого сегмента входит оборудование, обеспечивающее гарантированное скрытие содержания передаваемой информации.

Пограничный маршрутизатор обеспечивает подключение локальных сетей абонентов, построенных на коммутирующем и маршрутизирующем оборудовании относительно меньшей производительности, а также терминалов, к узлам доступа сети по медным или оптоволоконным линиям связи и передачу любых видов информации (речи, видео, синхронных и асинхронных данных), с преобразованием их в формат, принятый в сетях передачи данных на базе протокола IP.

Через шлюз VOIP телефонии передается речевая информация по сетям передачи данных с протоколом IP (интерфейсы *Ethernet, E1, E3, оптического (SFP)*) от АТС.

В открытом сегменте могут использоваться любые цифровые АТС при условии сопряжения с оборудованием по стыку E1 сигнализации DSS1.

Рассматриваемая телекоммуникационная сеть имеет возможность предоставления внутриузловой и межузловой открытой и режимной телефонной связи с автоматической коммутацией и одновременной передачей данных в режиме коммутации пакетов (протокол IPv4). В сети обеспечивается безопасность информации, включая шифрование информации, передаваемой по каналам связи, защиту информации от НСД и технических средств разведки, а также технологическое управление оборудованием комплексов, входящих в состав изделия.

Сложность создания NGN заключается в том, что несмотря на принимаемые решения, IP-сети изначально не приспособлены для передачи разнородной информации – данных, голоса, видео и т. п. – т. е. необходимо тщательно планировать сети и предусматривать меры обеспечивающие требуемое качество услуг.

Многие проблемы при построении телекоммуникационных сетей могут быть решены качественной подготовкой специалистов, способных выполнять требуемые сетевые расчеты, осуществлять подбор оборудования и обслуживать новые сети.

Таким образом, путь развития сетей военной связи мало чем отличается от направлений развития телекоммуникационных сетей других министерств и ведомств. В настоящее время осуществляется активное внедрение цифрового оборудования сетей связи следующего поколения, что обеспечит возможность предоставления внутриузловой и межузловой от-

крытой и режимной телефонной связи с автоматической коммутацией и одновременной передачей данных в режиме коммутации пакетов.

### **Список используемых источников**

1. **Быть сильными: гарантии национальной безопасности для России / В. Путин // Российская газета. – № 5708(35) от 17 февраля 2012.**
2. **Сети связи пост-NGN / Б. С. Гольдштейн, А. Е. Кучерявый. – СПб. : БХВ-Петербург, 2013. – 160 с.**
3. **NGN: принципы построения и организации / И. Г. Бакланов. – М. : Эко-Трендз, 2008. – 400 с.**

**УДК 621.396.94**

**С. В. Воронин (начальник цикла военной кафедры – старший преподаватель ИВО СПбГУТ)**  
**А. А. Крючков (студент группы СП-22 СПбГУТ)**

### **РАДИОЭЛЕКТРОННАЯ ЗАЩИТА СТАНЦИИ СПУТНИКОВОЙ СВЯЗИ**

Радиоэлектронная защита – это совокупность мероприятий и действий войск (вооружённых сил) по устраниению или ослаблению воздействия на свои радиоэлектронные объекты средств радиоэлектронного поражения противника, защите от поражения самонаводящимся на излучение оружием, защите от непреднамеренных взаимных радиопомех и от технических средств радиоэлектронной разведки противника [1–3].

Меры технического характера по радиоэлектронной защите реализуются на этапах разработки образца в промышленности в соответствии с техническим заданием, и осуществляются личным составом экипажей станции в период эксплуатации, с помощью специальных средств защиты от помех, самонаводящегося оружия, воздействия ионизирующих и электромагнитных излучений. Основными техническими средствами являются:

- правильный выбор частотного диапазона;
- выбор принципов работы (построения) приемных и передающих устройств, видов сигналов и методов их обработки;
- применение устройств изменения рабочих частот, мощности передатчиков, направления излучения и приема сигналов;
- выполнение требований к характеристикам излучения и приема сигналов в широкой полосе частот.

Организационные мероприятия по радиоэлектронной защите обеспечиваются:

- выбором способов использования станций спутниковой связи;
- соблюдением временных, частотных, пространственных и других ограничений на работу радиоэлектронных средств;
- применением различных диапазонов с различными ретрансляторами и методами обработки сигналов;
- соблюдением порядка использования специальных способов, средств и устройств радиоэлектронной защиты;
- правильным размещением станции спутниковой связи на местности с учетом экранирующих свойств местности и местных предметов, а также соблюдением норм частотно-территориального разноса;
- соблюдением установленного порядка работы, условий, приоритета и запретов при работе станции спутниковой связи;
- своевременным выявлением источников преднамеренных помех и принятием мер по исключению (снижению) их влияния;
- организацией поиска, своевременным выявлением к уничтожению забрасываемых передатчиков помех;
- подготовкой экипажей к работе в условиях ведения радиоэлектронной борьбы и воздействия непреднамеренных помех радиоэлектронных средств.

Основными способами радиоэлектронной защиты станций от отдельных видов воздействия противника является совокупность технических мер и организационных мероприятий, направленных на предотвращение или снижение эффективности воздействия преднамеренных помех, создаваемых противником.

К основным способам защиты относится обеспечение связи в помехозащищенном режиме. В этом случае, защита от помех обеспечивается за счет применения фазоманипулированных широкополосных псевдослучайных сигналов (ФМ-ШПС). Спутниковая связь с использованием данного режима аппаратуры обеспечивается только через стволы, работающие в режиме прямой ретрансляции сигналов.

Номера дежурного расчета (начальник станции) при появлении помех и сбоев синхронизации аппаратуры уплотнения должен немедленно сообщить об этом старшему станции сети. Изменение режима работы осуществляется по команде старшего станции.

Защита станции от самонаводящегося оружия обеспечивается:

- периодической сменой боевых позиций;
- максимальным использованием маскирующих свойств местности, маскировкой аппаратной штатными и подручными средствами;
- инженерным оборудованием позиции станции;
- выносом электропитающих агрегатов на максимальную длину электропитающего кабеля, их укрытием и созданием теплоизоляционных экранов над ними;
- оборудованием укрытий для личного состава дежурной смены;

- установкой тепловых ловушек;

Защита станций спутниковой связи от ионизирующих и электромагнитных излучений она обеспечивается:

- согласованным маневром частотами и режимами работы в зависимости от условий распространения радиоволн;
- использованием обходных направлений связи и дублированием станций спутниковой связи;
- оперативным доведением до дежурных смен станций спутниковой связи информации о радиационной обстановке и областях повышенной ионизации;
- техническими мерами защиты (экраны, разрядники, заземление и др.).

Обеспечение электромагнитной совместимости станций спутниковой связи – есть совокупность технических мер и организационных мероприятий, направленных на предотвращение или снижение степени воздействия непреднамеренных помех на станции СС.

Она достигается:

- оптимальным распределением и назначением рабочих и запасных частот станциям спутниковой связи;
- размещением станций спутниковой связи с учетом рельефа местности и норм частотно-территориального разноса;
- введением временных, пространственных и частотных ограничений на работу станций спутниковой связи;
- своевременным выявлением источников непреднамеренных помех и принятием мер по исключению этих помех.

Ввиду того, что спутниковая связь централизованного управления в Вооруженных силах Российской Федерации, содержание и этапы выполнения основных мероприятий по защите станций спутниковой связи от комплексного воздействия противника планируются и реализуются централизованно – высшими органами управления СС.

#### **Список используемых источников**

1. **Защита от радиопомех** / М. В. Максимов, М. П. Бобнев, Б. Х. Кривицкий и др. – М. : Советское радио, 1976. – 496 с.
2. **Реализация широкополосных систем пространственной режекции помех** / И. П. Егоров, П. В. Русаков, Д. Д. Ганзий. – М. : Радиотехника, 2008. – № 2. – С. 90–92.
3. **Расцвет и кризис спутниковой связи** / Л. Я. Кантор. – М. : Электросвязь, 2007. – № 7.

УДК 004.056.5

**Н. А. Вьюговская (студентка группы ИКТВ-32 СПбГУТ)**  
**А. К. Сагдеев (преподаватель УВЦ ИВО СПбГУТ)**

## **АЛГОРИТМ ФУНКЦИОНИРОВАНИЯ И ПРЕДЛОЖЕНИЯ ПО СОСТАВУ АППАРАТНОЙ КОНТРОЛЯ БЕЗОПАСНОСТИ СВЯЗИ В СЕТЯХ СВЯЗИ ВОЕННОГО НАЗНАЧЕНИЯ**

Обеспечение безопасности связи – одна из важнейших составных частей общей системы мер по сохранению сведений в военной области, составляющих государственную тайну. Оно взаимосвязано с мероприятиями скрытого управления войсками, оперативной маскировки и режимом секретности. Непременным условием достижения безопасности связи является систематическое проведение квалифицированного контроля организации и состояния безопасности связи [1].

Под контролем безопасности связи (КБС) будем понимать комплекс организационных и технических мероприятий, направленных на установление факта, содержания, времени совершения нарушений безопасности связи, а также на предупреждение и пресечение этих нарушений установленным порядком [2].

Для ведения контроля безопасности связи на действующих линиях связи в Вооруженных Силах (ВС) Российской Федерации (РФ) создана единая система контроля безопасности связи, сложившаяся исторически как система внешнего контроля, в которой практически отсутствуют средства для ведения сетевого контроля безопасности связи.

В общевойсковой армии контроль безопасности связи осуществляется пунктом контроля безопасности связи, который представляет собой трех машинный вариант комплекса контроля безопасности связи Р-452КС. Он предназначен для контроля обеспечения безопасности связи на радио- и радиорелейных линиях связи в диапазоне частот от 1 до 500 МГц. Аппаратура комплекса контроля безопасности связи Р-452КС размещена на шасси трех автомобилей ЗИЛ-131.

Всего комплекс контроля безопасности связи Р-452КС обеспечивает развертывание одиннадцать постов контроля безопасности связи, характеристика которых представлена в таблице.

ТАБЛИЦА. Характеристика постов контроля безопасности связи

№ п/п	Наименование аппаратных	Количество постов контроля безопасности связи		
		КВ, слух.	УКВ, слух.	БПЧ
1.	AM-1	5	-	-
2.	AM-2	1	3	-
3.	AM-4	-	-	2
Всего постов		6	3	2

Проведенный анализ возможностей комплекса Р-452КС показал, что имеющиеся в его составе средства не позволяют вести контроль безопасности связи при передаче информации базовыми станциями по цифровым каналам управления в системах связи с подвижными объектами (ССПО) стандартов *MPT-1327* и *TETRA*, а также при передаче информации базовыми станциями по цифровым информационным каналам в ССПО стандарта *TETRA*. Таким образом, можно сделать вывод о том, что состоящий на вооружении комплекс Р-452КС не позволяет вести эффективный контроль безопасности связи в существующих и перспективных ССПО военного назначения.

Таким образом, в настоящее время имеется необходимость обоснования состава разрабатываемого подвижного комплекса контроля безопасности связи.

Для повышения эффективности ведения контроля безопасности связи в сети связи с подвижными объектами военного назначения предлагается следующий алгоритм функционирования подвижной аппаратной контроля безопасности связи (ПА КБС), представленный на рисунке [1-3].

В блоке 1 осуществляется непрерывный контроль каналов управления всех базовых станций доступных ПА КБС с требуемой вероятностью электромагнитной доступности.

В блоке 2 проверяется условие: есть ли управляющий сигнал запроса готовности от одной из базовых станций, контролируемых ПА КБС. Если управляющий сигнал запроса готовности от одной из базовых станций есть, то переходят к блоку 3, в обратном случае переходят к блоку 1.

В блоке 3 по управляющему сигналу запроса готовности, передаваемому базовой станцией по каналу управления, осуществляется определение адресов вызывающей и вызываемой абонентских станций.

В блоке 4 проверяется условие: есть ли управляющий сигнал перехода от базовой станции. Если управляющий сигнал перехода есть, то переходят к блоку 5, в обратном случае переходят к блоку 1.

В блоке 5 по управляющему сигналу перехода осуществляется определение номинала частоты информационного канала, по которому базовая

станция будет передавать информацию подвижному абоненту, находящемуся в ее зоне обслуживания, от его собеседника.

В блоке 6 проверяется условие: свободен ли первый оператор поста контроля. Если первый оператор поста контроля свободен, то переходят к блоку 7, в обратном случае переходят к блоку 12.

В блоке 12 проверяется условие: свободен ли второй оператор поста контроля. Если второй оператор поста контроля свободен, то переходят к блоку 13, в обратном случае переходят к блоку 18.

В блоке 18 проверяется условие: свободен ли третий оператор поста контроля. Если третий оператор поста контроля свободен, то переходят к блоку 19, в обратном случае переходят к блоку 24.

В блоке 24 проверяется условие: свободен ли четвертый оператор поста контроля. Если четвертый оператор поста контроля свободен, то переходят к блоку 25, в обратном случае переходят к блоку 1.

В блоках 7, 13, 19, 25 осуществляется контроль информационных каналов базовых станций соответственно первым, вторым, третьим и четвертым операторами постов контроля с целью выявления возможных нарушений безопасности связи, а также осуществляется запись контролируемых сеансов связи на жесткий диск ПЭВМ каждого поста контроля.

В блоке 8 проверяется условие: выявлено ли нарушение безопасности связи первым оператором поста контроля. Если первый оператор поста контроля выявил нарушение безопасности связи, то переходят к блоку 9, в обратном случае переходят к блоку 32.

В блоке 14 проверяется условие: выявлено ли нарушение безопасности связи вторым оператором поста контроля. Если второй оператор поста контроля выявил нарушение безопасности связи, то переходят к блоку 15, в обратном случае переходят к блоку 32.

В блоке 20 проверяется условие: выявлено ли нарушение безопасности связи третьим оператором поста контроля. Если третий оператор поста контроля выявил нарушение безопасности связи, то переходят к блоку 21, в обратном случае переходят к блоку 32.

В блоке 26 проверяется условие: выявлено ли нарушение безопасности связи четвертым оператором поста контроля. Если четвертый оператор поста контроля выявил нарушение безопасности связи, то переходят к блоку 27, в обратном случае переходят к блоку 32.

В блоках 9, 15, 21, 27 осуществляется определение категорий нарушений безопасности связи соответственно первым, вторым, третьим и четвертым операторами постов контроля согласно принятой классификации нарушений.

В блоках 10, 16, 22, 28 осуществляются доклады начальнику аппаратурной о фактах совершения нарушений безопасности связи соответственно первым, вторым, третьим и четвертым операторами постов контроля с использованием внутриобъектовой локальной вычислительной сети [3]. При

этом в докладах указываются адреса абонентских станций, время совершения и категории нарушений безопасности связи.

В блоках 11, 17, 23, 29 проверяется условие: свободен ли начальник аппаратной. Если начальник аппаратной свободен, то переходят к блоку 30, в обратном случае переходят к блоку 1.

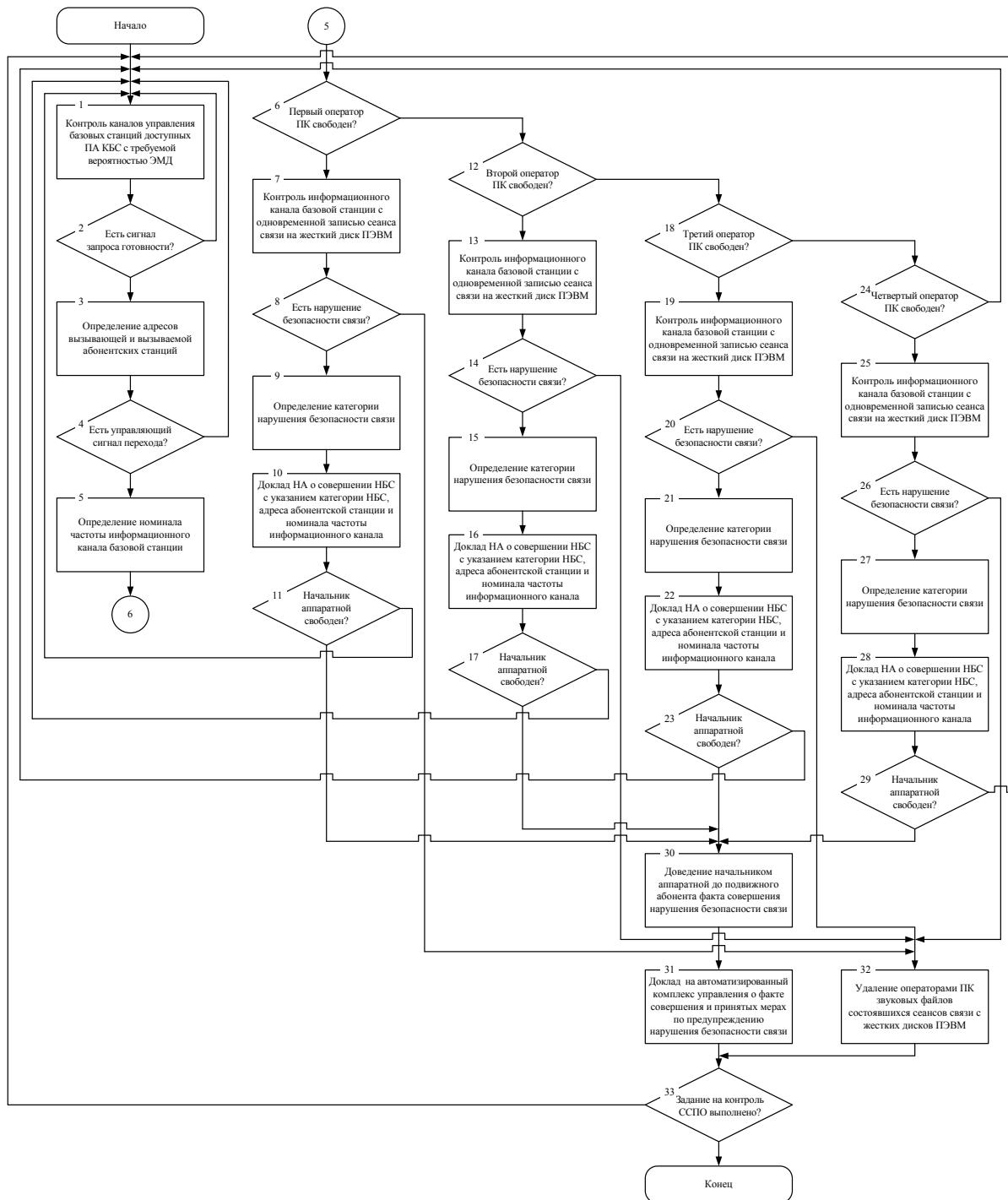


Рисунок. Алгоритм функционирования ПА КБС при ведении контроля в сети связи с подвижными объектами военного назначения

В блоке 30 осуществляется подключение начальника аппаратной к разговорам подвижных абонентов для доведения им факта совершения нарушения безопасности связи путем передачи установленной фразы, используя сервисные возможности современных сетей связи с подвижными объектами.

В блоке 31 осуществляется доклад начальником аппаратной о факте совершения и принятых мерах по предупреждению нарушений безопасности связи на автоматизированный комплекс управления.

В блоке 32 осуществляется удаление операторами постов контроля с жестких дисков ПЭВМ звуковых файлов состоявшихся сеансов связи, при контроле которых не были выявлены нарушения безопасности связи.

В блоке 33 проверяется условие: выполнено ли задание на контроль сети связи с подвижными объектами, указанное в схеме-приказе подвижной аппаратной контроля безопасности связи. Если задание на контроль сети связи с подвижными объектами выполнено, то контроль прекращается, в обратном случае переходят к блоку 1.

Разработанный алгоритм позволил сформулировать предложения по составу подвижной аппаратной контроля безопасности связи [4].

Для эффективного ведения контроля безопасности связи в существующих и перспективных ССПО военного назначения необходимо следующее количество приемных каналов:

- семь каналов для непрерывного контроля каналов управления базовых станций (по максимальному количеству базовых станций доступных каждой ПА КБС с требуемой вероятностью электромагнитной доступности);
- четыре канала для контроля информационных каналов базовых станций (по количеству постов операторов постов контроля).

Кроме того, требуется один приемный канал начальнику аппаратной для выборочного контроля работы постов операторов контроля и поста экспресс-анализа радиоэлектронной обстановки и технического анализа и два приемных канала для радиопеленгования на посту экспресс-анализа радиоэлектронной обстановки и технического анализа [4].

#### **Список используемых источников**

1. Радиоинтерфейсы наземных систем мобильного радиосервиса / В. В. Дурынин, Ю. Л. Хохленко, В. Д. Чельшев, В. В. Якимовец. – СПб. : ВАС, 2008. – 236 с.
2. Контроль безопасности связи и информации: учебн. пособие / Ю. И. Стародубцев, В. С. Киреев, О. К. Савицкий, М. М. Тараксин. – СПб. : ВАС, 2010. – 292 с.
3. Цифровая связь. Теоретические основы и практическое применение / Б. Склар. – М. : Вильямс, 2003. – 1104 с.
4. Контроль безопасности связи в сети связи с подвижными объектами военного назначения / В. М. Величко, А. К. Сагдеев // Международная научно-практическая

конференция «Наука и образование: проблемы и тенденции развития»: материалы конференции. – Уфа, 20–21 декабря 2013: в 3-х ч. Часть II. – Уфа: РИЦ БашГУ, 2013. – С. 119–125.

**УДК 621.3.052**

**А. М. Галкин (доцент кафедры СС СПбГУТ)**  
**С. М. Кадашников (студент группы МТВ-93 СПбГУТ)**

## **ОБОСНОВАНИЕ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ DWDM НА СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ**

Последние несколько десятилетий потребности людей в обмене информацией растут высокими темпами. Быстрая и надежная передача разнородной информации (видео, голоса, данных) необходима для развития экономики и общества в целом. Оптическое волокно способно передавать большое количество информации благодаря своей огромной пропускной способности. Поэтому развитие и внедрение оптических технологий в телекоммуникации – это основной путь удовлетворения растущих потребностей общества в обмене информацией. Однако скорость передачи сигналов по единичному каналу ограничивается быстродействием оптических передатчиков и приемников, осуществляющих электронно-оптическое и обратное преобразование. Максимальная скорость передачи информации с помощью систем связи, применяемых на сетях доступа, составляет 10 Гбит/с.

На сегодняшний день созданы и испытаны системы СЦИ работающие со скоростью до 40 Гбит/с, однако, их широкое внедрение в промышленную эксплуатацию затруднено по экономическим причинам, так как существует нерешенная проблема с оптической физической средой.

Несмотря на это, существуют системы спектрального разделения каналов передачи (WDM), которые позволяют многократно (более чем в 100 раз) увеличить суммарный поток передаваемой информации по одному волокну. Вследствие чего, открывается возможность значительно увеличить пропускную способность передачи информации между региональными узлами на глобальных сетях. Это актуально для сетей связи России с ее огромными расстояниями, малой населенностью и суровыми климатическими условиями при разработке линий связи с протяженностью от 300 до 500 км по малонаселенной и труднодоступной территории. Основные требования в нашей стране – это отсутствие промежуточных пунктов обслуживания и экономичность предлагаемого решения. Данные требования

позволяют решить сверхдлинные однопролетные DWDM-системы связи [1–3].

Оптическое мультиплексирование с разделением по длине волны (*Wavelength Division Multiplexing*, WDM) – сравнительно новая технология оптического (или спектрального) уплотнения, которая была предложена в 1980 г. Дж. П. Лауде (компания *Instruments SA*).

Сущность метода WDM заключается в одновременной передаче по одному волокну независимых сигналов компонентами светового пучка с различными длинами волн (разных цветов). Каждая компонента с определенной длиной волны представляет собой отдельный оптический канал передачи информации со своим передатчиком и приемником. Выражаясь простым языком, это гибкая технология, т. е. составляющие сигнала могут передавать цифровые потоки, сформированные на основе различных транспортных технологий - ATM, SDH, PDH и т. д. (рис. 1) Грубо говоря – дорога по которой ездит множество транспортных средств различных габаритов.

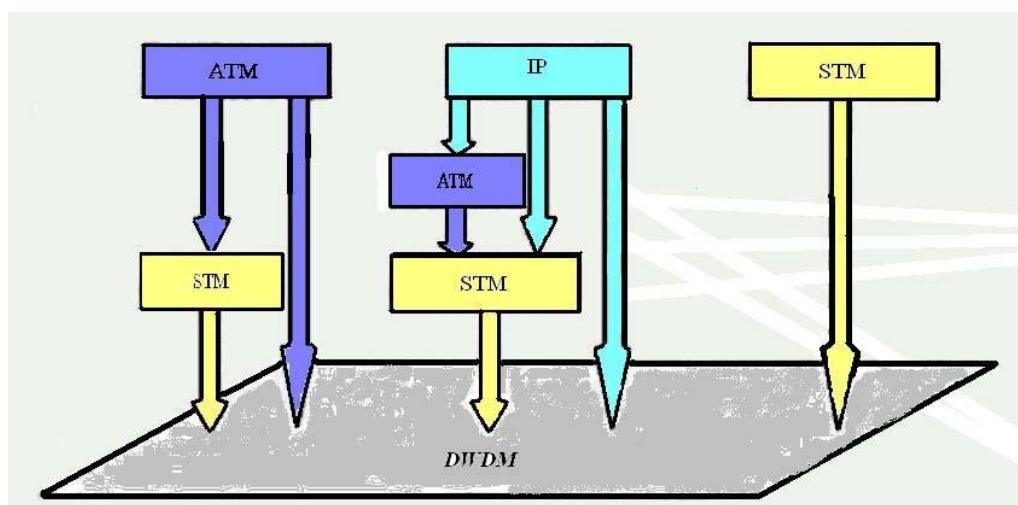


Рис. 1. Пример схемы реализации различных транспортных технологий с помощью спектрального мультиплексирования

В настоящее время принято выделять три типа WDM-мультиплексоров: обычные (CWDM), плотные (DWDM), высокоплотные (HDWDM):

- CWDM-системы – имеют частотный разнос каналов не менее 200 ГГц, сейчас позволяют мультиплексировать не более восьми каналов;
- DWDM-системы – обеспечивают разнос каналов от 100 до 50 ГГц и дают возможность мультиплексировать не более 32–40 каналов;
- HDWDM-системы – поддерживают разнос каналов 50 ГГц и менее, в настоящее время позволяют мультиплексировать не менее 40 каналов.

В городских транспортных сетях широко используется технология DWDM.

Принцип работы WDM-систем поясняет рис. 2.

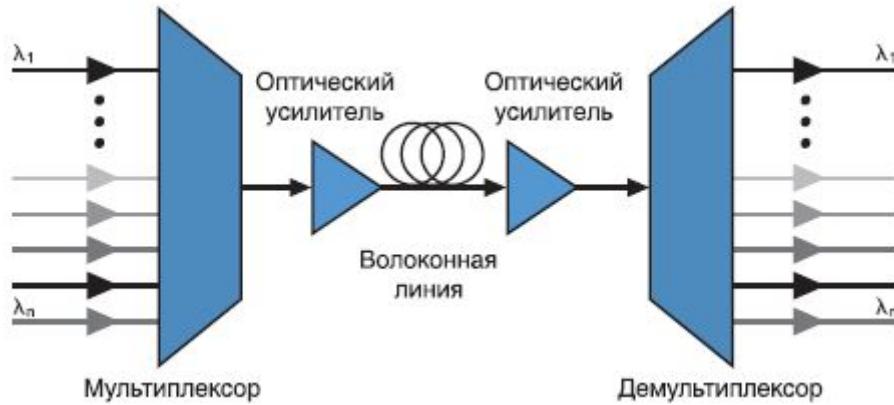


Рис. 2. Принцип работы WDM-систем

Световые сигналы с разными длинами волн, генерируемые несколькими оптическими передатчиками (транспондерами), объединяются мультиплексором и вводятся в оптическое волокно линии связи. При больших расстояниях передачи на линии связи устанавливается один или несколько оптических усилителей. На приемном конце линии связи демультиплексор принимает составной сигнал, выделяет из него исходные компоненты с разными длинами волн и направляет их на соответствующие фотоприемники. Такая система передачи «точка-точка» обеспечивает увеличение пропускной способности линии связи между двумя узлами. Однако возможности и преимущества технологии WDM в еще большей степени раскрываются в сложных насыщенных сетях связи, содержащих много различных узлов. На промежуточных узлах некоторые каналы могут быть добавлены или выделены из составного сигнала посредством мультиплексоров ввода/вывода, а остальные каналы проходят через узел без преобразования в электрический сигнал (рис. 3).

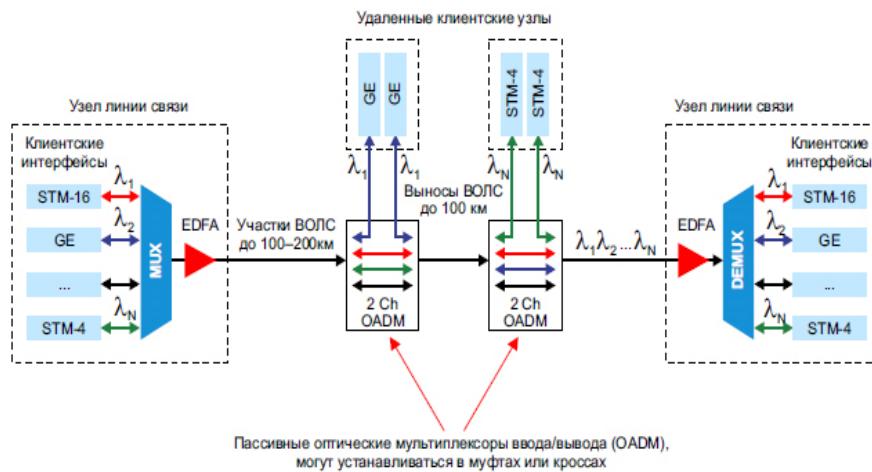


Рис. 3. WDM – система с использованием оптических мультиплексоров

Использованием и дальнейшим развитием технологии спектрального мультиплексирования занимаются все ведущие иностранные фирмы-производители, но наряду с ними существует Российский производитель создающий оборудование мирового класса. Российская компания «Т8» способна заменить таких гигантов как *Cisco*, *Juniper*, *Huawei* в данном сегменте. Оборудование «Т8» отвечает международным стандартом и является конфигурированным под разные задачи. А так же не маловажным является то, что это компания не первый год побивает мировые рекорды по передачи сигнала 100 Гбит/с в однопролетном режиме.

Модернизация сети связи специального назначения назрела давно. Более того, на высоком уровне начинают открыто обсуждаться вопросы безопасности каналов связи, недекларированных возможностей иностранного оборудования, устойчивости сети связи к несанкционированным воздействиям, а так же требования компании, имеющим статус отечественного производителя, а оборудование должно быть в реестре инновационной продукции, рекомендованной к закупкам в рамках 94-ФЗ и 223-ФЗ законов.

Такая сеть должна быть реализована как телекоммуникационная сеть со стратегической инфраструктурой, а применение иностранного оборудования запрещено. Отечественные производители предлагают полный спектр канaloобразующего DWDM- и CWDM-оборудования для построения сетей связи специального назначения любого масштаба, с реализацией специфических функций.

#### **Список используемых источников**

1. **Спектральное** уплотнение каналов [Электронный ресурс]. – Режим доступа: [http://ru.wikipedia.org/wiki/Спектральное\\_уплотнение\\_каналов](http://ru.wikipedia.org/wiki/Спектральное_уплотнение_каналов). (Дата обращения 22.04.2014).
2. **Основы** технологии спектрального мультиплексирования каналов передачи (wdm) / О. Е. Наний // Lightwave Russian Edition. – 2004. – № 2.
3. **Шанс** для отечественных производителей / В. Трещиков // Технологии и средства связи. – 2014. – № 1.

УДК 621.317.7

**О. А. Гильдеева (доцент кафедры ЭБЖД СПбГУТ)**  
**В. А. Савостина (студентка гр. ЭП-21 СПбГУТ)**

## **ИНОВАЦИОННЫЕ РЕШЕНИЯ В ОБЛАСТИ РАДИОЗОНДИРОВАНИЯ АТМОСФЕРЫ**

В последнее время в мире существенно возросло значение метеорологической информации, вследствие увеличения количества опасных природных явлений и неблагоприятных погодных условий, при которых гибнут сотни тысяч человек, а экономический ущерб достигает многие млрд. долларов.

По установившейся практике метеонаблюдений для получения метеорологической информации в атмосферу выпускаются в свободный полёт небольшие лёгкие измерительные приборы, радиозонды, снабжённые датчиками различных метеорологических параметров и радиопередатчиком. Радиозондирование представляет наиболее точные результаты непосредственных контактных измерений термодинамических параметров атмосферы на высотах от уровня земли до 35...40 км. Эти данные содержат информацию о вертикальных профилях температуры, влажности, скорости и направлении ветра, а также о давлении воздуха на заданных уровнях. Аэрологический радиозонд производит преобразование нескольких метеовеличин в радиотелеметрические сигналы и передает их по радиоканалу на наземную станцию сопровождения. Наземное оборудование аэрологических станций – аэрологический регистрационно-вычислительный комплекс РЛС, радиотеодолит или какая-либо навигационная система – обеспечивает сопровождение радиозонда в полёте, определение его координат (и тем самым измерение высоты самого зонда и параметров ветра), приём и регистрацию радиотелеметрических сигналов. В состав наземного оборудования входят также устройства для обработки сигналов радиозонда, подготовки и передачи потребителям аэрологического сообщения. В настоящее время на аэрологической сети действуют основные радиолокационные комплексы АВК-1, АВК-1М, РЛС нового поколения МАРЛ, а с 2008 г. – РЛС Вектор-М.

С момента создания первого отечественного радиозонда в 1930 г. изобретателем П. А. Молчановым, наряду с разработками по усовершенствованию техники и методики радиозондирования проводились исследования точности радиозондовых измерений. За многие десятилетия техника и методы радиозондирования атмосферы прошла целый ряд качественных этапов, которые характеризовались увеличением высоты, автоматизацией измерений и обработки данных. При этом совершенствование техники и

метода радиозондирования атмосферы всегда было тесно связано с развитием радиоэлектроники и, по сути, отражало достижения в этой области.

К 1982 г. была создана аэрологическая сеть СССР, насчитывающая около 200 станций, был разработан транзисторный радиозонд МАРЗ и начато серийное производство. Госстандарт СССР аттестовал его как средство измерений.

В 1998–2001 гг. было освоено серийное производство новой радиолокационной станции (РЛС) МАРЛ, основанной на современной элементной базе и принципах обработки сигналов. Станция МАРЛ выполнена в виде одноблочной конструкции. Из производственного цикла были исключены работы по изготовлению точной механики для системы сопровождения радиозонда. В качестве антенны используется активная фазированная антенна решетка (АФАР). Станция МАРЛ автоматически находит и сопровождает зонд в полёте, выдаёт его текущие координаты, принимает и обрабатывает метеорологическую информацию.

В рамках изучения дисциплины «Учение об атмосфере» кафедрой Экологии и БЖД организовано взаимодействие с действующей станцией метеонаблюдений ГГО им. А. И. Войкова, на которой регулярно производится запуск радиозондов. На рисунке 1 студенты группы ОП-21 во время посещения музея метеостанции, расположенной в пос. Войкова.



Рис. 1. Студенты ЭП-21 и преподаватели кафедры ЭиБЖД в музее ГГО

В настоящее время в практике радиозондирования применяются отечественные и зарубежные радиозонды. Известны радиозонды фирмы *VAISALA*, в которых используются емкостные чувствительные элементы для преобразования температуры, влажности и атмосферного давления в частотные телеметрические сигналы. Недостатком измерительных устройств этих радиозондов является схемная сложность, так как требует-

ся высокая чувствительность измерения емкости, например, при изменении температуры на 100 К емкость датчика изменяется всего на 7-8 пФ [1].

Разработаны радиозонды с низкоомными датчиками температуры. Недостатком этих устройств является также схемная сложность ввиду того, что нужно учитывать сопротивление проводов, которое изменяется в зависимости от окружающей температуры и приводит к возникновению термо – ЭДС в цепи преобразования.

Применяемый на сегодня серийный радиозонд МРЗ-3А [1], в котором происходит преобразование сопротивлений двух резистивных датчиков (температуры и влажности воздуха) в частотные сигналы, имеет недостаток в виде высокой погрешности измерения, особенно на больших высотах.

Известен преобразователь давления в электрический сигнал, в котором в качестве чувствительного элемента используется мостовой тензорезисторный преобразователь, сформированный на деформируемой мембране [2]. Данный преобразователь содержит тензорезисторный мост, дифференциальный усилитель, переключатель, резистивный делитель, блок ослабления напряжения. Недостатком преобразователя является температурная зависимость коэффициента тензочувствительности и начального разбаланса тензомоста.

Принцип действия любого преобразователя давления заключается в преобразовании давления, испытываемого чувствительным элементом, в электрический сигнал [3] и при необходимости обработка (усиление, термокомпенсация и др.). По способу преобразования механического перемещения в электрический сигнал выделяют различные виды преобразователей давления: потенциометрические, индуктивные, емкостные, тензорезистивные, оптические, пьезоэлектрические, пьезорезонансные преобразователи на объемных волнах [4–9].

Структурная схема датчика на объемных акустических волнах приведена на рисунке 2.



Рис. 2. Структурная схема датчика, где БЧЭ – блок чувствительных элементов

В настоящее время особую актуальность приобретает постановка задач по целесообразности разработок современных датчиков, внедрения и освоения их производства и, соответственно, переработки программного обеспечения обработки данных радиозондирования на основе учёта метрологических характеристик инновационных радиозондов и конкретных условий проведения измерений.

На 68 региональной научно-практической конференции представлен новый, разработанный в ОАО «Авангард» Санкт-Петербург, датчик воздушного давления для аэрологических радиозондов. Датчик предназначен для преобразования, подаваемого на него избыточного абсолютного давления воздуха, в цифровой код измеряемой величины. Датчик воздушного давления акустоэлектронный интерфейсный (ДДАЭ-И) относится к измерительной технике и может быть использован в метеорологических радиозондах для измерения вертикального профиля давления в атмосфере [5]. Анализ технических решений по созданию инноваций в области радиозондирования атмосферы приводит к заключению о том, что акустоэлектронные устройства могут являться одними из наиболее перспективных в решении данной проблемы.

Общий вид датчика давления ДДАЭ-И в разрезе представлен на рисунке 3. Основные характеристики ДДАЭ-И приведены в таблице.

ТАБЛИЦА. Основные характеристики ДДАЭ-И

Наименование параметров	Значение параметров
Диапазон измеряемого давления	8...2300 мм рт. ст.
Погрешность измерения	0,02 %
Диапазон рабочих температур	-60...+85 °C
Энергопотребление – не выше	1 Вт
Габаритные размеры корпуса не более	100×50×50 мм
Вид выходного сигнала	цифровой в стандарте RS 485



Рис. 3. Датчик давления ДДАЭ-И в разобранном виде

Прогнозируется, что использование акустоэлектронных сенсоров и датчиков давления на их основе сможет найти свое место как в случае классических вариантов приборного обеспечения радиозондирования атмосферы, так и в ряду перспективных технических решений при создании

специализированной автоматической метеорологической наблюдательной сети на базе вышек сотовой связи. Идея необходимости и целесообразности разработки подобной сети проработана авторами М. Б. Фридзон, Ю. М. Ермошенко [10].

Не исключена, также, возможность проработки вариантов применения акустоэлектронных датчиков давления с цифровым выходным сигналом при создании отечественной системы зондирования нового поколения – системы радиозондирования с использованием спутниковых навигационных систем *GPS* и ГЛОНАСС.

### Список использованной литературы

1. **Аэрология** / Н. А. Зайцев. – Ленинград : Гидрометеоиздат, 1990. – С. 187–191.
2. **Пат. SU 1610327 A1 СССР, G 01 L 9/04.** Преобразователь давления в электрический сигнал / Х.Н. Гайнанов, С.П. Ессяк, С.Г. Осипова и Г.С. Ранченко; заявитель и патентообладатель Уральский полит. ин-т им. С.М. Макарова – № 4447237/24-10; заявл. 27.06.88; опубл. 30.11.90, Бюл. № 44 – 3 с. : ил.
3. **Современные датчики.** Справочник / Дж. Фрайден. – М. : Техносфера, 2006.
4. **Пьезорезонансные датчики** / В. В. Малов. – М. : Энергоатомиздат, 1989.
5. **Датчик давления** акустоэлектронный / Д. М. Силаков, Д. Ю. Захаров // Сб. тр. международной научно-практической конференции НИУ ИТМО СПб «Sensorica 2013». – С. 26–28.
6. **О состоянии и перспективах развития** полупроводниковой электроники в России / Ж. И. Алферов // Нано и микросистемная техника. – 2005. – № 8. – С. 2–17.
7. **Перспективные ПАВ-датчики** / Н. Елисеев // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. – 2008. – № 1. – С. 40–45.
8. **Разработка и исследование частотных датчиков** механических величин на основе управляемых пьезоструктур: автореф. дис. канд. техн. наук / В. В. Малов. – М., 1971.
9. **Адаптивный алгоритм обработки** измерительной информации / Ю. О. Уразбахтина, Е. С. Хрусталева // Датчики и системы. – 2008. – № 8. – С. 22–24.
10. **Создание с минимальными затратами** специализированной автоматической метеорологической наблюдательной сети на базе вышек сотовой связи с целью повышения достоверности и надежности прогнозов опасных явлений погоды [Электронный ресурс] / М. Б. Фридзон, Ю. М. Ермошенко. – Метеорология и гидрология. – 2009. – № 2. – С. 93–100. – Режим доступа: [http://www.zondr.ru/userfiles/file/sozdanie\\_s\\_min.htm](http://www.zondr.ru/userfiles/file/sozdanie_s_min.htm).

*Статья подготовлена под научным руководством заведующего кафедрой ЭБЖД канд. воен. наук С. А. Панихицкова и канд. техн. наук, доцента кафедры ЭБЖД Н. Е. Манвеловой*

УДК 621.391

В. П. Грецев (доцент кафедры ВАС)  
С. В. Дьяков (доцент кафедры ВАС)  
С. Е. Иванов (заместитель начальника кафедры ВАС)  
А. В. Семизоров (курсант группы 1021 ВАС)

## ЗАДАНИЕ ИСХОДНЫХ ДАННЫХ АЛГОРИТМА СИНТЕЗА СИСТЕМЫ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ

В современных условиях поддержание оснащенности телекоммуникационных систем и сетей связи (ТКСС) на уровне необходимой достаточности может быть реализовано различными способами. Выбор рациональных требований к информационным направлениям (ИН) как составной части ТКСС на стадии НИОКР характеризуется большой степенью неопределенности ввиду того, что период использования по назначению отдален по времени иногда на довольно большой срок.

Одним из основных этапов оценивания надежности сложной информационной системы является этап разработки иерархически связанной системы показателей надежности (СПН) эксплуатации этой системы. Известно, что проблема обоснованной формулировки параметрического пространства состояний, обоснованности включения тех или иных показателей надежности (ПН) в состав синтезированной СПН и локальных СПН для последующего оценивания надежности ИН достаточно сложна, в т. ч. из-за их большой номенклатуры которые представлены в таблице [1, 2].

ТАБЛИЦА. Показатели надежности

Единичные			Комплексные
безотказность	восстанавливаемость	структурные	
вероятность безотказной работы	вероятность восстановления	сечение	коэффициент готовности
гамма-процентная наработка до отказа	гамма-процентное время восстановления	коэффициент связности	коэффициент оперативной готовности
средняя наработка до отказа	среднее время восстановления	вероятность связности	коэффициент технического использования
средняя наработка на отказ	интенсивность восстановления		коэффициент сохранения эффективности
интенсивность отказов	средняя трудоемкость восстановления		
параметр потока отказов			

Единичные			Комплексные
безотказность	восстанавливаемость	структурные	
осредненный параметр потока отказов			
вероятность сбоя			
гамма-процентная наработка на сбой			
средняя наработка на сбой			
интенсивность сбоя			
параметр потока сбоев			
осредненный параметр потока сбоев			

Для решения задач подобных типов применяется подход, основу которого составляет экспертизная система, предназначенная для снижения уровня неопределенности при формировании синтезируемой и локальных СПН, для прогнозирования состава данных систем по имеющимся априорным данным.

В разработанном алгоритме функционирования экстраполирующей нейронной сети (ЭНС) для синтеза СПН в условиях неполноты и противоречивости исходных данных и недостоверно заданных параметрах, характеризующих свойства ИН в различных условиях эксплуатации, в качестве исходных данных выступает множество ПН ИН, составляющих основу обобщенной СПН, и матрица связей, каждый элемент которой характеризует взаимосвязь, корреляционную зависимость ПН на  $k$ -м шаге эксплуатации ИН.

В ЭНС используется когнитивная карта, полностью задаваемая матрицей связей. Формирование когнитивных карт, где под когнитивной картой понимается ориентированный граф, узлы которого представляют собой некоторые объекты или концепты (в нашем случае – показатели надежности), а дуги – связи между ними, характеризующие причинно-следственные отношения, происходит следующим образом. Если увеличение (уменьшение) значения одного ПН приводит к увеличению (уменьшению) значения другого показателя, то причинная связь между ними положительна и наоборот. Отсутствие причинных связей между некоторыми ПН в конкретных условиях обстановки объективно закономерно и учитывается в когнитивной карте как ноль. В качестве примера представления знаний о причинных связях различных существенных свойств ИН, значений отклонений его ПН представлена когнитивная карта для семи концепт, характеризующая возможные причинно-следственные зависимости между некоторыми ПН ИН на  $k$ -ом шаге эксплуатации ИН:

концепт № 1 – показатель, характеризующий среднюю трудоемкость восстановления и имеющий физический смысл отклонения средней трудоемкости восстановления ИН от требуемых значений  $\Delta\bar{C}(k)$ ;

концепт № 2 – показатель, характеризующий среднее время восстановления и имеющий физический смысл отклонения среднего времени восстановления ИН от требуемых значений  $\Delta T_{\text{в}}(k)$ ;

концепт № 3 – показатель, характеризующий коэффициент сохранения эффективности и имеющий физический смысл отклонения коэффициента сохранения эффективности ПН от требуемых значений  $\Delta K_{\text{эф}}(k)$ ;

концепт № 4 – показатель, характеризующий среднюю наработку на отказ и имеющий физический смысл отклонения средней наработки на отказ ПН от требуемых значений  $\Delta\bar{T}(k)$ ;

концепт № 5 – показатель, характеризующий сечение ПН и имеющий физический смысл отклонения значения сечения ПН от требуемых значений  $\Delta S(k)$ ;

концепт № 6 – показатель, характеризующий среднюю наработку на сбой и имеющий физический смысл отклонения средней наработки на сбой ПН от требуемых значений  $\Delta\bar{T}_{\text{с}}(k)$ ;

концепт № 7 – показатель, характеризующий коэффициент оперативной готовности и имеющий физический смысл отклонения коэффициента оперативной готовности ПН от требуемых значений  $\Delta K_{\text{ор}}(k)$ .

Когнитивная карта полностью задается своей матрицей связей (матрицей весов), правила формирования которой описаны выражением (1).

$$\|\vec{W}(k)\| = \begin{vmatrix} w_{11}(k) & w_{12}(k) & \dots & w_{1n}(k) \\ w_{21}(k) & w_{22}(k) & \dots & w_{2n}(k) \\ \vdots & \vdots & \ddots & \vdots \\ w_{p1}(k) & w_{p2}(k) & \dots & w_{pn}(k) \end{vmatrix} \quad (1)$$

Для приведенного примера когнитивной карты матрица связей (весов) имеет вид (выражение (2)):

$$\|W(k)\| = \begin{bmatrix} 0 & -1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 0 & 1 & 0 & -1 \\ 1 & -1 & 1 & -1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 1 & 1 & 0 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & 0 \end{bmatrix} \quad (2)$$

Как правило, для составления подобных карт привлекают эксперта или группу экспертов. В их задачу входит установление параметрического пространства состояний – множества ПН (концепт), определяющих состояние объекта в выбранной предметной области (ИН, процессы, реализуемые в рамках эксплуатации ИН) и характера связей между этими концептами в конкретных условиях обстановки. Когнитивные карты позволяют естественным образом объединить знания нескольких экспертов в вопросах организации и управления связью, в вопросах влияния на ИН и реализуемые им процессы воздействий различного рода для более адекватного описания состояния данных процессов в различных условиях. Достоинством данного метода является возможность обобщения знаний различных экспертов в итоговой когнитивной карте, которая учитывает мнения всех привлеченных специалистов [3].

#### **Список используемых источников**

1. **Основы теории эффективности целенаправленных процессов / Г. Б. Петухов.** – М. : МО СССР, 1989. – 660 с.
2. **Кузнецов, В. Е. Диссертация... канд. техн. наук.** – СПб. : ВАС, 1998.
3. **Искусственные нейронные сети / М. А. Щербаков.** – Пенза : Изд. Пензенского государственного технического университета, 1996. – 85 с.

**УДК 391.7**

**В. В. Дворяков (доцент военной кафедры МИРЭИ)**  
**К. И. Стакеев (студент группы ИКТВ-33 СПбГУТ)**

### **МЕТОДОЛОГИЧЕСКИЕ ВОПРОСЫ СИНТЕЗА СТРУКТУРЫ СИСТЕМЫ СИНХРОНИЗАЦИИ НА ОСНОВЕ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СТРУКТУР**

Система синхронизации региональной транспортной сети связи специального назначения (СС РТСС СН) представляет собой иерархическую, многофункциональную и многоконтурную схему с достаточно сложными средствами связи, объединяющиеся в комплексах со встроенными функциями управления, мониторинга, анализа принятия решений и т. д. Данные комплексы распределены на значительной территории и входят в состав узлов связи различных уровней иерархии, которые соединены между собой каналами связи, обеспечивающих передачу информации, управления, сигнализации и синхронизации. Система СС РТСС СН предназначена для управления функциональными элементами (коммутационные и распреде-

лительные узлы магистральных, зоновых и местных сетей связи) при сквозном мониторинге характеристик подсистемы связи с подвижными объектами и обеспечение передачи, хранении и обработке информации заданного вида, выработке управляющих воздействий и контроле над их реализацией.

Появление новых образцов аппаратуры синхронизации с расширенными возможностями функций контроля и управления требуют совершенствования структуры СТСС и отдельных ее элементов.

Проблема структурного построения подобных систем включает распределение элементов и подсистем в пространстве; выбор комплекс технических средств, обеспечивающих выполнение функций управления с учетом пространственно-иерархического расположения; распределение множества функций по узлам системы с учетом применяемых технологий передачи информации и управления. При этом должны выполняться требования не только к качеству передаваемой информации, но и к качеству управления системы.

Решение задачи состоит в определении рационального отображения множества взаимосвязанных функций, выполняемых СС РТСС СН, на множество взаимосвязанных узлов связи с применяемыми на них техническими средствами при учете затрат на создание, развитие и функционирование системы, обеспечение требований по оперативности управления и устойчивости функционирования.

При синтезе структуры СС РТСС СН возникают задачи рационального распределения функций между всеми узлами связи, выбора технических средств в узлах и каналов связи между ними с учетом различных тактико-технических и технико-экономических характеристик [1].

Основными характеристиками, влияющими на выбор структуры СС РТСС, являются динамические и стохастические характеристики, связанные с функционированием системы управления и элементов системы.

СС РТСС СН должна обладать рядом характерных особенностей, основными из которых являются:

- *распределенность элементов СС РТСС СН*, которые располагаются на значительной территории от зонового до магистрального масштаба и включают в себя огромное количество управляемых и управляющих элементов;

- *подвижность элементов СС РТСС СН*. Включает в себя управляющие и управляемые объекты различных типов, которые могут быть подвижными или неподвижными. Движение элементов осуществляется постоянно или периодически по установленным (детерминированным) или неустановленным (стохастическим) траекториям;

- *наличие зон доступности СС РТСС СН*. Наличие функциональных взаимодействий между движущимися и неподвижными элементами в зоне или в узле доступа. Конфигурация зоны доступности определяется взаим-

ным расположением элементов в пространстве и типами применяемых средств связи;

– *быстродействие*. Необходимость в оперативно-технической выработке управляющих воздействий, обусловленной особенностями распределенной СС РТСС СН, которые накладывают высокие требования по быстродействию выполнения функций элементов;

– *недопустимость потерь информации*. Для ряда распределенных систем является важным недопустимость потерь информации определенного вида, что требует создание специальных мер защиты;

– *живучесть системы*. Во многих случаях функционирование СС РТСС СН протекает в условиях различных факторов воздействий, что приводит к нарушению нормальной работы отдельных элементов. Это определяет необходимость выполнения при синтезе структуры специальных мероприятий, направленных на повышение живучести системы.

При создании или совершенствовании СС РТСС СН важным этапом является разработка структуры системы. В общем случае задача синтеза структуры включает:

1. Определение оптимального числа, расположения и вариантов построения узлов СС РТСС СН.
2. Распределение функций управления по узлам и выбор варианта реализации задач управления.
3. Выбор мероприятий по обеспечению требуемой живучести системы.
4. Распределение функций и задач между средствами управления.
5. Выбор и распределение технических средств по узлам системы и т. д.

Анализ различных подходов к синтезу структуры СС РТСС СН показал, что задачи синтеза могут быть разбиты на две группы. К первой относятся задачи, связанные с синтезом топологической структуры системы, состоящей в определении состава, территориального расположения и типа управляющих узлов на всех уровнях иерархии системы и каналов связи между ними.

Ко второй группе относятся проблемы синтеза функциональной структуры системы, т.е. распределение функций управления между узлами системы, включая объект управления и распределение технических средств по узлам системы.

Последовательность задач и этапов синтеза структуры СС РТСС СН можно сформулировать следующим образом:

1. Формулировка задачи синтеза.
2. Обоснование и выбор критериев и характеристик вариантов построения структуры.
3. Определение состава узлов, в том числе и управления, и их взаимосвязей.

4. Формализация вариантов построения топологической структуры системы.
5. Определение состава функций и задач управления и их взаимосвязей.
6. Определение вариантов их выполнения.
7. Определение возможного набора технических средств выполнения функций и задач управления.
8. Модель оптимизации топологической структуры системы  $G_t$ .
9. Имитационная модель топологической структуры.
10. Блок анализа и коррекции решений.
11. Модель оптимизации функциональной структуры системы.
12. Имитационная модель функциональной структуры системы.
13. Блок анализа и коррекции решения.
14. Формализация вариантов выполнения функций и задач.
15. Формализация построения функциональной структуры системы.
16. Оптимальный (рациональный) вариант структуры СС РТСС СН.

На первоначальных этапах формулируются требования к разрабатываемой системе, выбирается и обосновывается состав учитываемых характеристик и критериев эффективности вариантов структуры системы. Определяется возможный состав узлов, варианты построения и территориальное расположение. Определяются функции управления в системе, которые необходимо детализировать до комплекса взаимоувязанных задач и вариантов их решения.

На следующем этапе сформированные варианты построения комплекса взаимосвязанных задач управления и варианты построения управляющих узлов, которые будут служить основой для формализации этапов синтеза топологической и функциональной структуры системы [2].

Таким образом, процесс синтеза структуры СС РТСС СН включает последовательность решения взаимоувязанных задач синтеза основных элементов и частей системы, которые позволяют произвести выбор наилучшего варианта всей системы по заданным критериям оптимальности. На каждом из этапов синтеза необходимо применять оптимизационно-имитационные процедуры с обязательной проработкой и уточнением вариантов построения отдельных подсистем, с учетом их динамических, а в некоторых и стохастических характеристик функционирования элементов управления и их взаимодействий между собой. При этом в процессе синтеза могут быть использованы итеративные схемы решения, с обязательной функцией возврата к предыдущим шагам синтеза с целью уточнения критериев и ограничений задач, состава и характеристик элементов топологической и функциональной структуры системы.

### **Список используемых источников**

1. Способы синхронизации цифровой сети и их классификация / Ю. А. Алексеев, В. А. Барков, М. Н. Колтунов // Электросвязь. – 1988. – № 10.
2. Имитационное моделирование в задачах синтеза структур сложных систем (оптимизационно-имитационный подход) / А. Д. Цвиркун, В. К. Акинфиев, В. А. Филиппов. – М. : Наука, 1985. – 174 с.

**УДК 654.16**

**В. Г. Ерышов (старший преподаватель ВАС)**  
**А. В. Давыдов (начальник кафедры ВАС)**  
**А. А. Панкин (преподаватель ВАС)**  
**П. А. Хайдакин (курсант группы 1221 ВАС)**

## **ПРОЦЕСС РАДИОКОНТРОЛЯ ИСПОЛЬЗОВАНИЯ РАДИОЧАСТОТНОГО СПЕКТРА**

Радиоконтроль (РК) использования радиочастотного спектра (РЧС) заключается в соблюдении установленных правил и процедуры его проведения. Задача РК заключается в обеспечении общего процесса управления использованием РЧС и решения проблем, связанных с обеспечением электромагнитной совместимости (ЭМС) радиоэлектронных средств (РЭС) [1].

При проведении РК проверяется соответствие технических параметров и параметров излучений РЭС данным их регистрации, требованиям технических регламентов, стандартов, норм и условиям, установленным в разрешениях на использование радиочастот или радиочастотных каналов соответствующим РЭС.

В случае обнаружения нарушений установленных правил использования РЧС и при необходимости определения параметров излучений РЭС может проводиться запись сигналов, контролируемых РЭС и реагирование на данные нарушения с целью их устранения.

Радиоконтроль осуществляется в целях [1]:

- выявления не разрешенных для использования РЭС и прекращения их работы;
- выявления источников радиопомех;
- выявления нарушения порядка и правил использования радиочастотного спектра, национальных стандартов, требований к параметрам излучения (приема) РЭС и (или) высокочастотных устройств;
- обеспечения ЭМС РЭС;
- обеспечения эксплуатационной готовности РЧС.

Процесс радиоконтроля можно представить ориентированным графом состояний и описать в терминах теории Марковских случайных процессов с дискретными состояниями и непрерывным временем. Под таким процессом будем понимать процесс, у которого в любой момент времени  $t$  множество его состояний  $S$  – счётно или конечно, а переходы из одного состояния в другое происходят в любой момент времени  $t$  наблюдаемого периода [2].

Будем полагать, что переходы из состояния в состояние происходят под воздействием пуассоновских потоков событий [2, 3]. Ориентированный граф состояний процесса радиоконтроля, описанного в терминах Марковских процессов с дискретными состояниями и непрерывным временем представлен на рисунке 1.

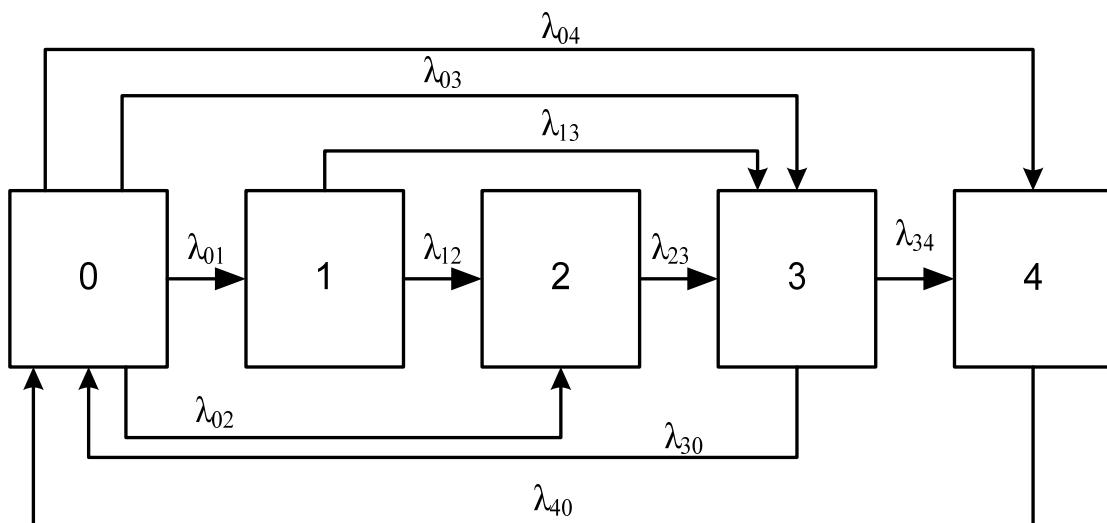


Рис. 1. Ориентированный граф состояний процесса радиоконтроля

Описание состояний процесса радиоконтроля, а также входящих и выходящих потоков его событий представлены в таблице.

ТАБЛИЦА. Состояние процесса радиоконтроля

№ п/п	Наименование состояния	$\lambda_{\text{вых}}$	$\lambda_{\text{вх}}$
$S_0$	Радиоконтроль	$\lambda_{01}, \lambda_{02}, \lambda_{03}, \lambda_{04}$	$\lambda_{30}, \lambda_{40}$
$S_1$	Анализ технических параметров и параметров излучений РЭС	$\lambda_{12}, \lambda_{13}$	$\lambda_{01}$
$S_2$	Определение местоположения РЭС	$\lambda_{23}$	$\lambda_{02}, \lambda_{12}$
$S_3$	Пресечение нарушений установленных правил использования РЧС	$\lambda_{30}, \lambda_{34}$	$\lambda_{03}, \lambda_{13}, \lambda_{23}$
$S_4$	Окончание радиоконтроля, документирование его результатов	$\lambda_{40}$	$\lambda_{04}, \lambda_{34}$

Составим для графа, представленного на рисунке 1, систему обыкновенных дифференциальных уравнений Колмогорова [2].

$$\begin{aligned}\frac{dp_0(t)}{dt} &= p_3(t)\lambda_{30} + p_4(t)\lambda_{40} - p_0(t)\{\lambda_{01} + \lambda_{02} + \lambda_{03}\} \\ \frac{dp_1(t)}{dt} &= p_0(t)\lambda_{01} - p_1(t)\{\lambda_{12} + \lambda_{13}\} \\ \frac{dp_2(t)}{dt} &= p_0(t)\lambda_{02} + p_1(t)\lambda_{12} - p_2(t)\lambda_{23} \\ \frac{dp_3(t)}{dt} &= p_0(t)\lambda_{03} + p_1(t)\lambda_{13} + p_2(t)\lambda_{23} - p_3(t)\{\lambda_{30} + \lambda_{34}\} \\ \frac{dp_4(t)}{dt} &= p_3(t)\lambda_{34} - p_4(t)\lambda_{40} \\ \sum_i^4 p_i(t) &= 1\end{aligned}$$

При этом рассмотрим частный случай, когда интенсивности событий не зависят от времени:  $\lambda_i(t) = \lambda_i = \text{const}$  (Марковский процесс является однородным [2–4]) и представляются в виде квадратной матрицы размером 5x5:

$$\|\lambda_i\| = \begin{pmatrix} 0 & \lambda_{12} & \lambda_{1j} & \lambda_{15} \\ \lambda_{21} & 0 & \lambda_{2j} & \lambda_{25} \\ \dots & \dots & \dots & \dots \\ \lambda_{51} & \lambda_{52} & \lambda_{5j} & 0 \end{pmatrix}$$

Решение системы уравнений Колмогорова было получено с помощью пакета математического программирования «Mathcad 2011». Результаты моделирования в виде графиков зависимости вероятностей состояний процесса радиоконтроля от времени, приведены на рисунке 2.

Таким образом, разработанная модель процесса радиоконтроля использования радиочастотного спектра, описанная в терминах теории случайных Марковских процессов позволила получить вероятностные и временные характеристики, описывающие состояния анализируемого процесса.

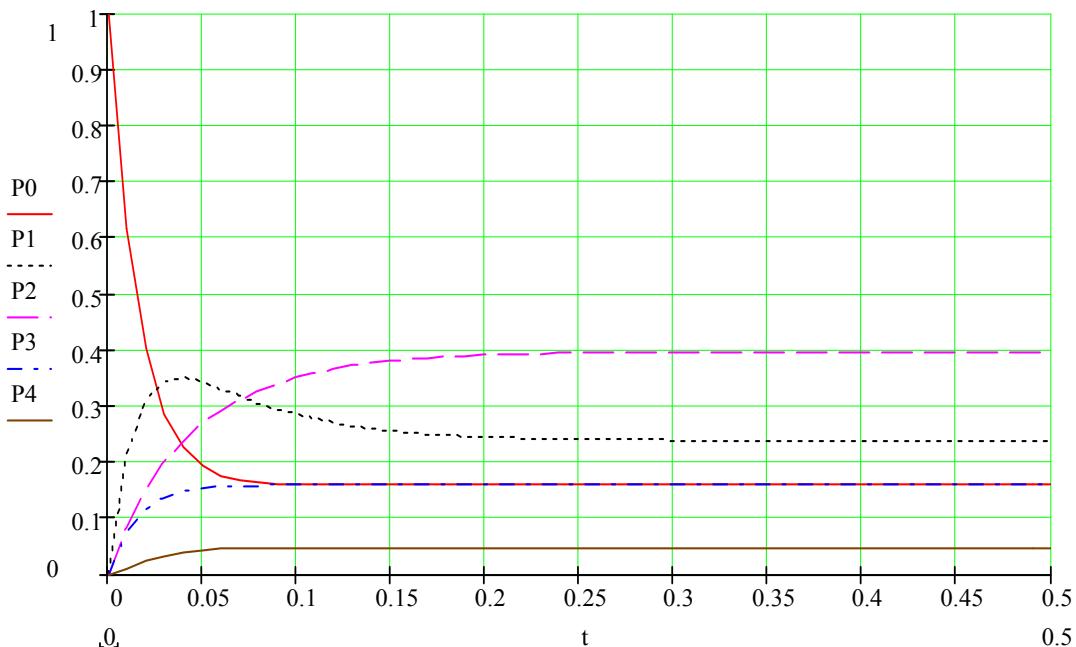


Рис. 2. Зависимости вероятностей состояний процесса радиоконтроля от времени

#### Список используемых источников

- Управление** радиочастотным спектром и электромагнитная совместимость: учебн. пособие / А. Л. Бузов, М. А. Быховский и др.; под ред. М. А. Быховского. – М. : Эко-Трендз, 2006. – 376 с.
- Теория** случайных процессов и ее инженерные приложения / Е. С. Вентцель, Л. А. Овчаров. – М. : Наука, 1991. – 384 с.
- Исследование** операций: задачи, принципы, методология / Е. С. Вентцель: 2-е изд., стер. – М. : Наука, 1988. – 208 с.
- Марковские** процессы / В. И. Тихонов, М. А. Миронов. – М. : Сов. Радио, 1977. – 488 с.

УДК 621.3.05

**О. П. Жадан (преподаватель кафедры МЭОСС ВАС)**

**М. А. Морозов (курсант группы 2941 ВАС)**

**И. Г. Стакеев (доцент УВЦ ИВО СПбГУТ)**

#### МОРФОЛОГИЧЕСКАЯ МОДЕЛЬ ПОЛЕВОЙ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В соответствии с концепцией построения и развития современных сетей связи специального назначения (СН) одним из важных составляющих является полевая транспортная сеть связи (ПТСС) СН, т. е. полевой ком-

понент, который предназначен для восстановления разрушенных элементов сети, управления подразделениями в чрезвычайных ситуациях, усиления сети и резервирования стационарной транспортной сети связи СН [1, 2].

В некотором смысле транспортные сети нового поколения могут рассматриваться как виртуальные надстройки более интеллектуальные первичные сети связи (системы переноса). ПТСС СН содержит ряд подсистем: система переноса, система управления, сигнализации, маршрутизации, восстановления, технической и эксплуатации и пр.

ПТСС СН должна создаваться как управляемая система, обладать необходимой инвариантностью к изменениям, происходящим в системах управления, а также в некоторой степени и к инфокоммуникационным технологиям сетей доступа.

Необходимостью формирования морфологической структуры ПТСС СН обусловлена: несоответствием характеристик существующих сетей связи современным требованиям, разобщенностью и несогласованностью силовых министерств и ведомств по созданию собственных систем связи, отсутствие единства систем связи, что приводит к их к нерациональному использованию канального ресурса.

На сегодняшний день задачи по формированию морфологической модели ПТСС СН проработаны не в полном объеме.

Морфологический анализ является весьма эффективным средством для решения подобных задач, поскольку он позволяет выявить, систематизировать и изучить всевозможные варианты и способы построения системы, предназначеннной для реализации заданных функций. Существенным свойством морфологического подхода является его направленность на поиск полноты и общности вариантов. Он позволяет систематически выявить всю полноту возможных вариантов построения ПТСС СН [3].

Морфологический подход состоит в реализации следующих этапов:

1. Формулировка решаемой задачи.
2. Выявление максимально полного перечня основных функций системы.

3. Определение различных альтернативных способов реализации каждой из выявленных функций и генерация всех возможных вариантов синтезируемой системы. При этом каждый вариант состоит из цепочки, содержащей ровно по одному способу реализации каждой отдельной функции.

4. Определение эффективности вариантов синтезируемой системы.
5. Выбор и реализация наиболее предпочтительного варианта.

В данном случае по построению или формированию морфологической модели можно представить из следующих составляющих структур: топологической, потоковой и физической.

Топологическая структура ПТСС СН во многом определяет ее показатели функционирования, возможности по управлению, реконфигурации, развитию, наращиванию, приведенной стоимости, использованию альтернативных путей [4].

Синтез топологической структуры представляет собой процесс конструирования некоторого множества графов с определенными топологическими параметрами и выбор из этого множества такого графа, который наилучшим образом соответствует заданным принципам построения, функциям и целям функционирования сети связи. Это соответствие определяется по совокупности топологических характеристик, среди которых выделяют следующие:

1. Количество узлов  $|A| = N$  и ребер  $|B| = n$  графа  $G_T(A, B)$ .

2. Диаметр графа  $d$  – величина, определяемая как максимальное число ребер в кратчайшем пути между любой парой вершин множества  $A$ .

3. Среднее расстояние  $p$ , рассчитываемое по формуле:

$$p = \frac{\sum_{i=1}^N \sum_{j=1}^N r_{ij}}{N(N-1)}, \quad (1)$$

где  $r_{ij} = r(\pi_{ij})$  – ранг кратчайшего пути  $\pi_{ij} = \min_{(t)} \pi_{ij}^t$  между  $i$  и  $j$ .

4. Связность графа  $h_{\text{св}}$ .

5. Число оставных деревьев графа  $N_{\text{од}}$ .

6. Ранг пути между вершинами  $r(\pi_{ij})$  – количество ребер образующих путь  $\pi_{ij}$  между вершинами  $a_i$  и  $a_j$ .

7. Ранг узла  $r(a_i), i = \overline{1, N}$  – количество ребер инцидентных узлу  $a_i$ .

8. Затраты на реализацию топологической структуры косвенно учитываются через минимальное число узлов и минимальную суммарную протяженность ребер с требуемой связностью на заданной структуре сети.

Характеристики ПТСС должны быть сформированы таким образом, чтобы имелась возможность выделения из ее состава двухполюсных сетей, предоставляющих корреспондирующие пары узлов (КПУ) требуемую пропускную способность, которая поддерживалась требуемой структурной надежностью, а характеристики цифровых каналов ПТСС обладали качеством необходимым для обеспечения услуг электросвязи, предоставляемых сетью. Кроме того, должны обеспечиваться потребности в пропускной способности и требуемой надежности обеспечивающих подсистем.

Таким образом, совокупность корреспондирующих пар узлов (КПУ) ПТСС  $Z' = \{z_{k'}\}$  представляет собой объединение перечисленных КПУ и обеспечивающих подсистем.

$$Z' = Z \bigcup Z^y \bigcup Z^c \bigcup Z^n \bigcup Z^{cc}. \quad (2)$$

Такое представление КПУ сети позволяет на ранних этапах синтеза определить особенности морфологического описания ПТСС и количественные требования к сетевым характеристикам: пропускной способности, устойчивости и приведенной стоимости.

Каналы требуемого качества, которые образуются между корреспондирующими парами  $Z'$ , определяются компонентами вектора:

$$V_{\Sigma} = [V_1, \dots, V_k, \dots, V_m : V_{\Sigma}^y, V_{\Sigma}^c, V_{\Sigma}^n]^T, \quad (3)$$

где  $V_{\Sigma}^y$ ,  $V_{\Sigma}^c$ ,  $V_{\Sigma}^n$  – суммарное количество каналов заданного качества, необходимое для обеспечения потребностей подсистем управления, сигнализации, связи с стационарными объектами, соответственно;  $V_k$  – потребность в каналах  $k$ -й КПУ. Общее количество каналов рассчитывается по формуле:

$$V_{\Sigma} = \sum_{k=1}^m V_k + V_{\Sigma}^y + V_{\Sigma}^c + V_{\Sigma}^n. \quad (4)$$

Требования к надежности задаются для каждого направления связи  $H_{z_k}^{\text{tp}}$ ,  $k = \overline{1, m}$ , а также для обеспечивающих подсистем  $H_y^{\text{tp}}$ ,  $H_c^{\text{tp}}$ ,  $H_{cc}^{\text{tp}}$  и представляются в виде вектора

$$\overrightarrow{H^{\text{tp}}} = [H_1^{\text{tp}}, \dots, H_k^{\text{tp}}, \dots, H_m^{\text{tp}} : H_y^{\text{tp}}, H_c^{\text{tp}}, H_n^{\text{tp}}, H_{cc}^{\text{tp}}]^T. \quad (5)$$

Согласно Рекомендациями МСЭ-Т серии G (G.701, G.810, G.820, G.821, G.822, G.823) требования к качеству цифровых каналов (ЦК) ПТСС задаются вектором:

$$\overrightarrow{Q^{\text{tp}}} = [K_{\text{ош}}^{\text{tp}}, J_{\text{вых}}^{\text{tp}}, t_{\text{кп}}^{\text{tp}}, P_{\lambda}^{\text{tp}}, \tau_{\pi}^{\text{tp}}, \delta_{\nu}^{\text{tp}}]^T, \quad (6)$$

где  $K_{\text{ош}}$  – коэффициент ошибки;  $J_{\text{вых}}$  – дрожание фазы цифрового сигнала на выходе ЦК;  $t_{\text{кп}}$  – относительное время действия импульсных помех и кратковременных прерываний в ЦК;  $P_{\lambda}$  – проскальзывания цифрового сигнала;  $\tau_{\pi}$  – время прохождения сигнала по ЦК;  $\delta_{\nu}$  – допустимое отклонение скорости передачи цифрового сигнала на выходе ЦК.

В задачах синтеза многопродуктовая сеть, как математический объект, представляется в виде взвешенного неориентированного связанных графа  $G(A, B, U, H)$ , где  $A$  – множество вершин графа, соответствующее сетевым узлам и сетевым станциям,  $B$  – множество ребер, представляющих собой линии связи,  $H$  – структурная надежность ПТСС. Каждому ребру  $b_{ij}$  графа сети ставится в соответствие два числа:  $u_{ij}$  – пропускная способность ребра, то есть величина максимального потока, передаваемого по ребру

$U = \{u_{ij}\}$ ,  $i, j = \overline{1, N}$ ,  $i \neq j$ ,  $b_{ij} \in B$ ;  $h_{ij}$  – надежность ребра сети (вероятность исправной работы, коэффициент готовности  $r^\mu$ -й системы передачи). Как правило, при синтезе сети узлы считают абсолютно надежными, а их ненадежности пересчитывают на ребра графа.

Основным критерием рациональности ПТСС служит расход сил и средств на ее построение, эксплуатацию и развитие. В качестве целевой функции учитывающей данные расходы используется приведенная стоимость, подлежащая минимизации:

$$W(G(A, B, U, H), R(R_x, R_y)) = W_A + W_B = W(r^\mu) + W(r^\psi) \rightarrow \min, \quad (7)$$

где  $W_A = W(r^\mu)$  и  $W_B = W(r^\psi)$  – приведенные стоимости, учитывающие расход сил и средств на развертывание и эксплуатацию узлов и линий ПТСС, соответственно.

Выделяются минимальные по пропускной способности и надежности покрытия, то есть «узкие места» сети по этим характеристикам.

В качестве целевых функций многокритериальной задачи оптимизации морфологической структуры ПТСС выбираются функции: структурной надежности сети:

$$H = f_1(\overrightarrow{\Pi}_Z^\lambda, r^\mu, r^\psi, U_{\text{ном}}, V_\Sigma, \overrightarrow{H^{\text{tp}}}, \overrightarrow{Q^{\text{tp}}}) = f_1(\alpha), \quad (8)$$

пропускной способности

$$C = f_2(\overrightarrow{\Pi}_Z^\lambda, r^\mu, r^\psi, U_{\text{ном}}, V_\Sigma, \overrightarrow{H^{\text{tp}}}, \overrightarrow{Q^{\text{tp}}}) = f_2(\alpha), \quad (9)$$

качества канального ресурса сети

$$Q = f_3(\overrightarrow{\Pi}_Z^\lambda, r^\mu, r^\psi, U_{\text{ном}}, V_\Sigma, \overrightarrow{H^{\text{tp}}}, \overrightarrow{Q^{\text{tp}}}) = f_3(\alpha), \quad (10)$$

приведенной стоимости на построение, эксплуатацию и развитие ПТСС

$$W = f_4(\overrightarrow{\Pi}_Z^\lambda, r^\mu, r^\psi, U_{\text{ном}}, V_\Sigma, \overrightarrow{H^{\text{tp}}}, \overrightarrow{Q^{\text{tp}}}) = f_4(\alpha). \quad (11)$$

Многокритериальная задача синтеза структуры ПТСС состоит в выборе морфологической структуры сети  $G^*$  – эффективной альтернативы  $\alpha \in A$ , характеризующейся такими совокупностями путей  $\overrightarrow{\Pi}_Z^\lambda = \{\overrightarrow{\Pi}_k\}$ ,  $k = \overline{1, m}$ ,  $\lambda = \overline{1, \Lambda_G}$  и покрывающих множеств  $C_{\min}(\overrightarrow{\Pi}_k)$ ,  $C(\overrightarrow{\Pi}_Z^\lambda)$ , при которых отклонения целевых функций от своих оптимальных значений минимальны.

Формально многокритериальную задачу можно представить в следующем виде:

$$\alpha \in A : \begin{cases} \overline{\Pi}_Z^\lambda = \{\overline{\Pi}_k^\rho\}; \\ C(\overline{\Pi}_Z^\lambda), C_{\min}(\overline{\Pi}_k); \end{cases} \quad (12)$$

$$\begin{cases} H = f_1(\overline{\Pi}_Z^\lambda, r^\mu, r^\psi, U_{\text{ном}}, V_\Sigma, \overrightarrow{H^{\text{tp}}}, \overrightarrow{Q^{\text{tp}}}) = f_1(\alpha); \\ C = f_2(\overline{\Pi}_Z^\lambda, r^\mu, r^\psi, U_{\text{ном}}, V_\Sigma, \overrightarrow{H^{\text{tp}}}, \overrightarrow{Q^{\text{tp}}}) = f_2(\alpha); \\ Q = f_3(\overline{\Pi}_Z^\lambda, r^\mu, r^\psi, U_{\text{ном}}, V_\Sigma, \overrightarrow{H^{\text{tp}}}, \overrightarrow{Q^{\text{tp}}}) = f_3(\alpha); \\ W = f_4(\overline{\Pi}_Z^\lambda, r^\mu, r^\psi, U_{\text{ном}}, V_\Sigma, \overrightarrow{H^{\text{tp}}}, \overrightarrow{Q^{\text{tp}}}) = f_4(\alpha); \end{cases} \quad (13)$$

$$\min_{\alpha} \Delta f_i(\alpha) = \begin{cases} f_i^0 - f_i(\alpha), \forall i \in I_1; \\ f_i(\alpha) - f_i^0, \forall i \in I_2; \end{cases}$$

$$i = \overline{1, 4}, \lambda = \overline{1, \Lambda}, \mu = \overline{1, Q_\mu}, \psi = \overline{1, Q_\psi}, r^\psi = \overline{1, Q_y}, r^\mu = \overline{1, Q_\lambda},$$

где  $f_i^0$  – оптимальное значение  $i$ -й функции цели на множестве допустимых альтернатив,  $I_1, I_2$  – множества индексов максимизируемых и минимизируемых функций цели, соответственно.

Многокритериальная задача оптимизации структуры ПТСС в общем виде (12), (13) разрешена быть не может. Это связано с взаимозависимостью целевых функций и отсутствием строгих математических методов решения таких задач. В связи с этим возникла необходимость разработки морфологической модели ПТСС СН.

#### Список используемых источников

1. От Взаимоувязанной сети связи к Единой сети электросвязи / В. Д. Москвитин // Вестник связи. – 2003. – № 9.
2. Цифровые сети связи: основы планирования и построения / А. В. Шмалько. – М. : ЭКО-ТРЕНДЗ, 2001. – 284 с.
3. Моделирование сложных систем / Н. П. Бусленко. – М. : Наука, 1978. – 156 с.
4. Теория графов. Алгоритмический подход / Н. Кристофиес: пер. с англ. – М. : Мир, 1978. – 432 с.

УДК 654.078

**С. С. Казаков (студент группы ИКТС-31 СПбГУТ)**  
**С. В. Мельников (заведующий кафедрой ССС СПбГУТ)**

## **АНАЛИЗ ПЕРСПЕКТИВ РАЗВИТИЯ СИСТЕМ ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ**

В настоящее время основные подходы к построению систем управления телекоммуникационными сетями определяются концепцией TMN (Telecommunication Management Network – сети управления телекоммуникациями). Концепция TMN базируется на протоколах SNMP (Simple Network Management Protocol), CMIP (Common Management Information Protocol) и на языке описания объектов (компонентов) ASN.1/GDMO (Abstract Syntax Notation One – язык для описания абстрактного синтаксиса данных/ Guidelines for the Definition of Managed Objects – Правила Определения Управляемых Объектов) [1].

Кроме этого, при практической реализации систем управления различные производители используют ряд технологий взаимодействия распределенных объектов, из которых наибольшее распространение получили [2, 3]:

- CORBA (Common Object Request Broker Architecture – Архитектура Общих Объектных Брокеров Запросов);
- JavaBeans, базирующаяся на языке Java, протоколе TCP (Transmission Control Protocol – протокол управления передачей) и методах RMI (Remote Method Invocation – программный интерфейс вызова удаленных методов);
- DCOM (Distributed Component Object Model – Распределенная Многокомпонентная Модель Объектов).

Для обеспечения эффективного управления сетями связи целесообразно на основе анализа достоинств и недостатков данных технологий управления выбрать ту, которая в наибольшей степени удовлетворит потребности системы управления связью с учетом особенностей функционирования и специфики требований, предъявляемых к параметрам и характеристикам сетей связи специального назначения.

Концепция TMN позиционируется как классическая концепция построения систем управления телекоммуникационными сетями. С системной точки зрения TMN представляет собой набор средств обмена информацией и взаимодействия распределенных приложений между собой в гетерогенной среде. Основная проблема состоит в унификации правил работы в этой сети, которые удовлетворяли бы требованиям управления. Для этого определяются правила по следующим четырем направлениям:

- структура и принципы взаимодействия распределенных объектов;
- средства взаимодействия между объектами управления (протоколы);
- средства структурного описания наборов данных и операций (объектно-ориентированный, структурный язык описания данных);
- система поддержки работы распределенных объектов (информационная база данных и средства работы с ней).

Каждый элемент в сети, с точки зрения управления, заменяется некоторой абстрактной информационной моделью, которая рассматривает объект как сетевой ресурс.

Информационная модель определяет основные параметры объекта:

- ATTRIBUTES – наборы и структуры данных;
- NOTIFICATIONS – уведомления. Модель предусматривает автономную генерацию объектом набора уведомлений, как реакции на события внутри него;
- ACTIONS – действия, фактически, удаленный вызов операции.

Для создания информационной модели объекта, который описывается как некоторый класс в терминах объектно-ориентированного подхода, необходимы специальные структуры и язык описания данных. В TMN для этих целей используются два инструментальных средства:

- структуры-шаблоны GDMO. Они строго определяют обязательные и дополнительные поля класса объекта управления (упомянутые выше параметры ATTRIBUTES, NOTIFICATIONS, ACTIONS и ряд других). Конкретное наполнение и количество стандартизованных полей определяется конкретным объектом;
- язык описания структур данных ASN.1. Его основная задача состоит в предоставлении возможности описания сложных структур данных, определения новых типов данных, определения начальных значений и диапазонов для типов данных.

Эти два средства настолько тесно взаимосвязаны, что на них часто ссылаются как на единый язык описания объектов управления ASN.1/GDMO. Они являются универсальным средством описания информационных объектов любой сложности.

Одним из важнейших компонентов системы сетевого управления является информационная база данных MIB (Management Information Base). Этот объект является ресурсом, разделяемым всеми объектами сети. База MIB является связующим звеном между Менеджером и Агентом, Информационная база данных является непременным атрибутом любой распределенной системы управления объектами.

### *Технология CORBA*

CORBA представляет собой общедоступную архитектуру с посредником для запросов к объекту, разработанную группой OMG. Центральным

компонентом CORBA является посредник для запросов к объекту ORB, который отвечает главным образом за реализацию связи между клиентами и серверами (объектами). ORB служит программной шиной, обеспечивающей взаимодействие между удаленными объектами, причем детали этого взаимодействия (поиск объекта в сети, его инициализация, транспортировка сообщений и данных) скрыты от пользователя и существуют как уже реализованная часть шины ORB.

Спецификация CORBA определяет принципы создания объектно-ориентированных распределенных приложений в архитектуре клиент/сервер. При использовании технологии CORBA в системе управления взаимодействие между элементами осуществляется по схемам, аналогичным классическим подходам концепции TMN. Роль менеджера в системе выполняет приложение клиента, а агента – приложение сервера.

Технология CORBA появилась позднее протоколов CMIP и SNMP, однако, за счет лучшей безопасности и простоты реализации она получила широкое распространение.

Взаимодействие приложений клиента и сервера осуществляется через ORB-интерфейс, который предоставляет набор функций, вызываемых непосредственно у брокера объектных запросов. Состав функций идентичен для всех объектов и не зависит от конкретной реализации объекта либо объектного адаптера. Далее, по программнойшине ORB осуществляется передача команды управления через объектный адаптер целевому объекту. Функции объектного адаптера заключаются в доведении управляющей информации до целевого объекта.

Для формирования запросов к объекту клиент должен знать типы операций, поддерживаемых объектом. Операции и типы данных, которые поддерживаются объектом, определяются с помощью интерфейсов объекта. Интерфейс определяет запросы, которые могут быть посланы объекту и обслужены им. Интерфейсы для объекта определяются на языке описания интерфейсов (Interface Definition Language – IDL).

Язык IDL, также как и ASN.1, является декларативным. Он не предназначен для непосредственной реализации распределенных приложений.

Для взаимодействия с распределенными объектами приложение должно знать типы интерфейсов, поддерживаемых конкретными объектами. Для этого предназначено хранилище интерфейсов (Interface Repository – IR) системы CORBA, через которое происходит программно-управляемый доступ к системе типов IDL во время выполнения задачи. Хранилище является аналогом базы MIB в TMN.

### *Технология JavaBeans*

Технология JavaBeans предоставляет открытую, стандартную, универсальную платформу для сетевых вычислений.

При разработке данной технологии особое внимание было уделено независимости приложений Java от конкретной аппаратно-программной платформы, что позволяет осуществлять обмен между приложениями и их фрагментами в гетерогенной вычислительной среде. К основным средствам создания кроссплатформенных приложений относятся новый язык программирования Java и виртуальная Java-машина, в коды которой (так называемые, байт-коды) транслируются Java-приложения, то есть, программы на языке Java.

Одним из узловых понятий в Java является способ доступа к удаленным объектам – RMI (вызов удаленных методов), – через предоставляемый объектом Java интерфейс (множество методов доступа).

В основе удаленного взаимодействия так же, как и в CORBA, лежит модель клиент-сервер.

В отличие от технологии CORBA, которая просто предоставляет метод взаимодействия и непроцедурный язык для работы с объектами и не ориентируется на конкретный стек протоколов, Java вместе с RMI использует стек протоколов Интернет (TCP/IP).

Для описания информационной модели объекта управления, также как и в технологии CORBA, используется язык IDL.

Роль информационной базы данных, в которой хранится информация об объектах управления, выполняет каталог зарегистрированных имен.

### *Технология DCOM*

Технология DCOM — это технологический стандарт от компании Microsoft, предназначенный для создания программного обеспечения на основе взаимодействующих распределенных компонентов, каждый из которых может использоваться во многих программах одновременно. Особенностью DCOM является жесткая привязка технологии к продукции Microsoft, а, следовательно, и к операционным системам серии Windows. В отличие от CORBA и Java, DCOM является, фактически, закрытой технологией.

Взаимодействие управляющего объекта и объекта управления, так же, как в CORBA и JAVA, осуществляется по схеме клиент-сервер.

Технология DCOM, также как и CORBA, представляет собой реализацию прикладного уровня эталонной модели взаимодействия открытых систем и не ориентирована на конкретный стек протоколов.

Для описания объектов здесь, также как и в CORBA, используется язык IDL.

Информация об объекте, включающая сведения о типе объекта, интерфейсах, свойствах, методах и параметрах методов, содержится в библиотеке типов.

Проведенный анализ показал, что во всех рассматриваемых технологиях взаимодействие между удаленными элементами осуществляется в со-

ответствии с принципами ЭМВОС. Основные различия заключаются в программной реализации на прикладном уровне ЭМВОС механизма обмена между распределенными объектами по схеме агент-менеджер, регламентированной стандартами концепции TMN.

Таким образом, рассмотренные технологии CORBA, JAVA и DCOM являются альтернативным вариантом решения прикладного уровня ЭМВОС системы управления телекоммуникационной сетью, отличающимся от классического TMN, использующего протоколы SNMP и CMIP.

### **Список используемых источников**

1. Управление сетями электросвязи по стандарту TMN : учеб. пособие / А. Ю. Гребешков. – М. : Радио и связь, 2004.
2. Сравнительный анализ технологий CORBA и COM [Электронный ресурс] / А. Цимбал. – Режим доступа: <http://www.interface.ru/fset.asp?Url=/borland/corbacom.htm> (Дата обращения 16.05.2014).
3. Компонентная модель JavaBeans [Электронный ресурс]. – Режим доступа: <http://www.osp.ru/jw/13032080/> (Дата обращения 16.05.2014).

**УДК 35:574**

**Д. А. Касперович (студент группы ИКТС-21 СПбГУТ)**  
**Н. Е. Манвелова (доцент кафедры Экологии и БЖД СПбГУТ)**

## **АКТУАЛЬНЫЕ ЭКОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ВОЕННО-ВОЗДУШНЫХ СИЛ**

Особенности современных экологических проблем Военно-воздушных сил обусловлены спецификой современной авиации и ее наземной инфраструктуры. Боевые и транспортные самолеты и вертолеты, аэродромное хозяйство, склады авиационного горючего с заправочными средствами, радиолокационные системы и, в целом, военные городки авиационных гарнизонов являются источниками загрязнения окружающей среды различными загрязнителями: авиационным топливом и продуктами его сгорания, акустическими и радиолокационным излучением, горюче смазочными материалами, твердыми отходами и т. д.

При этом, наиболее значимым видом загрязнения для данного рода войск является загрязнение окружающей среды авиационными топливами и продуктами их сгорания, которое имеет некоторые специфические особенности. В рамках изучения дисциплины «Военная экология» сформулирована задача исследования основных загрязнителей ВВС, источников их возникновения и попадания в окружающую среду, оценка

степени и характера влияния военной техники и технологий на качество окружающей среды.

Авиационное топливо керосин содержит повышенное количество циклических соединений, в том числе ароматических, вследствие чего он обладает повышенной токсичностью. Авиационный керосин имеет следующие характеристики: плотность 0,78–0,85 г/см<sup>3</sup> (при 20 °C), вязкость 1,2–4,5 мм<sup>2</sup>/с (при 20 °C), температура вспышки 28–72 °C, теплота сгорания около 43 МДж/кг [1].

В зависимости от химического состава и способа переработки нефти, из которой получен керосин, в его состав входят:

- предельные алифатические углеводороды – 20–60 %;
- нафтеновые углеводороды 20–50 %;
- бициклические ароматические 5–25 %;
- непредельные углеводороды – до 2 %;
- примеси сернистых, азотистых или кислородных соединений.

Основными источниками загрязнения окружающей среды авиационным керосином являются проливы при заправке и обслуживании топливных систем летательных аппаратов, потери его при транспортировании и хранении, а также при сливе невыработанного топлива из самолетов в воздухе в аварийных ситуациях (см. рис. 1). Кроме того, определенная часть авиационного керосина попадает в атмосферу при дозаправке в воздухе, которая может производиться с помощью самолета-заправщика ИЛ-78. Самолёт-заправщик Ил-78, созданный в 1987 г. на базе военно-транспортного самолёта Ил-76, имеет взлётную массу 190 т, массу передаваемого топлива 65 т (на рубеже 1000 км) или 36 т (на рубеже 2 500 км), дальность полёта 10 000 км, скорость до 830 км/ч, высоту полёта до 11 км, экипаж 6 человек. Самолёт-заправщик Ил-78 может производить заправку в воздухе одновременно трёх самолётов [2].

Процесс сжигания авиационного топлива сопровождается выбросом в атмосферу различного количества оксидов углерода, азота, серы и др. веществ. При этом, авиационные газотурбинные двигатели характеризуются повышенным дымлением только на режимах взлета и посадки, когда практически невозможно обеспечить благоприятные условия сгорания, вследствие чего, продукты сгорания авиатоплив наиболее неблагоприятное воздействие на окружающую среду оказывают именно в районе аэродромов.

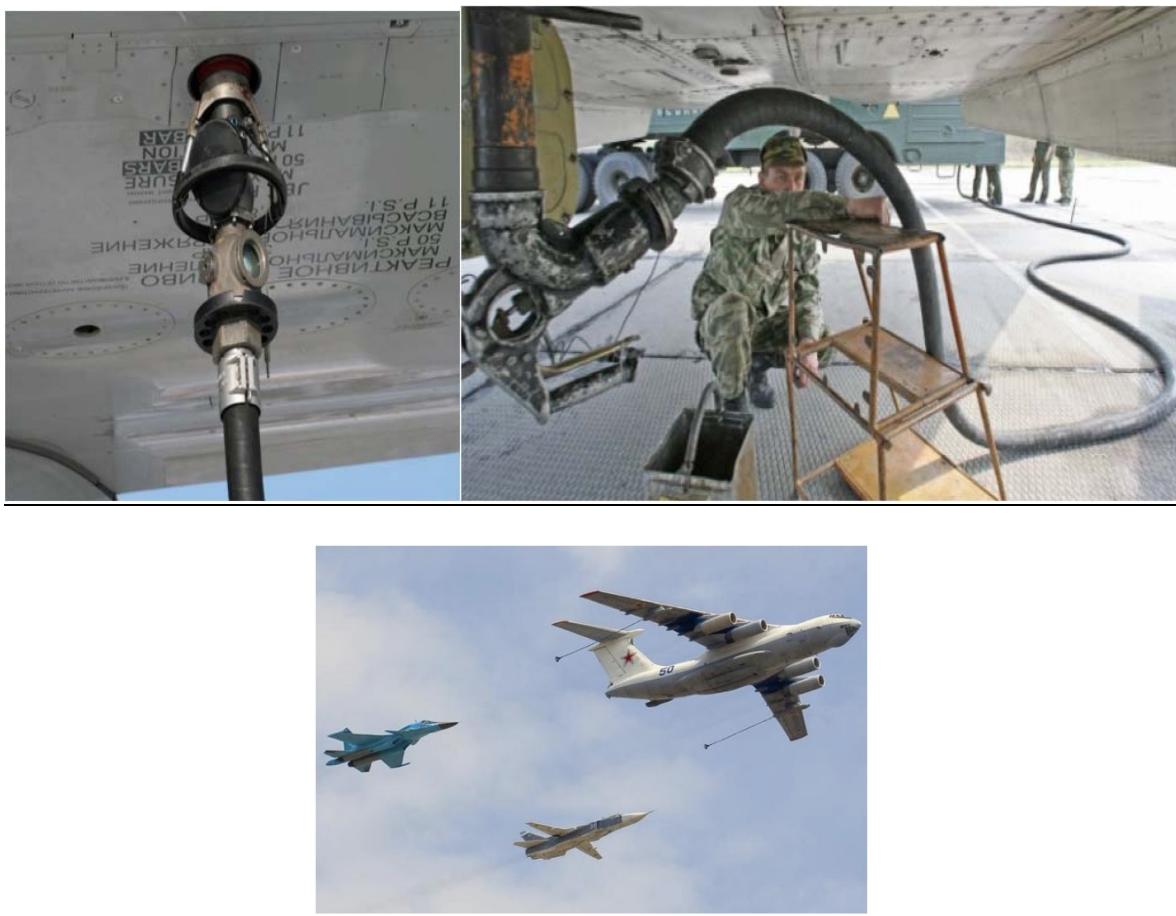


Рис. 1. Наземная и воздушная заправка самолетов

Масштабы применения авиационных топлив и вероятность попадания их в окружающую среду очень велики. Масса топлива, необходимого для обеспечения полета, оставляет от 30 до 60 % взлетной массы самолета. Общий запас топлива на борту самолета должен обеспечить выполнение программ полета по заданному маршруту, запуск и опробование двигателей, выруливание на земле и маневрирование в воздухе в зоне аэродрома, а также необходимый резерв посадки. Для современных самолетов невырабатываемый и несливаемый остаток топлива на борту достигает 3–4 % от полной заправки. С еще большим экологическим риском связаны режимы боевого маневрирования, взлет и посадка на авианесущие корабли, дозаправка топливом в воздухе, воздушно-десантные операции и др. Экологическая безопасность авиационной техники в целом во многом зависит от исправности и надежности топливной системы. Важнейшим элементом топливных систем самолетов являются баки. В боевых самолетах применяются мягкие топливные баки, изготовленные из многослойных резиноподобных композиционных материалов, между слоями оболочки бака размещается протектор из натурального каучука или сырой губчатой резины. В случае небольшого повреждения бака, например, пулей, протектор под действием топлива набухает, и пробоина затягивается. Основными недостатками мягких

топливных баков с экологической точки зрения являются их повышенная пожароопасность. Таким образом, специфика экологических последствий, обусловленных деятельностью Военно-воздушных сил, определяется с её негативным воздействием на атмосферу.



Рис. 2. Студент группы ИКТС-21 СПбГУТ Каспирович Д. А. во время доклада на ежегодной 68 региональной научно-технической конференции, апрель, 2014 г.

Следующим не менее, а в отдельных случаях, и более значимым источником негативного воздействия на окружающую среду являются склады хранения авиационного топлива. Современная летательная техника расходует много топлива, поэтому на аэродромах создаются склады авиационного топлива. Негативные экологические проблемы складов авиационного топлива возникли в связи с потерей надежности складского оборудования. В годы «холодной войны» с целью повышения устойчивости складов авиационного топлива к воздействию ядерных ударов противника, часть емкостей для хранения топлива, а также система трубопроводов размещалась под землей. В период разпада СССР и передела собственности сократилось финансирование, необходимое для поддержания в исправном состоянии авиационной техники, в том числе и складов авиационного топлива. Поэтому со временем надежность оборудования складов снизилась, появились утечки авиационного керосина в грунт. В результате в ряде военных аэродромов, например, в Моздоке, в Энгельсе, в Чкаловском и других образовались так называемые «керосиновые линзы», которые частично проникали в подземный водоносный слой, тем самым загрязняя питьевую воду

в военных городках и близлежащих населенных пунктах. Кроме того, образование «керосиновых линз» наносит непоправимый ущерб биоценозам прилежащих областей, практически полностью погибают геобионты и гидробионты, обитающие на этих территориях, безвозвратно теряется плодородие почвенного покрова. Мероприятия, направленные на устранение этих негативных последствия, требуют значительных финансовых средств и должны реализоваться на протяжении многих лет.

Помимо вышеуказанных видов химического загрязнения окружающей среды, деятельность ВВС связана с негативным физическим воздействием на окружающую среду в виде значительного акустического и радиолокационного излучения высокой интенсивности.

Известно, что длительное (более суток) воздействие на организм человека акустических колебаний с интенсивностью от 80 до 135 дБ, возникающие при посадках и взлетах самолетов и вертолетов, вызывает резкое понижение слуха, а также уменьшает производительность труда на 10–30 %. Шум интенсивностью 135 дБ относится к 3-й группе и является наиболее опасным. Такой шум создают самолеты всех родов авиации при полетах на предельно малых высотах, а также при запуске двигателей. Систематическое воздействие этого шума (в течение 8–12 ч) приводит к ухудшению состояния здоровья и резкому снижению производительности труда.

В связи с этим предъявляются следующие экологические требования к авиационной технике и аэродромам:

- трассы полета на малой высоте, взлета и посадки самолетов (вертолетов) не должны проходить над населенными пунктами;
- площадки опробования двигателей должны располагаться таким образом, чтобы во время пробы двигателей самолет был ориентирован носовой частью в сторону жилой застройки;
- должны применяться стационарные или передвижные средства шумопоглощения;
- создание на пути движения звуковых волн перед городками шумозащитных полос из двух–трех рядов деревьев в сочетании с кустарниками;
- применение звукоизоляционных материалов в медицинских учреждениях, школах, детских садах и других общественных зданиях и т. д.

Таким образом, деятельность Военно-воздушных сил РФ, как и многие другие виды техногенной деятельности, сопровождается негативным воздействием на окружающую среду в виде химического и физического загрязнения авиационным топливом и продуктами его сгорания, горюче смазочными материалами, твердыми отходами, акустическими и радиолокационным излучением. Для преодаления негативных последствий деятельности ВВС в 1997 г. была создана Экологическая служба Вооруженных Сил РФ, которая включает деятель-

ность штатных экологов практически во всех подразделениях – до дивизий и бригад. По данным на 2007 г. руководитель экологической службы округа имеет звание полковника. В ракетных войсках стратегического назначения, Военно-воздушных силах, Военно-морском флоте в штате экологической службы состоят семь экологов: шесть военных и один гражданский [4].

#### Список использованной литературы

1. **Большая советская энциклопедия.** Т. 1. – М. : «Советская энциклопедия», 1969. – С. 168–180.
2. <http://eko-monitor.ru/?p=339>
3. <http://www.airwar.ru/enc/craft/il78.html>
4. **Общая экология с основами экологической безопасности военной деятельности** : учебное пособие / В. В. Дроздов, С. А. Панихицников, – СПб. : Изд-во СПбГУТ, 2013. – 513 с.

**УДК 621.395.52, 621.315.28**

**Е. М. Колесова, М. А. Суранова (студентки группы ИКТВ-32 СПбГУТ)**

### **СИСТЕМА ДИСТАНЦИОННОГО ПИТАНИЯ ПОДВОДНЫХ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ**

Дистанционным питанием (ДП) – называется передача электрической энергии для питания аппаратуры связи, установленной на необслуживаемых усилительных пунктах (НУП), с использованием тех же цепей, по которым организуется связь (рис. 1) [1–2].

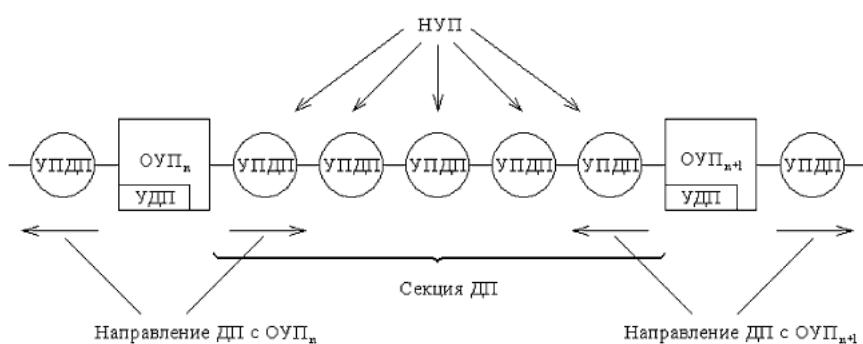


Рис. 1. Структурная схема организации ДП на магистрали связи

Участок магистрали связи между двумя смежными ОУП называется секцией ДП. Передача электроэнергии с ОУП, как правило, осуществляется

ся на длину полусекции. НУП другой полусекции получают питание со следующего ОУП.

Основные требования, предъявляемые к цепи ДП:

1. Наибольшая дальность ДП.
2. Бесперебойная подача энергии.
3. Хорошие массогабаритные показатели.
4. Минимальное влияние токов ДП на каналы связи.
5. Минимальное влияние посторонних помех на цепи ДП и каналы связи.

В современных системах передачи информации ДП позволяет автоматизировать (сделать необслуживаемым) до 98 % всех УП магистрали.

### *Анализ существующих схем ДП*

Классификация систем ДП

1. По типу применяемого кабеля.

Существуют три типа линий связи: на симметричном, коаксиальном и оптоволоконном кабелях. Их цепи ДП строятся по разному.

Кроме того, системы ДП делятся по следующим признакам:

2. По роду тока ДП (переменный или постоянный).

ДП постоянным током обеспечивает практически полное отсутствие влияния токов ДП на каналы связи и устройства ДП (УДП) проще. В связи с этим ДП постоянным током получило наибольшее применение.

ДП переменным током (промышленной частоты) применяется только на магистралях коаксиального кабеля в АСП (аналоговых СП) К-1920 и К-1920У, выполненных на электронных лампах.

3. По схемам передачи электроэнергии.

При ДП постоянным током используются две схемы: «провод-провод» и «провод-земля».

Схема «провод-провод» образуется из проводов линий связи. Она хорошо защищена от ближайших токов линий электропередач, электрифицированных железных дорог. Недостаток – малая дальность действия.

В схеме «провод-земля» обратным проводом служит земля, поэтому схема более подвержена влиянию различных посторонних ЭДС и токов.

4. По схемам включения нагрузок.

Нагрузки (НУП) могут включаться в линию последовательно, параллельно и раздельно (рис. 2, 3).

Последовательное включение нагрузок используется при ДП постоянным током. Ток в линии стабилизируется одним общим стабилизатором тока.

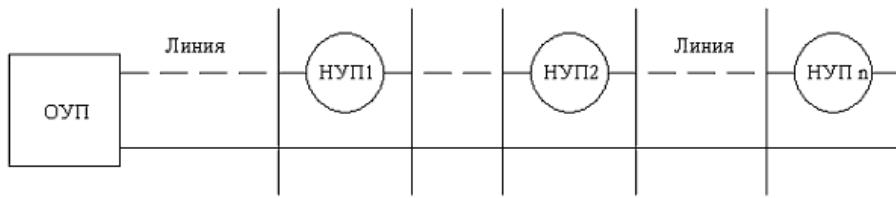


Рис. 2. Схема последовательного включения нагрузок НУП

Напряжение УДП:

$$U_{\text{ДП}} = \sum_{i=1}^n (U_{\text{НУП}_i} + I_{\text{ДП}} R_y), \quad (1)$$

где  $R_y$  – суммарное сопротивление прямого и обратного проводов усиливательного участка.

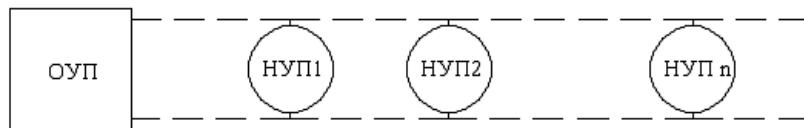


Рис. 3. Параллельная схема включения нагрузок НУП

Применяется для включения НУП ламповой аппаратуры при питании переменным током. Для уменьшения потерь в линии проще применить трансформаторы и увеличить дальность системы.

$$I_{\text{ДП}} = \sum_{i=1}^n (I_{\text{НУП}_i} + I_{\text{СДП}}). \quad (2)$$

Раздельное включение нагрузок НУП, когда в каждую цепь включается только один НУП, не позволяет получить большую дальность ДП. Она применяется при питании постоянным током вынесенных подстанций (ВПС) или концентраторов ВПК. Это характерно для современных цифровых сетей связи, которые строятся по радиально-узловому принципу.

##### 5. По принципам резервирования.

Резервирование ДП предусматривается на случай проведения профилактических или ремонтных работ на участках линии связи. Чтобы не нарушить действие связи в эти периоды, резервирование может осуществляться путем:

- подачи питания по второму кабелю с того же ОУП;
- с противоположного ОУП (сквозное резервирование);
- от стационарных резервных питающих пунктов, размещенных посередине между двумя ОУП;
- от передвижных питающих или усиливательных станций.

### Принципы организации цепей ДП

Цепи ДП образуются из тех же проводов, по которым передаются сигналы связи. В зависимости от типа линии связи используется тот или иной способ защиты линии связи от токов ДП.

1. На линиях с симметричным кабелем ток ДП поступает через среднюю точку трансформатора и делится пополам между проводами линии связи (рис. 4).

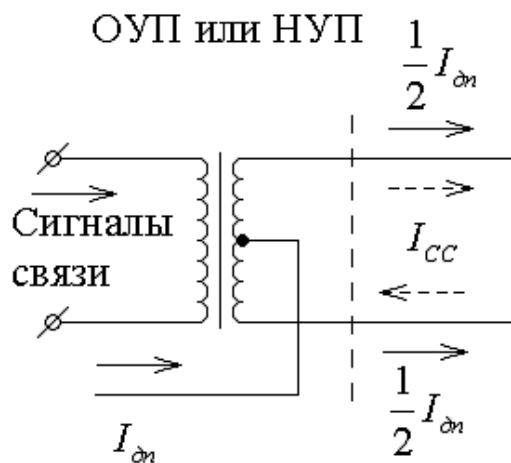


Рис. 4. Дифференциальная схема передачи токов ДП

2. Применение разделительных фильтров характерно для кабельных линий с коаксиальным кабелем (рис. 5).

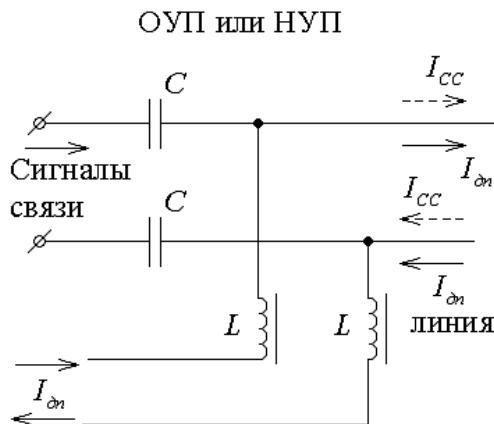


Рис. 5. Кабельная линия с коаксиальным кабелем

Цепи дистанционного питания могут состоять из одного, двух и четырех проводов. Выбор схемы зависит от числа жил, числа каналов связи и величины сопротивления проводов. Всегда лучше использовать максимально большее число пар жил для ДП. При этом потери в линии будут меньше. На рисунках 6–8 приведены схемы цепей ДП для симметричного кабеля.

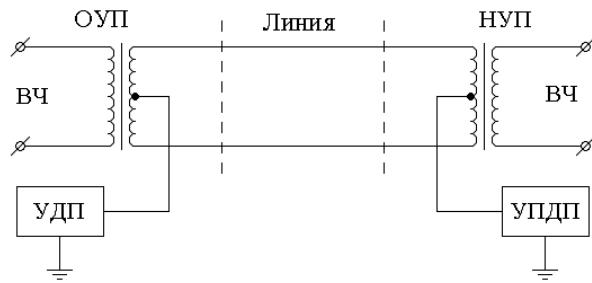


Рис. 6. Однопроводная «пара-земля»

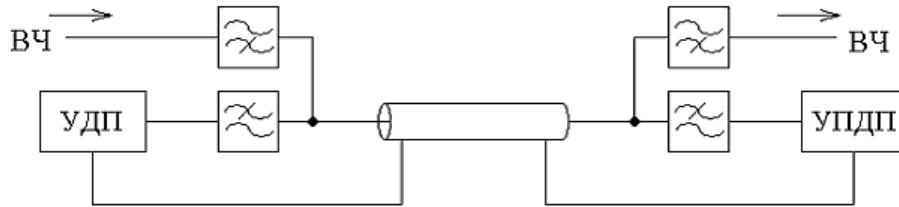


Рис. 7. Схема ДП коаксиального кабеля по типу двухпроводная «центральная жила – трубка»

Достоинство: рациональная организация питания усилителей.

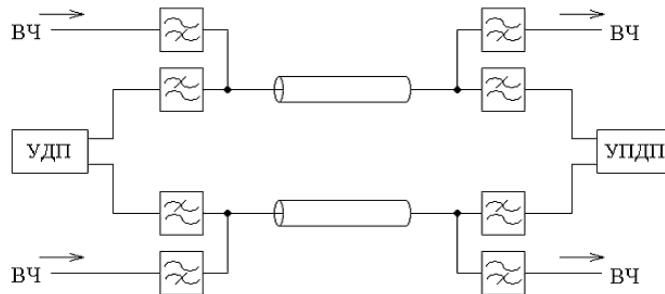


Рис. 8. Двухпроводная схема ДП «центральная жила - центральная жила»

Достоинство: меньшие потери, так как сопротивление трубы больше, чем сопротивление центральной жилы.

Анализ существующих технических решений по организации систем дистанционного питания позволяет сформулировать основные признаки систем питания подводных волоконно-оптических линий связи в районах Северного ледовитого океана:

- по роду тока – постоянный;
- по схеме передачи электроэнергии – провод-земля;
- по схеме включения нагрузок – последовательное;
- по схеме резервирования - с противоположного ОП (сквозное резервирование).

Достоинства представленных решений:

- реализация выбранной схемы организации дистанционного питания будет значительно дешевле аналогичной линии на переменном токе;

– старение изоляции кабеля на постоянном токе происходит медленнее из-за отсутствия частичных разрядов в изоляции.

Недостатки представленных решений:

– в схеме «провод-земля» обратным проводом служит земля, поэтому схема более подвержена влиянию различных посторонних ЭДС и токов.

– схема последовательного включения нагрузок НУП (НОУ), используется при ДП постоянным током. Ток в линии стабилизируется одним общим стабилизатором тока.

– увеличение параметра ток дистанционного питания ( $I_{dp}$ ) приводит к увеличению нагрева токоведущего проводника оптического кабеля и снижению КПД источника ДП.

– замыкание на землю в любой точке приводит к режиму КЗ и сопровождается значительными токами как в месте КЗ, так и в элементах оборудования.

#### **Список используемых источников**

1. **Подводные** кабельные магистрали связи / И. С. Равич, Д. Л. Шарле. – М. : Связь, 1971.

2. **Источники** вторичного электропитания / С. С. Букреев и др.; под ред. Ю. И. Конева. – М. : Радио и связь, 1983. – 280 с., ил.

*Статья представлена научным руководителем В. А. Александровым.*

**УДК 355.58**

**В. В. Коптяков (студент группы МС-22 СПбГУТ)**

**В. А. Феоктистов (старший преподаватель кафедры ЭБЖД)**

## **ВУЛКАНЫ. ИЗВЕРЖЕНИЯ ВУЛКАНОВ И ИХ ПОСЛЕДСТВИЯ, СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ОПОВЕЩЕНИЯ ВО ВРЕМЯ ИЗВЕРЖЕНИЯ**

Извержение вулкана – процесс выброса вулканом на земную поверхность раскаленных обломков горных пород, газообразных продуктов, пепла, излияние лавы (магмы).

Извержение вулканов происходит в результате процесса движения магмы из недр Земли к поверхности [1].

На глубине от 50 до 350 км образуются очаги расплавленного вещества – магмы. По участкам дробления и разломов земной коры магма поднимается и изливается на поверхность в виде лавы. Лава отличается от

магмы тем, что лава не содержит летучих компонентов, которые при падении давления отделяются от магмы и уходят в атмосферу.

Вулканом называется конусообразное или куполовидное возвышение в земной коре. Конус вулкана состоит из продуктов извержения. На вершине расположен кратер. Диаметры кратера различны и в среднем около 500–700 метров.

В настоящее время на Земле выявлено свыше 4 тысяч вулканов, из них более 600 действующих.

Действующие вулканы – необычайно интересное и грозное явление природы. В древние времена стихийная сила их извержений приводила человека, не знавшего их истинную природу, в суеверный ужас. Источниками наиболее крупных вулканических катастроф становились потухшие, давно покоящиеся вулканы. Погибали целые города и селения. Под десятками метров пеплов и шлаков погребалось всё живое, в этих местах на долгие годы замирала жизнь. Разлившиеся, раскалённые лавовые потоки не остывали в течение многих лет, и залитые лавой окрестности вулканов после извержения напоминали инопланетные ландшафты. Но проходили годы, вулканы замирали, и начинала торжествовать жизнь. Сначала появлялась редкая растительность. Потом всё больше и больше растений завоевывали свободные территории. Сформировавшиеся растительные ассоциации заселялись животными, рождались новые экологические сообщества.

Вулканические извержения угрожают приблизительно 1/10 части жителей Земли. Около 200 млн человек проживают в опасной близости к действующим вулканам. Они подвергаются определённой опасности, поскольку селиться на склонах вулканов рискованно. По статистике ЮНЕСКО, за последние 500 лет 200 тыс. человек погибли от вулканических извержений или от их последствий. Извержение вулкана всегда красивое и величественное зрелище. Но только если смотреть со стороны наблюдателя. И горе тому, кто окажется на пути сбегающей вниз клокочущей лавы или попадет под град раскаленных добела камней. Много неприятностей может принести извержение – тучи раскаленного пепла, заслоняющие пеленою мрака небо, покрывающие землю на долгие годы мёртвой коркой словно саваном, ядовитые газы, ужас и разрушения.

Различают действующие, уснувшие и потухшие вулканы. К действующим вулканам относятся: извергающиеся в настоящее время постоянно или периодически. К уснувшим относят вулканы, об извержениях которых нет сведений, но они сохранили свою форму и под ними происходят локальные землетрясения. Потухшими называются сильно разрушенные и размытые вулканы без каких-либо проявлений вулканической активности. Внешне каждый вулкан – это возвышение, необязательно высокое. Возвышение связано каналом с магматическим очагом на глубине. Мagma – это расправлена massa, состоящая в основном из силикатов. Мagma, подчиняясь определенным физическим законам, может подниматься вместе с

парами воды и газами из глубины наверх. Преодолевая на своем пути преграды, магма изливается на поверхность. Выброс из жерла вулкана паров, газов, магмы, горных пород и есть извержение вулкана.

Основные части вулканического аппарата: магматический очаг (в земной коре или верхней мантии); жерло – выводной канал, по которому магма поднимается к поверхности; конус – возвышенность на поверхности Земли из продуктов выброса вулкана; кратер – углубление на поверхности конуса вулкана.

Самые высокие из вулканов находятся в Эквадоре (Котопахи – 5 896 м и Сангай – 5410 м) и в Мексике (Попокатепетль – 5 452 м). В России находится четвертый в мире по высоте вулкан – это Ключевская Сопка, высотой 4 750 м.

Самым катастрофическим можно считать, в общем-то, невысокий – 800 м индонезийский вулкан Krakatau. Ночью с 26 на 27 августа 1883 года после трех страшных взрывов на небольшом безлюдном островке небо закрыл пепел, и вылилось 18 куб. километров лавы. Огромная волна (около 35 м) буквально смыла сотни прибрежных поселков и городов Явы и Суматры. В этой трагедии погибли 36 тыс. человек.

Вулканы бывают трех типов. Площадные вулканы. В настоящее время такие вулканы не встречаются, или можно сказать не существуют. Так как эти вулканы приурочены к выходу большого количества лавы на поверхность большой площади [2].

Трещинные вулканы. Они проявляются в излиянии лавы на земную поверхность по крупным трещинам или расколам. В отдельные отрезки времени, в основном на доисторическом этапе, этот тип вулканизма достигал довольно широких масштабов, в результате чего на поверхность Земли выносились огромное количество вулканического материала – лавы. В настоящее время трещинный вулканизм распространен в Исландии (вулкан Лаки), на Камчатке (вулкан Толбачинский), и на одном из островов Новой Зеландии.

Центральный тип. Он сопровождается образованием конусообразных вулканических гор, высота их контролируется гидростатическими силами.

При извержении вулкана выделяются продукты вулканической деятельности, которые могут быть жидкими, газообразными и твердыми.

Газообразные – фумаролы и софиони, играют важную роль в вулканической деятельности.

Состав газовых выделений во многом зависит от температуры. Различают следующие типы фумарол: сухие – температура около 5 000 °C, почти не содержит водяных паров; насыщен хлористыми соединениями; кислые, или хлористоводородно-сернистые – температура приблизительно равна 300–4 000 °C; щелочные, или аммиачные – температура не больше 1 800 °C; сернистые, или сольфатары – температура около 1 000 °C, глав-

ным образом состоит из водяных паров и сероводорода; углекислые – температура меньше 1000 °С, преимущественно углекислый газ.

Жидкие – характеризуются температурами в пределах 600–12 000 °С. Представлена именно лавой. Вязкость лавы обусловлена ее составом и зависит главным образом от содержания кремнезема или диоксида кремния.

Твердые продукты включают в себя вулканические бомбы, лапиллы, вулканический песок и пепел. В момент извержения они вылетают из кратера со скоростью 500–600 м/сек. Вулканические бомбы – крупные куски затвердевшей лавы размером в поперечнике от нескольких сантиметров до 1 м и более, а в массе достигают нескольких тонн. Они образуются при взрывном извержении, которое происходит при быстром выделении из магмы содержащихся в ней газов. Лапиллы – сравнительно мелкие обломки шлака величиной 1,5–3 см, имеющие разнообразные формы. Вулканический песок – состоит из сравнительно мелких частиц лавы (0,5 см). Еще более мелкие обломки, размером от 1 мм и менее образуют вулканический пепел, который превращается в вулканический туф.

В зависимости от количества, соотношения извергаемых вулканических продуктов (газовые, жидкие или твердые) и вязкости лав выделены четыре главных типа извержений: гавайский (эффузивный), стромболианский (смешанный), купольный (экструзивный) и вулканский.

Гавайский – вулканические горы имеют пологие склоны, их конуса сложены слоями остывшей лавы. В кратере действующих гавайских вулканов находится жидккая лава основного состава с очень небольшим содержанием газов. Она бурно кипит в кратере – небольшом озере на вершине вулкана, представляя собой великолепное зрелище, особенно ночью. При извержении уровень лавового озера начинает спокойно, почти без толчков и взрывов, подниматься и доходит до краев кратера, затем лава переливается через край и, имея весьма жидкую консистенцию, растекается на обширной территории, со скоростью около 30 км/ч, на десятки километров. Этапоном стромболианского типа является извержение вулкана Стромболи (Липарские острова) в Средиземном море. Обычно вулканы этого типа – стратовулканы и извержения, происходящие в них, сопровождаются сильными взрывами и подземными толчками, выбросами паров и газов, вулканического пепла, лапиллей. Иногда отмечается излияние лавы на поверхность, но вследствие значительной вязкости протяженность потоков бывает небольшой. Для купольного типа характерно выжимание и выталкивание вязкой лавы сильным напором из канала вулкана и образование куполов, криптокуполов и обелисков. В вулканском типе большую роль играют газы, производящие взрывы и выбросы огромных туч, переполненных большим количеством обломков горных пород, лав и пепла. Вязкие лавы образуют небольшие потоки.

Основными поражающими факторами при извержении вулканов являются: ударная волна, летящие вторичные снаряды (камни, деревья и др.),

вулканический пепел, вулканические газы, тепловое излучение, пирокластические потоки. Часто извержение сопровождается образованием цунами, оползней и возникновением пожаров. Мелкий пепел, рассеянный в воздухе, может вызывать затруднение дыхания, обструкцию дыхательных путей, асфиксию и смерть. В нем подчас содержатся токсические начала (например, фтор), отравляющие источники воды. Пыль и пепел затрудняют видимость, выводят из строя моторы автомобилей, радиосвязь, электротехнические системы.

Имеются и другие угрозы, связанные с выпадением вулканогенных осадков, такие, как пеплопады и респираторные угрозы.

При выпадении тонкозернистых пепловых осадков для защиты здоровья лучше всего пользоваться респиратором. Если толщина пеплового слоя превышает несколько сантиметров, крышу любого здания, в котором вы находитесь, следует регулярно очищать от пепла. При езде по вулканическому пеплу необходимо регулярно чистить охлаждающие поверхности радиатора. Во время пеплопада даже в полдень может быть очень темно.

Другой проблемой, не связанной с падением вулканических бомб, является респираторная угроза для дыхательных путей. Эта угроза сохраняется не только во время пеплопада, но и пока пепел остается на земле в рыхлом виде, когда он снова может подняться в воздух от ветра, движущихся автомобилей или даже от попытки пройти по нему. В сущности, такая же проблема возникает в случаях, когда мелкие частицы пепла выпадают из облаков, поднимающихся над пирокластическими потоками. Дождь, как правило, очень эффективно очищает воздух и либо смывает тонкие пепловые осадки, либо превращает их в грязь. Это ликвидирует респираторную угрозу, но создает условия, которые могут приводить к образованию вулканических грязевых потоков [3].

К признакам предстоящего извержения вулкана принято относить: усиление сейсмической активности; «ворчание», доносящееся из кратера вулкана и из-под земли; запах серы, исходящий из протекающих рядом с вулканом рек и ручьев; выпадение кислотных дождей; пемзовая пыль в воздухе; вырывающиеся время от времени из кратера газы и пепел.

Зная об извержении, можно изменить путь лавовых потоков с помощью специальных желобов и лотков. Они позволяютпустить поток в обход жилищ, удержать его в нужном русле. В 1983 году на склоне знаменитой Этны удалось взрывами создать направленное русло для лавы, что спасло от угрозы ближайшие селения.

Иногда помогает охлаждение лавового потока водой – такой способ использовали жители Исландии при борьбе с вулканом, «проснувшимся» 23 января 1973 года. Около 200 мужчин, оставшихся после эвакуации, направили пожарные струи на ползущую к порту лаву. Остывая от воды, лава каменела. Удалось спасти большую часть города.

Существует вопрос: «Как подготовиться к извержению вулкана»?

В первую очередь требуется следить за предупреждением о возможном извержении вулкана. Лучшим вариантом будет своевременно покинуть опасную территорию. При получении предупреждения о выпадении пепла обязательно нужно закрыть все окна, двери и дымовые заслонки. Запастись источниками освещения и тепла, водой, продуктами питания на 3–5 суток.

Как и другие природные катализмы, извержение вулкана часто случается неожиданно и человеку ничего не остается, как оперативно реагировать на это происшествие. Большинство мощных извержений сопровождается землетрясениями, которые как бы предупреждают все живое вокруг, что опасность очень вероятна в ближайшее время. Именно в такой ситуации службы по чрезвычайным ситуациям оповещают население о потенциальном извержении вулкана.

#### **Список используемых источников**

1. **Безопасность** жизнедеятельности в чрезвычайных ситуациях природного характера : учебн. пособие / С. Ю. Блинов, А. П. Зверев. – СПб. : СПбГУТ, 2013. – 80 с.
2. **Камчатские** вулканы не утихают. Электронные ресурсы сети Internet ECOPortal. – Режим доступа: ECOPortal.su/news.php?id=54265 (Дата обращения 09.05.2014).
3. **Безопасность** жизнедеятельности. Защита населения и территорий в чрезвычайных ситуациях : учебн. пособие для вузов / Я. Д. Вишняков и др. – М. : Академия, 2008. – 304 с.

**УДК 681.3**

**М. С. Корчагин (студент группы ИКТВ-33 СПбГУТ)**

**А. К. Сагдеев (преподаватель УВЦ ИВО СПбГУТ)**

**Ю. А. Фролова (студентка группы ИКТВ-33 СПбГУТ)**

#### **ПРИМЕНЕНИЕ ЛЛИПТИЧЕСКИХ КРИВЫХ В СИСТЕМАХ КРИПТОГРАФИИ**

Проблема защиты информации все больше привлекает внимание специалистов, связанных с информационными технологиями. Проблема эта многогранна и решается комплексно, с использованием множества мер и способов.

Как известно, одним из ключевых вопросов обеспечения безопасности информации, хранимой и обрабатываемой в информационных системах, а также передаваемой по линиям связи, является защита ее от несанкционированного доступа. Для защиты информации применяются различные меры и способы, начиная с организационно-режимных и заканчивая применением сложных программно-аппаратных комплексов [1–3].

Одним из путей решения проблемы защиты информации, а точнее – решения небольшой части вопросов из всего спектра мер защиты, является криптографическое преобразование информации, или шифрование.

В случае применения шифрования легальный пользователь получает доступ к закрытым данным только путем их расшифровывания. Получение доступа к зашифрованным данным полностью теряет смысл, если алгоритм и способы осуществления шифрования неизвестны. Однако использование систем криптографической защиты, построенных на основе стойких алгоритмов, само по себе еще не гарантирует надежной защиты.

Современная криптография знает два типа криптографических алгоритмов: классические алгоритмы, основанные на использовании закрытых, секретных ключей (симметричная криптография), и алгоритмов с открытым ключом, в которых используются один открытый и один закрытый ключ (эти алгоритмы называются также асимметричными). Кроме того, существует возможность шифрования информации и более простым способом – с использованием генератора псевдослучайных чисел [2].

У методов симметричной криптографии в результате опыта практического использования выявились следующие недостатки: число возможных ключей должно быть велико, так как если количество ключей мало, то атакующий имеет возможность взломать шифр простым перебором вариантов; кроме этого каждая из переписывающихся сторон должна иметь копию общего секретного ключа, что создает сложнейшую проблему управления ключами.

В алгоритмах асимметричного шифрования используются шифры, основанные на задачах односторонних функций, таких как: разложение целых чисел на множители, вычисление дискретных логарифмов, вычисление квадратных корней по модулю составного числа. Это позволило устранить недостатки, присущие алгоритмам симметричного шифрования.

Однако и алгоритмы асимметричного шифрования не избавлены от ряда недостатков, а именно: надежность алгоритма зависит от сложности использованного разложения, в результате чего увеличивается время дешифрования; увеличение размера ключа также приводит к увеличению времени дешифрования, а также требует дополнительных затрат к памяти. Поэтому необходим алгоритм на основе открытого ключа, обеспечивающий высокий уровень безопасности при относительно малой длине ключа. Алгоритмы, основанные на математических объектах алгебро-геометрических кодов, известных как эллиптические кривые, предлагают новые возможности, благодаря которым можно «избавиться» от некоторых недостатков, присущих алгоритмам асимметричного шифрования [1, 2].

Существуют «четные» и «нечетные» эллиптические кривые [3].

Эллиптическая кривая описывается математическим уравнением вида:

$$y^2 = x^3 + ax + b, \quad (1)$$

где все вычисления выполняются по модулю  $p$ , и  $a^3 + b^2$  не равно 0.

Этот случай называется «нечетным». «Четный» случай аналогичен, вычисления ведутся в конечном поле  $GF(2^m)$  для некоторого целого числа  $m$ .

Математическое свойство, которое делает эллиптические кривые полезными для криптографии, состоит в том, что если взять две различных точки на кривой, то соединяющая их хорда пересечет кривую в третьей точке (так как мы имеем кубическую кривую). Зеркально отразив эту точку по оси  $X$ , мы получим еще одну точку на кривой (так как кривая симметрична относительно оси  $X$  (рис. 1)). Это позволяет точно определить форму кривой. Если мы обозначим две первоначальных точки как  $P$  и  $Q$ , то получим последнюю – отраженную – точку как  $P+Q$ . Это «сложение» удовлетворяет всем известным алгебраическим правилам для целых чисел, позволяя определить единственную дополнительную точку – «бесконечно удаленную точку», выполняющую роль 0 (начала отсчета) для целых чисел.

Другими словами, мы можем определить форму кривой по заданным точкам (плюс бесконечно удаленной точке), что является обычным алгебраическим действием. Выражаясь математическими терминами, мы можем определить конечную абелеву группу (абстрактную группу с коммутативной бинарной операцией) на точках кривой, где нулем будет являться бесконечно удаленная точка. В частности если точки  $P$  и  $Q$  совпадут, то можно вычислить  $P + P$ , т. е.  $2P$ . Далее, можно определить  $kP$  для любого целого числа  $k$ , и, следовательно, определить значение  $P$  и значение наименьшего целого числа  $k$ , такого, что  $kP = F$ , где  $F$  – бесконечно удаленная точка. Теперь можно сформулировать «Проблему Дискретного Логарифма Эллиптической Кривой» (Elliptic Curve Discrete Logarithm Problem – ECDLP), на которой основана рассматриваемая система: «Даны «базовая точка»  $P$  и расположенная на кривой точка  $kP$ ; найти значение  $k$ ».

Секретным ключом пользователя является число  $d$ , открытым ключом – точка  $Q$ .

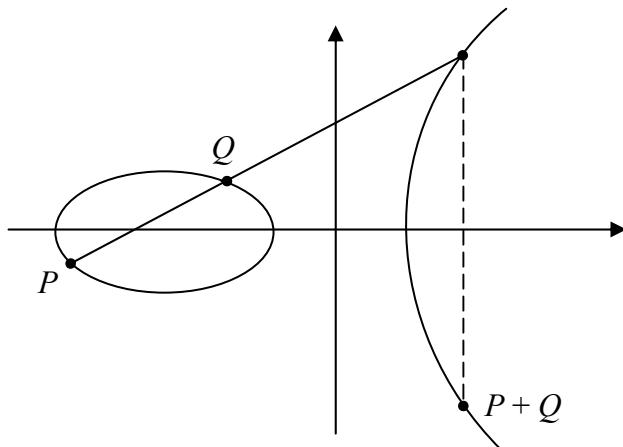


Рис. 1. Принцип «сложения» точек  $P$  и  $Q$  на эллиптической кривой

Рассмотрим, как осуществляются процессы зашифрования и расшифрования сообщений с использованием алгоритмов, основанных на эллиптических кривых.

Зашифрование сообщения (пользователь  $A$  шифрует сообщение  $M$  для пользователя  $B$ ) [4–5]:

1. Сообщение разбивается на блоки  $M_i$ , которые определенным образом дополняются слева (длина каждого блока равна  $2L - 16$  бит, где  $L$  равно ближайшему большему целому от  $\log_2 q$ ).
2. Полученный блок разбивается на две части равной длины:  $m_{i1}$  и  $m_{i2}$ .
3. Выбирается случайное целое число  $k$ ,  $1 < k < n - 1$ .
4. Вычисляется точка  $(x_1, y_1) = kP$ .
5. Вычисляется точка  $(x_2, y_2) = kQ_B$ .
6. С помощью определенного преобразования из  $m_{i1}$  и  $m_{i2}$  и  $x_2$  получают  $c_1$  и  $c_2$ .
7. Зашифрованные данные:  $(x_1, y_1, c_1, c_2)$ .

Расшифрование сообщения (пользователь  $B$  расшифровывает полученное от пользователя  $A$  зашифрованное сообщение) [4–5]:

1. Вычисляется точка  $(x_2, y_2) = d(x_1, y_1)$ .
2. Восстанавливается исходное сообщение  $m_{i1}$  и  $m_{i2}$  из  $c_1$ ,  $c_2$  и  $x_2$ .

В случае перехвата сообщения злоумышленником  $C$  нужен один из секретных ключей: знание обоих открытых ключей не решит проблемы. Чтобы взломать секретный ключ  $A$  (возможно, это и попытается сделать  $C$  в первую очередь),  $C$  должен определить  $d$ . Для этого ему потребуется решить задачу дискретного логарифмирования на эллиптических кривых, на что может понадобиться несколько миллионов лет, поэтому  $C$  может попытаться применить атаку с прямым перебором. Проблема в том, что  $d$  имеет тот же размер, что и диапазон значений. Так если абонент  $A$  выбрал 160-битный или 170-битный диапазон, что означает, что  $d$  также имеет длину 160 или 170 битов, то прямой перебор не даст результата [4–5].

Решить задачу дискретного логарифмирования на эллиптической кривой сложнее, чем решить задачу дискретного логарифмирования или разложения на множители.

Из-за очевидной трудности взлома алгоритм ECDLP можно применять для высоко защищенных систем. Обеспечивая сопоставимый уровень безопасности, алгоритм имеет значительно меньшие размеры ключа, чем, например, алгоритмы RSA или DSA. Следовательно, использование эллиптических кривых позволяет строить высоко защищенные системы с ключами явно меньших размеров по сравнению с аналогичными «традиционными» системами типа RSA или DSA. В частности такие системы менее требовательны к вычислительной мощности и объему памяти оборудования [2].

Разумеется, существуют и проблемы, которые ограничивают повсеместное распространение криптографических систем на основе эллиптических кривых. Некоторые использовавшиеся для отработки алгоритмов шифрования эллиптические кривые, фактически не подходят для таких операций. Такие кривые являются «аномальными» кривыми.

При определении системы эллиптической кривой требуются сама кривая и базовая точка ( $P$ ). Причем, эти элементы не являются тайной и могут быть одинаковыми для всех пользователей системы. Для данной кривой и точки несложно сгенерировать открытые и частные ключи для пользователей (частный ключ – просто случайное целое число  $k$ , а открытый ключ – точка  $kP$  на кривой). Однако, чрезвычайно трудно создать подходящую кривую и точку. Главная проблема – подсчитать количество точек на кривой. Для этого необходимо выбрать подходящую базовую точку  $P$ , координаты которой должны иметь достаточно большое значение, чтобы гарантировать трудность взлома ECDLP. Но координаты  $P$  должны делиться на количество точек на кривой (точки на кривой вместе с бесконечно удаленной точкой образуют конечную группу). И весьма вероятно, что, найдя число точек на кривой, мы не сможем найти базовую точку.

Несмотря на то, что «четные» и «нечетные» эллиптические кривые подобны, они все же различаются настолько, что «нечетная» система гарантированно несовместима с «четной» системой. Кроме того, в случае «четной» системы существуют различные способы представления кривых и базовых точек, причем пользователи систем с разными способами представления не имеют возможности связаться друг с другом [3–5].

Но несмотря на имеющиеся трудности, из-за проблемы выбора эллиптической кривой для осуществления шифрования, криптосистемы на основе эллиптических кривых получают все большее распространение, поскольку системы на основе ECDLP имеют некоторые преимущества, особенно при использовании в устройствах с маломощными процессорами и/или маленькой памятью. Однако из-за существующих сложностей скорее как альтернатива, а не замена системам на основе RSA. Таким образом, разработка алгоритмов криптографической защиты, основанных на использовании эллиптических кривых, является перспективной научной задачей.

### Список используемых источников

1. Алгоритмические основы эллиптической криптографии / А. А. Болотов, А. Б. Гашков и др. – М. : Московский энергетический институт, 2000. – 112 с.
2. Защита информации в компьютерных системах / К. Ю. Гундарь, А. Ю. Гундарь, Д. А. Янишевский. – К. : Корнейчук, 2000. – 152 с.
3. Защита информации и безопасность компьютерных систем / В. В. Домарев. – К. : Диасофт, 1999. – 480 с.
4. Применение алгебро-геометрических кодов в системах криптографии / А. К. Сагдеев, Н. И. Червяков // 4-я научно-техническая конференция «Инфокоммуни-

кационные технологии в науке, производстве и образовании»: сборник докладов. – Ставрополь : СКГТУ, 2010. – С. 56–59.

5. **Линейное** разделение секрета для алгебро-геометрических кодов на эллиптических кривых / А. К. Сагдеев, Н. И. Червяков // Всероссийская научная конференция «Параллельная компьютерная алгебра»: материалы конференции. – Ставрополь : СГУ, 2010. – С. 245–251.

**УДК 676.1**

**Н. П. Куров, С. А. Рудик (студенты группы ТСС-26 СПбГУТ)**

## **О ЦЕЛЕСООБРАЗНОСТИ ИСПОЛЬЗОВАНИЯ МАЛООТХОДНЫХ, РЕСУРСОСБЕРЕГАЮЩИХ И ЭКОЛОГИЧЕСКИ БЕЗОПАСНЫХ ТЕХНОЛОГИЙ ХИМИЧЕСКОЙ ПЕРЕРАБОТКИ ДРЕВЕСИНЫ**

Россия является крупнейшей лесной державой мира, на ее долю приходится четверть мирового лесного покрова. Лесам России принадлежит исключительное глобальное биосферное значение, поскольку они обеспечивают экологическую безопасность страны и планеты.

Леса занимают почти половину территории Российской Федерации, являются возобновляемым природным ресурсом и отличаются значительным природным разнообразием. Леса относятся к одному из ключевых факторов социально-экономического развития страны, выполняют многочисленные средообразующие и экологические функции, обеспечивают сохранение благоприятной окружающей среды.

Сегодня лесной сектор экономики страны нуждается в развитии инновационных технологий лесопользования, в появлении новых видов древесной продукции, ужесточении экологических требований, особенно, в части широко используемых отечественной целлюлозно-бумажной промышленностью (ЦБП) технологий химической переработки древесины.

ЦБП – одна из важнейших отраслей РФ. Продукция ЦБП составляет 1,24 % от объема промышленной продукции России и около 2 % от мирового производства. Традиционными способами химической переработки древесины, применяемыми отечественной целлюлозно-бумажной промышленностью, являются сульфатный и сульфитный способы производства целлюлозы. Сравнительная характеристика этих способов приведена в таблице 1.

**ТАБЛИЦА 1. Сравнительная характеристика основных способов сульфатного и сульфитного производства целлюлозы**

	Сульфатная целлюлоза	Сульфитная целлюлоза
Положительные	Возможна переработка практически любой древесины выход целлюлозы в среднем 45 %; бумага имеет более высокую прочность, термостойкость, долговечность, непрозрачность; обладает более высокими диэлектрическими свойствами (кабельная, конденсаторная, телефонная бумага); из сульфатной целлюлозы производят мешочную и оберточную бумаги, картонную тару, бумажный шпагат.	Более высокий выход целлюлозы, порядка 50 %, из древесины обеспечивает повышенную способность к размолу, лучшие оптические и деформационные свойства, высокую белизну, что позволяет использовать ее в массовых видах бумаги, типа газетной, в небеленом виде; высокая способность к отбелке, в том числе без применения хлора; при получении в атмосферу не поступают метилмеркаптаны, сероводород и дурнопахнущие летучие вещества, а в сточных водах отсутствуют сульфиды;
Отрицательные	Волокна целлюлозы более гибкие и они, труднее размываются; волокна бурого цвета; без регенерации сульфатный способ технологически не может функционировать; содержит дурнопахнущие серосодержащие вещества, значительный объем высокотоксичных сточных вод – высокая экологическая агрессивность	Проблема утилизации отработанных щелоков, которые загрязняют окружающую среду. При варке происходит повышенное воздействие на окружающую среду (водоемы), в основном, из-за ограниченности сбыта технических лигносульфонатов (упаренных щелоков), а также отсутствие систем регенерации химикатов и тепла из отработанных щелоков, утилизируется лишь 30 – 40 % сухих веществ щелока; высокий расход серы и варочного основания; не используются вторичные тепловые ресурсы органических веществ щелока; щелока при разбавлении становится хорошими питательным субстратом для многих микроорганизмов, вызывая сильное обрастание подводных сооружений.

Как следует из таблицы 1 как сульфатный, так и сульфитный способ переработки древесины являются экологически агрессивными, реализация этих процессов сопровождается сбросом значительных объемов высокотоксичных сточных вод и выбросом загрязненных отходящих газов. Выход целлюлозы при традиционных технологиях химической обработки порядка 50 %. Кроме того, значительный вклад в загрязнение окружающей среды привносит, также, производство картона и бумаги, блок-схема этого технологического процесса представлена на рисунке 1. Большинство технологических операций в технологии производства бумаги связано со значи-

тельным расходом воды и образованием больших объемов загрязненных сточных вод.

В целом, целлюлозно-бумажная промышленность РФ – наиболее сложная отрасль лесного комплекса, связанная химической переработкой древесины, включает производство целлюлозы, бумаги, картона и изделий из них.

Целлюлозно-бумажная промышленность РФ отличается:

- высокой материалоёмкостью: для получения 1 т целлюлозы необходимо в среднем 5–6 куб. м. древесины;
- большой водоёмкостью: на 1 т целлюлозы расходуется в среднем 350 куб. м. воды;
- значительной энергоёмкостью: 1 т продукции требует в среднем 2000 кВт/ч [1].

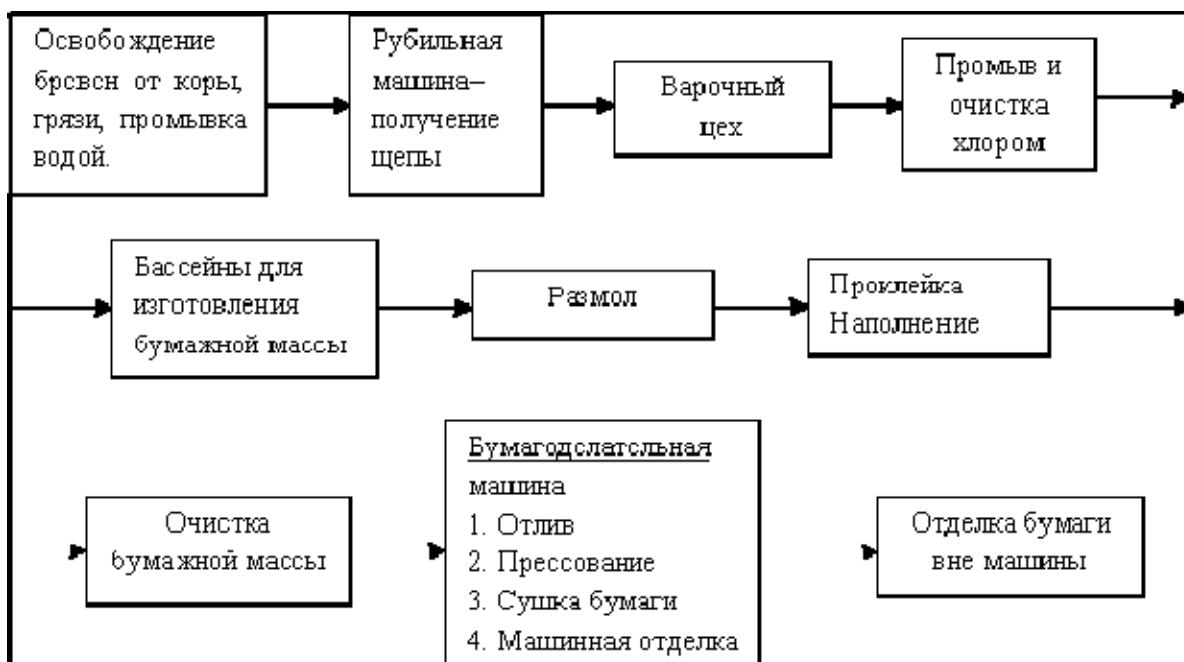


Рис. 1. Блок-схема производства бумаги

С наступлением XXI века проблемы сохранения и использования лесов становятся все более сложными. В новых социально-экономических условиях, а также в связи с увеличением рисков природных, техногенных и экологических катастроф существующие подходы к химической переработке древесины требуют изменений. Попыткой решения этих актуальных задач явились новые малоотходные технологии переработки древесины, обеспечивающие выход целевого продукта – волокнистого (целлюлозного) полуфабриката порядка – 90–99 % от массы исходной древесины. В девяностых годах XX века появилось множество модификаций производства полуфабрикатов высокого выхода: ДДМ, ДМД, РММ, ТММ, ХТММ, ХММ использование которых позволяет почти вдвое увеличить

выход полезного продукта по сравнению с сульфатным и сульфитным производством целлюлозы и, соответственно, сократить количество промышленных выбросов, снизить себестоимость продукции [2]. При этом, выход полуфабрикатов из древесины косвенно, в свою очередь, обуславливает загрязнённость сточный воды. Чем больше выход целевого продукта, тем меньше загрязненность сточной воды. По увеличению загрязнённости сточных вод различные виды производств высокого выхода располагаются в следующем порядке:

ДДМ>ДМД>РММ>ТММ>ХТММ>ХММ,

где ДДМ – дефибривированная древесная масса;

ДМД – дефибривированная древесная масса, полученная под давлением;

РММ – рафинерная механическая масса;

ТММ – термомеханическая масса;

ХТММ – химико-термомеханическая масса;

ХММ – химико-термомеханическая масса.

На рисунке 2 студенты гр. ТСС-26 Рудик С. О., Курев Н. П. СПбГУТ во время выступления на 68 ежегодной научно-практической конференции, апрель 2014 года с докладом о малоотходных технологиях химической переработки древесины.



Рис. 2. Студенты гр. ТСС-26 во время доклада о необходимости перехода на экологически ответственное лесопользование и освоении малоотходных способов химической переработки древесины

При этом, по мере повышения интенсивности химического воздействия на древесное сырьё в процессе термогидролитической или химико-

термо-гидролитической обработки древесины снижается выход целлюлозного полуфабриката и повышается загрязнённость сточных вод: содержание БПК и ХПК (биохимическое потребление кислорода, химическое потребление кислорода в образующихся сточных водах этих производств). Данные по степени загрязненности сточных вод в зависимости от выхода целевого продукта представлены в таблице 2.

ТАБЛИЦА 2. Зависимость степени загрязненности сточных вод различных производств целлюлозных полуфабрикатов в зависимости от величины выходы целевого продукта

Влияние выхода из древесины на содержание БПК и ХПК в сточной воде								
Выход из древесины, %	95	94	93	92	91	90	89	88
Содержание БПК, кг/т	35–40	40–47	45–51	48–55	53–59	56–63	63–65	63–70
Содержание ХПК, кг/т	76–86	83–98	93–110	110–119	110–129	120–128	129–146	135–153

Как следует из таблицы 2, чем меньше выход целевого продукта, чем в большей степени древесина подвергается химической обработке, тем больше загрязненность образующихся сточных вод и тем выше экологическая агрессивность производства в целом [3].

Таким образом, сегодня развитие технологии химической переработки древесины должно быть направлено на достижение стратегической цели – устойчивого развития отечественного лесопромышленного комплекса с учётом необходимости внедрения малоотходных ресурсосберегающих и экологически безопасных технологий переработки древесины, обеспечивающих охрану водных, воздушных и лесных ресурсов Земли.

#### Список используемых источников

1. Путь к рациональной экосистеме / Н. Е. Манвелова // Целлюлоза, бумага, картон. –2005. – № 7. – С. 74–77.
2. Современные технологии механической массы. Т. 2 / С. С. Пузырев. – СПб. : СПб ЛТА, 1996. – С. 177–179.
3. Сточные воды производства механической массы / С. С. Пузырев, О. П. Ковалева, Ю. А. Поляков, Н. Е. Манвелова // Целлюлоза, бумага, картон. – 2005. – № 5. – С. 46–50.

*Статья подготовлена под научным руководством к.т.н., доцент кафедры ЭБЖД Н. Е. Манвеловой*

УДК 504:550.1

**Н. Е. Манвелова (доцент кафедры ЭБЖД СПбГУТ)**  
**Д. Г. Никитин (студент группы ИКТС-21 СПбГУТ)**  
**С. А. Панихидников (заведующий кафедрой ЭБЖД СПбГУТ)**

## **ЭКОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ОКОЛОЗЕМНОГО КОСМИЧЕСКОГО ПРОСТРАНСТВА**

Сегодня развитие общества уже немыслимо представить без широкомасштабного использования космической техники. Радиосвязь и телевидение, навигация и картография, разведка полезных ископаемых, метеорология и контроль состояния биосферы – вот далеко не полный перечень областей, в которых находит применение космическая техника и используется получаемая с её помощью информация. В космической отрасли, как и в других областях техногенной деятельности человечества в 20 веке, постепенно решались ключевые задачи, каждая из которых знаменовала важный этап в развитии космических исследований и космической техники. На начальном этапе главной целью был сам факт прорыва в космос, т. е. запуск первого искусственного спутника Земли (ИЗС). Далее потребовалось измерение разнообразных параметров космической среды с помощью ИЗС, для чего было необходимо разработать соответствующие методы и приборы. Позднее наступили этапы создания различных космических систем для решения широкого круга прикладных и научных задач. Таким образом, космонавтика стала важной составляющей хозяйственного механизма, а ее достижения – неотъемлемой частью нашей повседневной жизни. При этом, развитие деятельности человека в космосе происходило по тем же основным канонам, что и развитие технической и хозяйственной деятельности на Земле: сначала нужно было «покорить природу и заставить ее служить людям», а затем обеспечить эффективное и длительное использование открывающихся новых возможностей и природных ресурсов. Но практически в любой сфере широкомасштабной хозяйственной деятельности на определенном этапе неизбежно приходится решать задачи, связанные с охраной окружающей природной среды. Космическая деятельность не является исключением в этом отношении. Уже к середине 1970-х годов стало ясно, что эксплуатация ракетно-космической техники может оказывать существенное влияние на состояние околоземной среды, и возникла необходимость проведения серьезных исследований по этой проблеме. В космической деятельности, таким образом, к вопросам, связанным с защитой окружающей природной среды, пришло обратиться менее чем через 20 лет после начала космической эры [1].

При этом, современная цивилизация оказывает такой уровень техногенного воздействия на ближний космос, какой не испытывает ни одна

другая среда: ни гидросфера, ни литосфера, ни приземная атмосфера. Освоение этой среды ведется самыми мощными современными средствами. При этом установлено, что околоземное пространство имеет на много порядков меньше, чем биосфера связей, обеспечивающих его устойчивость. Глобальные соотношения по выбросам энергии и вещества здесь значительно превышают подобные соотношения для биосферы. Техногенные воздействия в околоземном космическом пространстве в настоящее время имеют мощность на два порядка меньшую мощности естественных воздействий, при том, что их рост проходит практически по экспонциальному закону [2].

На рисунке 1 представлена общая схема процессов, возникающих в верхней атмосфере в результате запусков ракетно-космической техники [3].



Рис. 1. Схема физических процессов и последствий запусков ракетно-космической техники на верхнюю атмосферу

Основными видами техногенного воздействия на околоземное космическое пространство (ОКП) являются: механическое, химическое, радиоактивное и электромагнитное загрязнение. Данные о типах и последствиях техногенного загрязнения ОКП при осуществлении космической деятельности представлены в таблице 1 [4].

**ТАБЛИЦА 1.** Типы и последствия техногенного загрязнения ОКП при осуществлении космической деятельности

Типы загрязнений	Источники	Последствия
Механическое	Фрагменты космических аппаратов и ракет, частицы покрытий космических аппаратов, твердые частицы выбросов ракетных двигателей	Космический мусор и пыль, повреждения космических аппаратов, помехи астрономическим наблюдениям, воздействия на верхнюю атмосферу
Химическое	Ракетные двигатели, электроракетные двигатели, наземные источники	Ионосферные дыры, нарушения радиосвязи, изменения состава верхней атмосферы, разрушение озонового слоя, неустойчивости в магнитосфере
Радиоактивное	Бортовые ядерные энергетические установки	Опасность радиоактивного загрязнения атмосферы и поверхности Земли при разрушении устройств
Электромагнитное	Бортовые передатчики ВЧ, наземные передатчики ВЧ и ОНЧ	Возмущения ионосферы и магнитосферы, высыпания заряженных частиц, помехи радиосвязи

Проблему техногенных отходов в ОКП можно рассматривать как с точки зрения экологии космоса, так и исходя из вопросов воздействия этих отходов на земную природу с целью предотвращения (или, по крайней мере, уменьшения) такого воздействия.

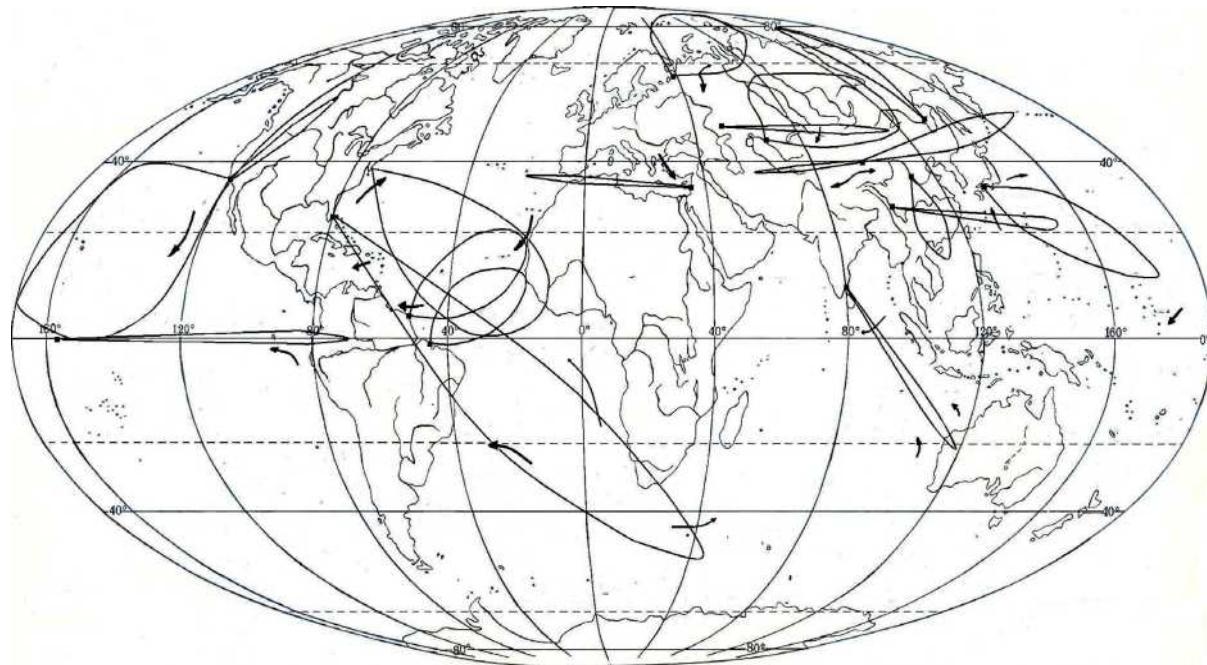


Рис. 2. Зоны действия основных космодромов мира (стрелки – направления ветра)

Проблема увеличения числа техногенных объектов в ОКП становится все более актуальной в связи с рядом факторов:

- проблемами безопасности пилотируемых космических полетов;
- столкновениями космических объектов друг с другом или с техногенным мусором с образованием новых осколков;
- возможностью непрогнозируемого выпадения космических объектов и техногенных осколков на Землю, химическим, биологическим, радиоактивным заражением ее поверхности и атмосферы;
- разрушением космических объектов в результате взрывов на орбите и взрывов их ракет-носителей в верхних слоях атмосферы при старте, прямо воздействующих на земную природу;
- заражением верхней атмосферы, ионосферы, биосферы продуктами сгорания ракетного топлива при запусках космических объектов;
- возникновением помех астрономическим наблюдениям и различным экспериментам в ОКП;
- изменением свойств ОКП, верхней атмосферы и ионосферы Земли, что может привести к необратимым изменениям в биосфере.

Отмечено, что наиболее уязвимыми, с точки зрения положения зон загрязнения на земной поверхности, образованных основными действующими космодромами мира представлены на рисунке 2 [4].

Область выпадения остатков конструкций ракетоносителей для космодрома Байконур простирается до Якутии, трасса запусков с космодромов *Cape Canaveral* заканчивается над Индийским океаном около островов Принс-Эдуард. Полётная трасса базы *Vandenberg* имеет протяжённость около 10 000 км и простирается над Тихим океаном и заканчивается у острова Кантон (острова Феникс) и близ атолла Кваджалейн (Маршалловы острова). Основным районом старта при запусках по проекту «Морской старт» является экваториальная зона в Тихом океане вблизи острова Рождества, зона падения отделяющихся частей достигает территории Южной Америки. Хотя надо признать, что последний проект является одним из самых экологичных: после отделения космического аппарата разгонный блок уводится на орбиту хранения, где из него стравливаются остатки топлива и газы [4, 5].



Рис. 3. Студент Никитин Д. Г. гр. ИКТС-21 докладывает о возможностях предотвращения техногенного загрязнения околоземного космического пространства

В рамках изучения дисциплины «Военная экология» рассматривались следующие возможности предотвращения техногенного загрязнения околоземного космического пространства, которые были изложены в докладе студента гр. ИКТС-21 Никитина Д. Г. (рис. 3):

- формирование технологий и конструкций ракетно-космической техники, приводящих к минимизации отходов;
- разработка конструкций космического оборудования, включая служебные системы и научную аппаратуру, приспособленных для использования в космосе после истечения своего ресурса;
- выбор наиболее эффективных направлений применения в космическом полете отходов, образующихся в результате функционирования оборудования и жизнедеятельности экипажа.

Таким образом, космическое пространство постепенно становится своеобразной частью среды обитания и деятельности человека, происходит расширение содержания понятия «окружающая природная среда» с включением в это понятие околоземного космического пространства. Космическая техника способна вызывать определенные возмущения в окружающей космической среде. Околоземное пространство в целом представляет собой весьма динамичную и нестабильную систему, которая под влиянием внешних воздействий может переходить в неустойчивое состояние.

#### Список использованной литературы

1. **Основы экологии** околоземного космического пространства / Л. С. Новиков. – М. : МГУ им. М. В. Ломоносова, 2006. – 83с.

2. **Физические основы экологии** околоземного пространства / А. К. Муртазов. – Рязань : РГУ им. С. А. Есенина, 2008. – 270 с.
3. **Экологические проблемы и риски** воздействия ракетно-космической техники на окружающую среду. Справочное пособие / В. В. Адушкин, С. И. Козлов, А. В. Петров. – М. : Анкид, 2000.
4. **Модель космоса.** Т. 1, 2 / Под ред. М. И. Панасюка и Л. С. Новикова. – М. : КДУ, 2007. – 346 с.
5. **Экология околоземного** космического пространства / А. К. Муртазов. – М. : ФИЗМАТЛИТ, 2004. – 304 с.

**УДК 623.459:591.571(261.22)**

**Н. Е. Манвелова (доцент кафедры ЭБЖД СПбГУТ)  
С. А. Панихидников (заведующий кафедрой ЭБЖД СПбГУТ)  
К. С. Филиппов (студент группы ИКТС-21 СПбГУТ)**

## **НЕКОТОРЫЕ АСПЕКТЫ УТИЛИЗАЦИИ ХИМИЧЕСКОГО ОРУЖИЯ**

Одной из актуальных проблем, волнующих все человечество является проблема утилизации отравляющих веществ химического оружия. Первая попытка решения этой глобальной задачи была осуществлена в соковые годы минувшего столетия. После окончания 2-й Мировой войны на оккупированной территории Германии было обнаружено 296 103 т химического оружия. На Потсдамской мирной конференции стран антигитлеровской коалиции в 1945 г. было принято решение об уничтожении этого химического оружия. В результате, в Балтийское море, его заливы и проливы было сброшено 267,5 тысяч тонн бомб, снарядов, мин и контейнеров в которых содержалось 50–55 тысяч тонн боевых отравляющих веществ 14 видов. Активное участие в этом деле принимал и СССР. Его ВМС затопили в Балтийском море 35 000 тонн химического оружия. Наиболее крупное (примерно 33 000 т.) официально подтвержденное захоронение химического оружия находится в первом районе в 35 милях восточнее принадлежащего Дании о. Борнхольм в Борнхольмской впадине на глубине 70–100 метров. Второй, официально подтвержденный район захоронения химического оружия, значительно меньший по количеству затопленного химического оружия (около 2 000 т), но существенно превышающий его по площади, находится в 65 милях от Лиепая юго-восточнее о. Готланд в Готландской впадине на глубине 70–120 метров. Этот район состоит из нескольких захоронений и находится в территориальных водах нескольких государств (Швеции, Польши и Латвии). Третий, официально

подтвержденный район захоронения химического оружия (примерно 5 000 т), располагается южнее пролива Малый Бельт [1].

Однако, вследствие частичной и/или полной разгерметизации в морской воде контейнеров и боеприпасов, содержащих отравляющие вещества, последние, рано или поздно, попадают в воды Балтийского моря и становятся реальной угрозой поражения, что определяет негативные последствия этого способа утилизации химического оружия. Наибольшую опасность для среды обитания представляет иприт, большая часть которого окажется на морском дне в виде кусков ядовитого студня. Дело в том, что иприт и люизит хорошо гидролизуются, соединяясь с водой, и образуют токсичные вещества, сохраняющие свои свойства в течение нескольких десятилетий. Свойства люизита аналогичны иприту, однако, люизит – это мышьякорганическое вещество, так что экологически опасны практически все продукты его трансформации [1].

На рисунке представлена фотография студента гр. ИКТС-21 Филиппова К. С. (Институт военного образования СПб ГУТ), выступающего с докладом, посвященным проблемам утилизации химического оружия, на региональной НТК, состоявшейся в апреле 2014 года.



Рисунок. Выступление с докладом по вопросу утилизации химического оружия  
Филиппова К. С. студента гр. ИКТС-21 ИВО СПб ГУТ

В настоящее время отравляющие вещества подразделяются на несколько видов: кожно-нарывные, нервнопаралитические, удушающие, общеядовитые, психохимические и раздражающие. При этом часть из них относится к оружию нелетального воздействия, такие вещества часто используются службами правопорядка для разгона несанкционированных митингов и демонстраций. К примеру, американская полиция часто применяет аэрозоли со слезоточивым газом или седативными препаратами, например, диазепамом. Если же говорить о боевых отравляющих веществах, то наибольшее распространение в мире получили: зоман, зарин, табун, VX (нервнопаралитического действия), люизит (кожно-нарывного действия), дифосген (удушающий), а также хлорпикрин (раздражающего действия) [2].

Следующая попытка решения задачи утилизации химического оружия была предпринята в конце XX века. В 1993 году в Женеве для подписания была открыта «Конвенция о запрещении химического оружия». К данной конвенции присоединилось большинство государств мира, хотя по большому счету этот документ задумывался лишь для 2-х стран: России и США, которые на то время обладали более чем 90 % всех мировых запасов химоружия. Данная Конвенция, вступила в законную силу в 1997 году. После этого шесть стран открыто признали наличие у них отравляющих веществ – Албания, Индия, Ливия, Россия и США, а также государство, которое отказалось от упоминания в официальных документах (этим государством была Южная Корея).

Программа по утилизации химического оружия стартовала в последние годы XX века. Согласно международной Конвенции страны, её подписавшие, должны были уничтожить 1 % своих запасов химического оружия к апрелю 2000 года, 20 % – к апрелю 2002 года, 45 % – к апрелю 2004 года и 100 % химоружия – к апрелю 2007 года. Однако из-за необходимости постройки ряда достаточно технически сложных производств по утилизации химических боеприпасов, последний срок можно было перенести на апрель 2012 года. Первыми правом переноса воспользовались США [3].

В Российской Федерации для успешного выполнения условий Конвенции была разработана Федерально-целевая программа: «Уничтожение запасов химического оружия в Российской Федерации», утвержденная постановлением Правительства Российской Федерации от 21 марта 1996г. № 305. На начало 2012 года в РФ функционировало шесть предприятий по утилизации отравляющих веществ: «Горный» (Саратовская область), «Камбарка» (Удмуртская Республика), «Леонидовка» (Пензенская область), «Марадыково» (Кировская область), «Почеп» (Брянская область), «Щучье» (Курганская область). При этом, «Горный» и «Комбарка» закончили переработку ОВ в 2008 и 2009 годах и приступили к переработке промышленных отходов. Ввод предприятия «Кинзер» в Удмуртии намечен на 2015 год на предприятии планируется утилизировать порядка 1,8 тыс.

тонн химического оружия в год. Завод будет приспособлен для уничтожения сложных боеприпасов. Речь идет о ракетах, авиабомбах и артиллерийских снарядах. В таких боеприпасах помимо ОВ содержатся еще и взрывчатые вещества. Утилизация такого рода боеприпасов занимает больше времени, так как, первоначально их необходимо разобрать, после чего отдельно провести детоксикацию отравляющих веществ и уничтожить взрывчатое вещество. При этом в России обезвреживание зомана и зарина осуществляется с помощью воды иmonoэтаноламина, VX – изобутилата калия, люизита – методом щелочного гидролиза.

В настоящее время разработано и освоено несколько методов утилизации химического оружия, основными из которых являются: химические и термические методы. Химические методы утилизации отравляющих веществ основаны на реакциях их с различными химическими реагентами, в результате которых образуются нетоксичные продукты. К примеру, щелочной гидролиз отравляющих веществ, который протекает в специальных водных растворах щелочей с образованием соли метилалкилфосфорной кислоты, которая не является токсичным соединением. При окислительном хлорировании в роли окислителя применяют хлор, гипохлорит натрия и кальция, пероксид водорода. Из-за высокой реакционной способности данных веществ, разложение химических веществ может сопровождаться взрывом, поэтому данные реакции с отравляющими веществами можно проводить в суспензиях или водных растворах.

Термическое уничтожение химического оружия в боеприпасах заключается в разложении отравляющих веществ в замкнутом пространстве без доступа к нему кислорода. Термодеструкция может использоваться для уничтожения отравляющих веществ прямо в боеприпасах, которые обладают существенным запасом прочности по отношению к внутреннему давлению. При нагревании химических боеприпасов до высоких температур 150 °C в них значительно увеличивается внутреннее давление в результате термического расширения химических веществ. При дальнейшем нагревании боеприпасов до температур выше 200 °C внутреннее давление в них достигает предельных значений и осуществляется разгерметизация корпуса боеприпасов, которая сопровождается выбросом газообразных продуктов, составляющих от 30 до 40 % от исходного объема вещества. При этом образовавшиеся газообразные продукты используются для дальнейшего термического разложения, которое осуществляется на нагретом до 500 °C катализаторе, после чего газы поступают на щелочной скруббер. Дальнейший процесс нагревания корпуса боеприпасов обеспечивает их полное обезвреживание. В зависимости от длительности и скорости нагревания можно достичь степени уничтожения химически опасных веществ от 90 до 99 %.

В настоящее время в РФ, крупнейший в Европе завод по ликвидации ХО работает в городе Почепе. Завод функционирует круглые сутки. Днем

и ночью 3 полностью автоматических линии производят, если говорить техническим языком, «расснаряжение боеприпасов» различных калибров. Каждый, кто отправляется в его цеха, надевает на себя особые герметичные костюмы. Данные костюмы абсолютно безопасны, но находиться в них в рабочих цехах можно не более 4-х часов.

В зависимости от калибра в бомбах хранится до 270 кг химических реагентов, для того чтобы утилизировать такой боеприпас тратится 5 минут. Основной профиль предприятия в Почепе – это утилизация авиационных бомб, снаряженных зоманом, зарином и веществом VX. Весь процесс утилизации боеприпасов протекает внутри полностью герметичных автоматизированных станций. Сначала боеприпасы проходят процедуру взвешивания, после чего отправляются в герметичную камеру, в которой происходит операция по проколу корпуса и извлечению из него ОВ. На случай возникновения возможных утечек (за все время работы не было ни одной) на территории предприятия осуществляется постоянный мониторинг по десяткам различных параметров, а работающий здесь личный состав, проходит специальную подготовку. Из центрального пункта управления ведется автоматизированный контроль за ходом уничтожения ХО. После того как отправляющее вещество было нейтрализовано с помощью особых реагентов, а оболочки боеприпасов отправились в печи обжига, полученная малотоксичная масса подается на заключительную стадию термического обезвреживания. В огромных печах при помощи горения природного газа поддерживается температура порядка 1200 °C. Под воздействием такой высокой температуры осуществляется разложение поступивших масс на шлам и дымовые газы [4].

Полная ликвидация российского арсенала химического оружия в РФ должна закончиться в 2015 году, в год столетия первого в мире масштабного боевого использования ХО. После этого предприятие будет перепрофилировано для использования в гражданских целях [5].

Таким образом, решение сложной общественно значимой проблемы утилизации химического оружия требует серьезных, последовательных усилий со стороны мирового сообщества, осознавшего необходимость этого шага.

#### Список использованной литературы

1. **Затопленное химическое оружие:** состояние проблемы / В. Т. Пака // Рос. хим. журнал. – 2004. – Т. XLVIII, № 2. – С. 99–109.
2. **Основы экологической токсикологии :** учебное пособие / В. С. Янин. – Пенза : ПГУАС, 2005. – 124 с.
3. **Мировое сообщество и химическое оружие** / В. В. Щелученко, В. В. Демидюк. – М. : Агентство Ракурс, 2000. – 165 с.
4. **Экологическая безопасность** при эксплуатации и уничтожении химического оружия: научное пособие / В. К. Марынин. – Пенза : ПГУАС, 2004. – 82 с.
5. <http://lenta.ru/news/2013/01/31/chemistry>

УДК 621.395.52, 621.315.28

И. Ф. Пырву (студентка группы ИКТВ-32 СПбГУТ)

## СХЕМОТЕХНИЧЕСКОЕ РЕШЕНИЕ ПО ПОСТРОЕНИЮ ПРИЕМНИКА ДИСТАНЦИОННОГО ПИТАНИЯ НЕОБСЛУЖИВАЕМОГО ОПТИЧЕСКОГО УСИЛИТЕЛЯ

В настоящее время строительство подводных волоконно-оптических линий передачи (ВОЛС) приобретает огромное значение. Строительство подводных ВОЛС сопряжено с большими технико-экономическими затратами связанными с жёсткими физико-географическими условиями эксплуатации. В связи с этим возникает проблема в разработке надёжных схем организации питания необслуживаемых оптических усилителей (НОУ) и элементов схем [1].

Приемник дистанционного питания (ПДП) необслуживаемого оптического усилителя предназначен для отбора мощности из линии ДП, преобразовании токов и напряжений до требуемых величин с целью организации питания элементов и схем усилителя.

Функциональная схема ПДП представлена на рисунке 1.

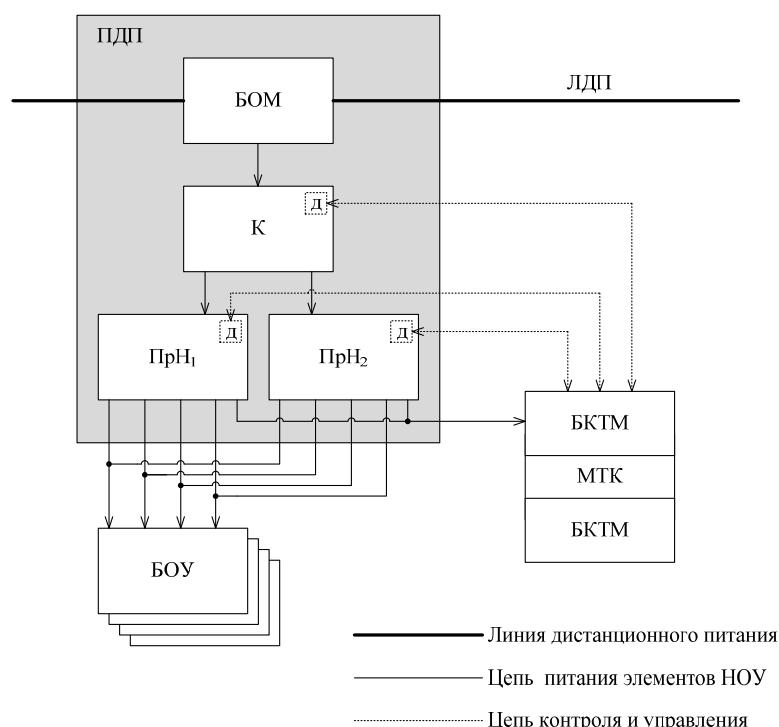


Рис. 1 Функциональная схема приемника дистанционного питания НОУ  
(ЛДП – линия дистанционного питания; ПДП – приемник дистанционного питания;  
БОМ – блок отбора мощности; ПрН – преобразователь напряжений; К – коммутатор;  
БОУ – блок оптических усилителей; БКТМ – блок контроля и телемеханики НОУ;  
МТК – узел МТК)

В состав ПДП входят следующие блоки:

БОМ – блок отбора мощности;

ПрН<sub>1</sub> – преобразователь напряжений основной;

ПрН<sub>2</sub> – преобразователь напряжений резервный;

К – коммутатор.

Блоки отбора мощности каждого НОУ включаются в линию ДП последовательно и обеспечивают требуемую нагрузку цепи ДП для эффективного отбора мощности.

Блок отбора мощности должен обеспечить ответвление из цепи ДП мощности, требуемой для питания всех элементов НОУ, в допустимых пределах работы системы ДП ВОЛС и защиту от опасных токов и напряжений, а также подавление помех различного происхождения.

Преобразователь напряжений основной (резервный) формирует сетку напряжений необходимую для питания всех элементов и схем усилителя.

Коммутатор предназначен для оперативного подключения выхода БОМ и входа ПрН<sub>1</sub> и ПрН<sub>2</sub> с целью повышения надежности ПДП НОУ.

Блоки К, ПрН<sub>1</sub> и ПрН<sub>2</sub> в своем составе должны иметь датчики контроля состояния которые включены в систему телеконтроля блока БКТМ.

Приемник дистанционного питания (ПДП) содержит (рис. 2) стабилитрон  $VD_1$ , включенный в линию ДП последовательно. Параллельно стабилитрону  $VD_1$  через фильтрующий конденсатор  $C_1$  подключены два устройства отбора энергии (основной и резервный), к выходам которых через фильтрующие конденсаторы  $C_2$  и  $C_3$  и автоматический переключатель источников питания ( $VS_1$  и  $VS_2$ ) подключена нагрузка ПДП  $R_h$ .

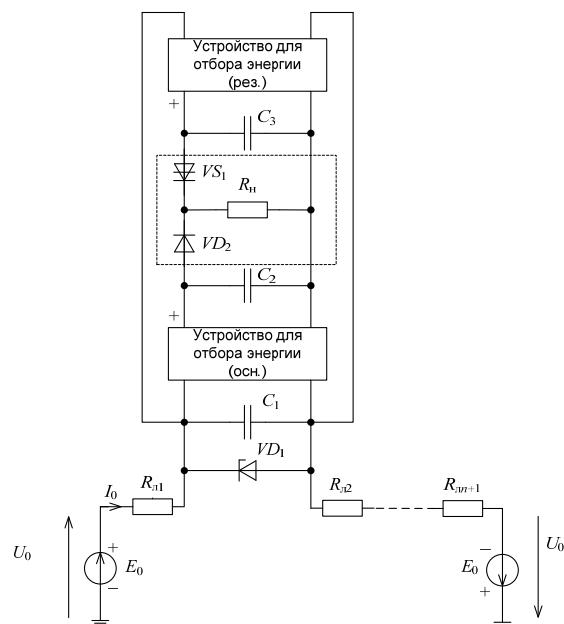


Рис. 2. Параметры стабилитрона  $VD_1$  выбираются исходя из тока в цепи ДП и потребляемой мощности нагрузкой.

В качестве устройства отбора энергии используется понижающий преобразователь постоянного напряжения (ППН), который может быть выполнен как на дискретных элементах, так и посредством понижающего контроллера *DC/DC*.

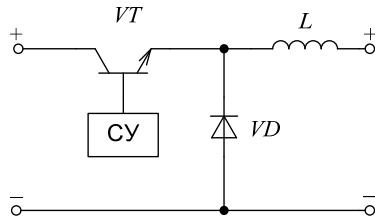


Рис. 3. Функциональная схема преобразователя напряжения

На рисунке 3 показана схема непосредственного ППН, понижающего напряжение, выполненного на дискретных элементах. Принцип действия ППН поясняется следующим: если транзистор *VT* включается в момент  $t_1$ , напряжение источника питания прикладывается к нагрузке (к нагрузке прикладывается импульс напряжения), а когда он выключается в момент  $t_2$ , ток нагрузки протекает за счет энергии, запасённой в индуктивности *L*, и замыкается через диод *VD*. В момент  $t_3$  процессы повторяются. Диод *VD* служит для пропускания тока, проходящего при выключении транзистора *VT* за счет энергии, запасённой в индуктивности *L*. Конденсатор *C<sub>1</sub>* (рис. 2) уменьшает потери в источнике питания, делая потребление энергии от него более постоянным, а конденсаторы *C<sub>2</sub>* и *C<sub>3</sub>* обеспечивают сглаживание импульсов тока на выходе ППН. Для регулирования напряжения на выходе ППН изменяют длительность включенного состояния транзистора посредством схемы управления (*СУ*).

Для дополнительной стабилизации выходного напряжения ППН может применяться шунтирующий регулятор (рис. 4), который будет сбрасывать избыточную энергию, гарантируя тем самым, что потребление энергии нагрузкой не превышает требуемый уровень.

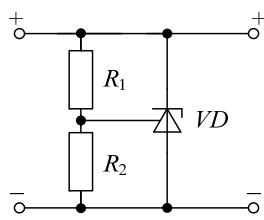


Рис. 4. Шунтирующий регулятор

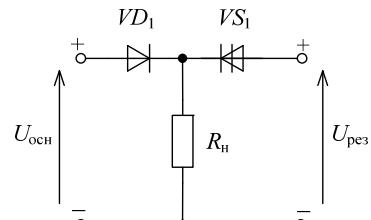


Рис. 5. Переключатель резервного источника напряжения

Переключатель (рис. 5) автоматически включает резервный источник питания *U<sub>рез</sub>* при неисправности (пропадании напряжения) основного источника питания *U<sub>осн</sub>*. Напряжение резервного источника питания *U<sub>рез</sub>* и

тип динистора  $VS_1$  выбираются так, чтобы выполнялось условие  $U_{\text{осн}} > U_{\text{рез}} > (U_{\text{прк}} + I_{\text{прк}}R_h)$ , где  $U_{\text{прк}}$  и  $I_{\text{прк}}$  – напряжение и ток переключения динистора  $VS_i$ . Пока нагрузка  $R_h$  питается от основного источника, динистор закрыт, так как напряжение между его анодом и катодом меньше или равно нулю. При исчезновении напряжения  $U_{\text{осн}}$  (выходе из строя основного источника) к динистору в прямом направлении прикладывается напряжение  $U_{\text{рез}}$ , переключающее прибор в открытую состоянию, и нагрузка  $R_h$  оказывается подключенной к резервному источнику питания. При этом диод  $VD_1$  устраняет связь резервного и основного источников. Если после устранения неисправности вновь включить источник  $U_{\text{осн}}$ , то между анодом и катодом динистора  $VS_1$  появится напряжение, равное  $(U_{\text{осн}} - U_{\text{рез}}) < 0$ , прибор закроется, а источник  $U_{\text{рез}}$  отключится.

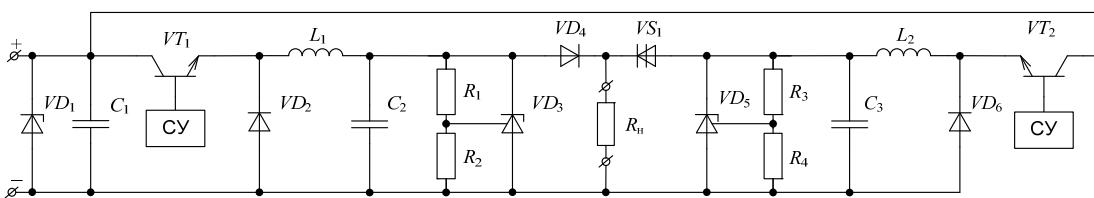


Рис. 6. Принципиальная схема ПДП

На рисунке 6 представлена принципиальная схема ПДП, а на рисунке 7 показана схема дистанционного питания ВОЛС.

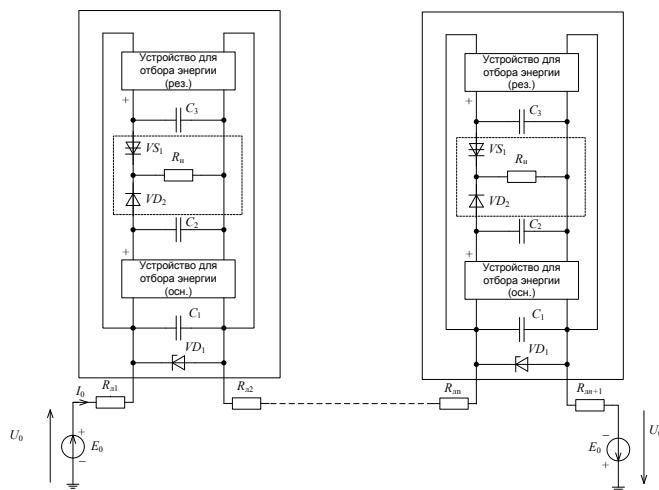


Рис. 7. Схема дистанционного питания ВОЛС

### Список используемых источников

1. Источники вторичного электропитания / С. С. Букреев и др.; под ред. Ю. И. Конева. – М. : Радио и связь, 1983. – 280 с., ил.

*Статья представлена научным руководителем канд. техн. наук, доцентом М. С. Проценко.*

УДК 654.739

**И. С. Размётова (студентка группы МС-22)**  
**В. А. Феоктистов (старший преподаватель кафедры ЭБЖД)**

## **ПРОБЛЕМЫ ПАРНИКОВОГО ЭФФЕКТА И СПОСОБЫ ИХ РЕШЕНИЯ**

Еще в 1827 году французский физик Жозеф Фурье предположил, что атмосфера земли выполняет функцию своего рода стекла в теплице: воздух пропускает солнечное тепло, не давая ему при этом испариться обратно в космос. И он был прав. Этот эффект достигается благодаря некоторым атмосферным газам второстепенного значения, каковыми являются, например, водяные испарения и углекислый газ. Они пропускают видимый и «ближний» инфракрасный свет, излучаемый солнцем, но поглощают «далекое» инфракрасное излучение, имеющее более низкую частоту и образующееся при нагревании земной поверхности солнечными лучами. Если бы этого не происходило, Земля была бы примерно на 30 градусов холоднее, чем сейчас, и жизнь бы на ней практически замерла.

Парниковый эффект – это явление, при котором атмосферные газы удерживают восходящее от Земли тепло в тропосфере, не давая ему подниматься в более высокие слои атмосферы. При этом происходит нагревание, как самой атмосферы, так и земной поверхности [1].

К причинам, вызывающим обострение парникового эффекта в атмосфере, относят: хозяйственную деятельность; сжигание углеродсодержащих видов топлива; выхлопные газы автомобильных двигателей; функционирование теплоэлектростанций; сельское хозяйство, связанное с излишним гниением и переизбытком удобрений, значительным приростом поголовья скота; добычу природных ископаемых; выброс отходов быта и промышленных производств; вырубку лесов.

Основным источником жизни и всех природных процессов на Земле является лучистая энергия Солнца. Энергия солнечной радиации всех длин волн, поступающая на нашу планету в единицу времени на единицу площади, перпендикулярной солнечным лучам, называется солнечной постоянной и составляет  $1,4 \text{ кДж/см}^2$ . Это лишь одна двухмиллиардная доля энергии, излучаемой поверхностью Солнца. Из общего количества солнечной энергии, поступающей на Землю, атмосфера поглощает 20 %. Примерно 34 % энергии, проникающей вглубь атмосферы и доходящей до поверхности Земли, отражается облаками атмосферы, аэрозолями, в ней находящимися, и самой поверхностью Земли. Таким образом, до земной поверхности доходит 46 % солнечной энергии и поглощается ею. В свою очередь поверхность суши и воды излучает длинноволновую инфракрасную (тепловую) радиацию, которая частично уходит в космос, а частично остается

в атмосфере, задерживаясь входящими в ее состав газами и нагревая приземные слои воздуха. Эта изоляция Земли от космического пространства создала благоприятные условия для развития живых организмов.

Атмосфера, содержащая газы, непрозрачна. Такая непрозрачность атмосферы становится хорошим теплоизолятором, что, в свою очередь, приводит к тому, что переизлучение поглощённой солнечной энергии в космическое пространство происходит в верхних холодных слоях атмосферы. В результате эффективная температура Земли как излучателя оказывается более низкой, чем температура её поверхности.

Таким образом, задерживаемое идущее от земной поверхности тепловое излучение (подобно пленке над парником), получило образное название парниковый эффект. Газы, задерживающие тепловое излучение и препятствующие оттоку тепла в космическое пространство, называют парниковыми газами. Благодаря парниковому эффекту среднегодовая температура у поверхности Земли в последнее тысячелетие составляет примерно 15°C. Без парникового эффекта эта температура опустилась бы до -18°C и существование жизни на Земле стало бы невозможным.

Основными химическими веществами, создающими парниковый эффект, являются следующие пять газов: углекислый газ (50 % парникового эффекта); хлорфтоторуглероды (25 %); оксид азота (8 %); озон приземного уровня (7 %); метан (10 %).

Углекислый газ попадает в атмосферу в результате сжигания различных видов топлива. Около 1/3 количества углекислого газа обусловлено выжиганием и сведением лесов, а также процессами опустынивания. Ежегодно содержание углекислого газа в атмосфере Земли увеличивается в среднем на 0,5 %.

Хлорфтоторуглероды вносят около 25 % вклада в создание совокупного парникового эффекта. Они имеют двойную опасность для человека и природы Земли: во-первых, способствуют развитию парникового эффекта; во-вторых, разрушают атмосферный озон.

Метан – один из важных «парниковых» газов. Содержание метана в атмосфере за последние 100 лет удвоилось. Основным источником поступления метана в атмосферу Земли является естественный процесс анаэробного брожения. Нефтяное загрязнение поверхности суши и Мирового океана также вносит свой существенный вклад в увеличение свободного метана в атмосфере нашей планеты.

Оксид азота образуется во многих технологических процессах современного сельскохозяйственного производства, а также в результате сжигания все возрастающих объемов различного топлива.

Главная проблема парникового эффекта – это повышение уровня Мирового океана. При очень значительном потеплении катастрофически начнет сокращаться (примерно в 3–5 раз) площадь горного оледенения, в

Арктике уменьшатся площадь и толщина морских льдов, начнут таять материковые ледники Гренландии и Антарктиды [2].

Поднятие уровня океана, даже незначительное, может иметь весьма негативные экологические и социально – экономические последствия: Будут затоплены приморские равнины, ухудшится водоснабжение прибрежных районов. Если же уровень океана повысится существенно, будут затоплены значительные участки суши и ущерб будут огромными. Подсчитано, что при подъёме уровня мировых вод на 1 м будет затоплено 20 % территории Бангладеш, сельскохозяйственные земли Египта, некоторые крупные города Китая, катастрофическим наводнениям подвергнется Венеция.

Положительные экологические последствия парникового эффекта: потепление климата, скорее всего, благоприятно отразится на растительности, в частности на лесных экосистемах и сельском хозяйстве; повышение концентрации CO<sub>2</sub> в атмосфере может увеличить интенсивность фотосинтеза и, значит, способствовать росту и развитию растений; увеличение концентрации диоксида углерода в атмосфере может оказать благоприятное воздействие на урожайность многих сельскохозяйственных культур; глобальное потепление климата может привести к изменению структуры и местоположения биомов Земли.

Так как предполагаемое потепление климата, вызванное человеческой деятельностью, на 50 % происходит в результате потребления энергии, напрашивается вывод о том, что для того, чтобы предотвратить кризис, надо изменить практику этого потребления. По мнению Агентства по охране окружающей среды США, мировое сообщество должно предпринять серьезные меры. Если опасения, связанные с потеплением климата, оправдаются, то плата за бездействие будет намного выше, чем затраты на предотвращение кризиса.

По мнению экологов, наиболее действенными будут такие меры, как повышение эффективности энергопользования и переход к альтернативным видам топлива.

В 1980 году более 100 миллионов тонн CO<sub>2</sub> было выброшено в атмосферу в восточной части Северной Америки, Европе, западной части СССР и крупных городах Японии. Выбросы CO<sub>2</sub> развитых стран в 1985 году составили 74 % от общего объема, а доля развивающихся стран составила 24 %. Ученые предполагают, что к 2025 году доля развивающихся стран в производстве углекислого газа возрастет до 44 %. В последние годы Россия и страны бывшего СССР значительно увеличили выбросы в атмосферу CO<sub>2</sub> и других тепличных газов. Это, прежде всего, связано с переменами, происходящими в этих странах, и возрастанием уровня производства.

В декабре 1997 года на встрече в Киото (Япония), посвященной глобальному изменению климата, делегатами из более чем ста шестидесяти

стран была принята конвенция, обязывающая развитые страны сократить выбросы CO<sub>2</sub>. [2].

Киотский протокол обязывал тридцать восемь индустриально развитых стран сократить к 2008–2012 годам выбросы CO<sub>2</sub> на 5 % от уровня 1990 года: Европейский союз должен сократить выбросы CO<sub>2</sub> и других тепличных газов на 8 %, США – на 7 %, Япония – на 6 %.

Протокол предусматривал систему квот на выбросы тепличных газов. Суть его заключается в том, что каждая из стран (пока это относится только к тридцати восьми странам, которые взяли на себя обязательства сократить выбросы), получает разрешение на выброс определенного количества тепличных газов. При этом предполагается, что какие-то страны или компании превысят квоту выбросов. В таких случаях эти страны или компании смогут купить право на дополнительные выбросы у тех стран или компаний, выбросы которых меньше выделенной квоты. Таким образом, предполагалось, что сокращение выбросов тепличных газов в последующие 15 лет на 5 % - будет выполнено.

В последние годы, переговоры по вопросу сокращения выбросов тепличных газов идут очень сложно. Прежде всего, конфликт существует на уровне официальных лиц и бизнеса с одной стороны и неправительственного сектора – с другой. Неправительственные экологические организации считают, что достигнутое соглашение не решает проблемы, так как пятипроцентное сокращение выбросов тепличных газов недостаточно для того, чтобы остановить потепление, и призывают сократить выбросы как минимум на 60 %. Кроме того, конфликт существует и на уровне государств. Такие развивающиеся страны, как Индия и Китай, вносящие значительный вклад в загрязнение атмосферы тепличными газами, присутствовали на встрече в Киото, но не подписали соглашение. Развивающиеся страны с настороженностью воспринимают экологические инициативы индустриальных государств. Аргументы просты:

- а) основное загрязнение тепличными газами осуществляют развитые страны;
- б) ужесточение контроля на руку индустриальным странам, так как это будет сдерживать экономическое развитие развивающихся стран.

В любом случае проблема глобального потепления климата – яркий пример того, какие механизмы, подчас, включены в решение экологической проблемы. Такие компоненты, как научная неопределенность, экономика и политика нередко играют в этом процессе ключевую роль.

Выход из сложившейся ситуации один: изыскать новый вид топлива, либо в корне поменять технологию использования существующих разновидностей топливных ресурсов. Уголь и нефть при сгорании выделяют на 60 % больше диоксида углерода, активного парникового газа, чем любое другое топливо для производства единицы энергии. Ученые и экологи предлагают меры, чтобы убежать от угрозы развития парникового эффек-

та: сократить потребление ископаемого топлива, особенно угля, нефти и природного газа; использовать специальные фильтры и катализаторы для удаления диоксида углерода из всех выбросов в атмосферу; повысить энергетический КПД теплоэлектростанций за счет использования скрытых экологичных резервов; увеличить использование альтернативных источников энергии; прекратить вырубку зеленых насаждений и наладить целенаправленное озеленение; остановить всеобщее загрязнение планеты.

Сейчас идет активное обсуждение таких мер снижения антропогенного воздействия, как регулярное удаление углекислого газа из атмосферы, путем использования высокотехнологичных устройств, сжижать и нагнетать его в воды Мирового океана, тем самым приблизиться к естественной циркуляции. Пути решения проблемы есть, главное, взяться за это всем вместе, населению, правительству и подрастающему поколению, и провести огромную, но такую полезную, работу по очищению матушки-Земли. Пора прекратить потребительское отношение и начать вкладывать силы и время в свое будущее, светлую жизнь следующих поколений, пришло время отдавать природе то, что мы у нее регулярно забираем. Нет, сомнения, что гениальное и предприимчивое человечество справится и с этой, очень сложной и ответственной, задачей!

Важно понимать, что парниковый эффект на Земле был всегда. Без парникового эффекта, обусловленного наличием углекислого газа в атмосфере, океаны давно бы замерзли, и высшие формы жизни не появились бы. В настоящее время научные дебаты о парниковом эффекте идут по вопросу глобального потепления: не слишком ли мы, люди, нарушаляем энергетический баланс планеты в результате сжигания ископаемых видов топлива и прочей хозяйственной деятельности, добавляя при этом излишнее количество углекислого газа в атмосферу? Сегодня ученые сходятся во мнении, что мы ответственны за повышение естественного парникового эффекта на несколько градусов. Деятельность человека столь грандиозна по размаху, что уже приобрела глобальный природообразующий масштаб. До сих пор мы по преимуществу искали, как можно больше взять у природы. И поиск в этом направлении будет продолжаться. Но наступает пора столь же целеустремленно поработать и над тем, как отдать природе то, что мы у нее забираем. Нет сомнения, что гений человечества способен решить и эту грандиозную задачу.

#### **Список используемых источников**

1. Экология и экологическая безопасность : учебн. пособие для вузов / Ю. Л. Хотунцев. – М. : Академия, 2004. – 480 с.
2. Экология и безопасность жизнедеятельности : учебн. пособие для вузов / Под. ред. Л. А. Муравья. – М. : ЮНИТИ-ДАНА, 2000. – 447 с.

УДК 621.39

**Д. С. Самаркин (старший преподаватель УВЦ ИВО СПбГУТ)**  
**Н. Г. Строева (студентка группы МТВ-93 СПбГУТ)**

## **АНАЛИЗ РЕАЛИЗАЦИИ ОПТИЧЕСКИХ КОММУТАТОРОВ НА ОСНОВЕ ЭФФЕКТА ПОККЕЛЬСА**

Коммутатором в обобщенном смысле обычно называют устройство, позволяющее передать мгновенно и с минимальными искажениями исходный сигнал, поступивший на один из нескольких входов, на один из нескольких выходов в соответствии с заданным алгоритмом переключения. Соответственно под оптическими коммутаторами подразумеваются коммутаторы, осуществляющие коммутацию сигналов, представленных в виде оптического излучения. Оптическая коммутация и маршрутизация могут быть реализованы на основе различных технологий:

- механические оптические коммутаторы;
- электрооптические;
- термооптические;
- оптоэлектронные с полупроводниковыми усилителями света;
- интегральные активные волноводные;
- на многослойных световодных жидкокристаллических матрицах;
- на интегральных схемах с набором матриц оптоэлектронных вентилей, связанных оптическим лучом;
- на основе фотонных кристаллов.

Указанные технологии позволяют создавать большое разнообразие коммутаторов. Определенные конфигурации коммутаторов могут обеспечить оптическую маршрутизацию в оптическом узле.

Оптические коммутаторы выполняют в АОСП ту же функцию, что и обычные электронные коммутаторы в традиционных сетях, а именно обеспечивают коммутацию каналов или коммутацию пакетов. Наряду с простейшим коммутатором 2x2 в настоящее время начали поставляться коммутаторы с числом портов 4x4, 8x8, 16x16.

Оптическая коммутация принципиально отличается от механической коммутации потоков. При механической коммутации время срабатывания составляет десятки миллисекунд (в среднем от 20 до 50 мс). При оптической коммутации время срабатывания определяется переходными процессами в электрической цепи управления оптического коммутатора и обычно на несколько порядков меньше. Оптический коммутатор – это один из наиболее важных элементов полностью оптической сети, без которого невозможно строить масштабируемые архитектуры. Большинство основных конструкций оптических коммутаторов должно иметь, по крайней мере, два выхода. Основными параметрами коммутатора являются:

- 1) скорость переключения;
- 2) управляющее напряжение;
- 3) перекрестные помехи;
- 4) вносимые помехи.

В иерархии скоростей переключения в оптических сетях различают четыре уровня.

В настоящее время используются разнообразные типы оптических коммутаторов:

- направленные ответвители;
- мостовой балансовый интерферометр;
- коммутатор на скрещивающихся волноводах.

В основе работы оптического коммутатора используется линейный электрооптический эффект Поккельса, который заключается в изменении показателя преломления материала пропорционально напряжённости приложенного электрического поля. Эффект Поккельса может наблюдаться только в кристаллах, не обладающих центром симметрии.

Устройства мультиплексирования/демультиплексирования WDM, волновые фильтры и оптические коммутаторы имеют одну общую деталь – в основе их работы лежат в той или иной степени интерференционные эффекты. Основные принципы работы легче рассмотреть на простейшем четырехполюснике – разветвителе-коммутаторе [1]. Схема сплавного разветвителя X-типа показана на рисунке 1.

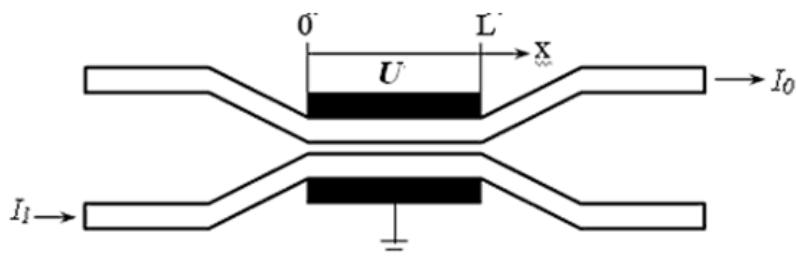


Рис. 1. Направленный ответвитель-переключатель.

Излучение, введенное в один волновод, проникает в другой за счет перекрытия реактивных полей двух волноводов. Погонный коэффициент связи  $k$  зависит от параметров волновода, длины волны  $\lambda$  и ширины зазора  $g$  между волноводами. Разветвитель характеризуется разностью постоянных распространения двух волноводов  $\Delta B = 2\pi(N_1 - N_2)/\lambda$ , (где  $N$  - эффективные показатели преломления) и длиной  $L$ . Прикладывая электрическое напряжение к электродам, расположенным по бокам или сверху и снизу волноводов, образующих так называемую ячейку Поккельса, можно регулировать фазовую расстройку за счет линейного электрооптического эффекта [2].

Далее следует решить систему двух комплексных дифференциальных уравнений, описывающих взаимосвязанные моды:

$$iR' = -\delta R + kS, \quad (1)$$

$$iS' = \delta k + kR, \quad (2)$$

где  $\delta = \Delta B/2$ ,  $R$  и  $S$  - комплексные амплитуды волн в двух волноводах, штрих - означает производную по  $x$ . В частном случае, когда только в один волновод вводится единичная мощность, т. е.  $R(0) = 1$ ,  $S(0) = 0$ , можно, решая уравнения (1) и (2), определить мощность, переданную в другой волновод, т. е. величину  $|S(L)|^2$ , которая также носит название эффективность передачи:

$$\eta = 1/p \times \sin^2 kL p^{1/2},$$

$$p = 1 + (\delta/k)^2,$$

В случае полностью симметричной конструкции на основе двух одинаковых волноводов (рис. 1) в отсутствии напряжения ( $\delta = 0$ ) мы имеем  $\eta = \sin^2 kL$ . Полная передача мощности происходит при  $kL = (2n + 1)\pi/2$ , где  $n$  – целое число, и минимальная длина при этом будет определяться выражением  $L = \pi/2k$ .

В силу полной линейности и однородности системы уравнений (1) и (2), любая линейная комбинация двух решений также будет решением. Добавляя свойство симметрии, получаем, что при условиях ( $\delta = 0$  и  $L = \pi/2k$ ), полная (кроссовая) передача мощности будет иметь место для обоих сигналов, входящих в каждый волновод - сигналы должны быть одной и той же длины волны, а именно той, для которой рассчитывался коэффициент передачи  $k$ , и, соответственно, длина участка взаимодействия  $L$ . Заметим, что при  $\delta \neq 0$  полная передача мощности невозможна ни при каких значениях  $kL$ .

Параллельное прохождение ( $\eta = 0$ ) можно обеспечить за счет подачи электрического потенциала, вводя фазовую расстройку  $\Delta\beta$ . Легко определить величину необходимой расстройки  $\Delta\beta = 3^{1/2}\pi/L$ . В отсутствии напряжения эффективность связи между волноводами коммутатора составляет 100 % (оптические сигналы полностью кроссируются - входят в один волновод, выходят из другого), а при подаче необходимого напряжения эффективность связи уменьшается до 0. Поскольку уравнения (1) и (2) линейны по обоим аргументам и однородны, то суперпозиция любых двух, являющихся по отдельности решениями, также будет решением. Таким образом, разветвитель-коммутатор 2x2 осуществляет коммутацию без блокировки.

Еще одна реализация разветвителя-коммутатора 2x2, состоящая из двух последовательных X-разветвителей, представлена на рисунке 2. Оптические сигналы после прохождения по разным плечам интерферируют во втором разветвителе. Путем изменения напряжения на электродах, охватывающих одно из плеч, можно регулировать разность фаз между

приходящими во второй разветвитель сигналами и тем самым влиять на характер интерференции.

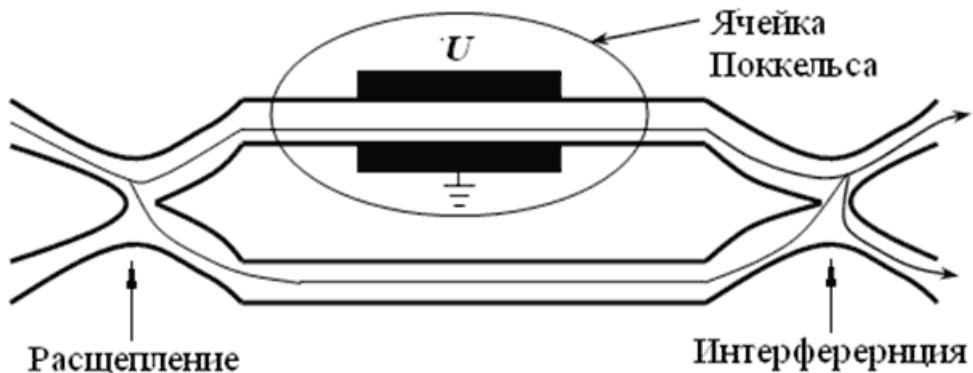


Рис. 2. Двухплечевой оптический разветвитель-коммутатор.

Наряду с электрооптическим эффектом, для осуществления коммутации также широко используется акустооптический эффект.

На основе простых оптических разветвителей-коммутаторов  $2 \times 2$ -элементов – строятся более сложные оптические коммутаторы  $n \times n$ . Поскольку составные элементы  $2 \times 2$  принимают на входные полюсы сигналы одной и той же длины волны, то и весь коммутатор  $n \times n$  изготавливается для работы с поступающими оптическими сигналами одной и той же заданной длиной волны. Другими важными характеристиками коммутатора, кроме рабочей длины, являются максимальные вносимые потери и попечерные помехи на выходных полюсах.

Матричный строго неблокирующий коммутатор  $4 \times 4$  (рис. 3) с шестнадцатью элементами представляет частный случай более общего матричного коммутатора.

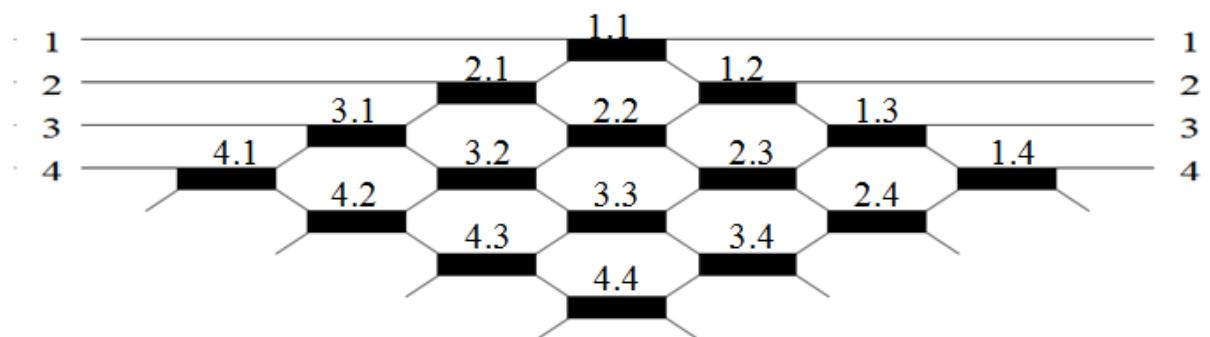


Рис. 3. Матричный коммутатор  $4 \times 4$ , 16 элементов

Число элементов между разными парами входных и выходных полюсов может меняться в пределах от минимального (элемент 1.1) до максимального 7 (элементы 4.1, 4.2, 4.3, 4.4, 3.4, 2.4, 1.4). Если учесть, что по прохождению каждого элемента теряется доля мощности полезного сигнала, а также вносится шум, то в заведомо неравном положении оказываются

различные пути, с малым и большим числом промежуточных элементов. Соединение между любым входным и выходным полюсом всегда можно установить независимо от того, как с коммутированы оставшиеся пары полюсов, и не влияя на их соединение (свойство строгой неблокируемости коммутатора) [3]. Путь соединения однозначно определяется входным и выходным полюсами.

#### **Список используемых источников**

1. **Оптическое** мультиплексирование с разделением по длине волны [Электронный ресурс] / Н. Слепов // Сети. – 1999. – № 4. – Режим доступа: <http://www.osp.ru/nets/1999/04/144015/> (Дата обращения 14.05.2014).
2. **Волоконно-оптические сети** / Р. Р. Убайдуллаев. – М. : Эко-Трендз, 2001.
3. **Оптические усилители** / Н. Слепов // Connect! Мир связи. – 1999. – № 8.

**УДК 629.124.74; 621.315.285**

**А. И. Симоненко (студент группы ИКТС-31 СПбГУТ)**

**И. Г. Стакеев (доцент УВЦ ИВО СПбГУТ)**

**А. А. Яхункина (студентка группы ИКТС-31 СПбГУТ)**

## **ПОСТРОЕНИЕ ПОДВОДНОЙ ТРАНСОКЕАНСКОЙ ЛИНИИ СВЯЗИ РОССИИ**

Россия - страна океанских и речных систем. Ее омывают 2 океана (Тихий и Серный-Ледовитый), а так же из тридцать четырёх крупнейших рек мира 6 полностью протекают по территории России (Лена, Енисей, Обь, Волга, Оленек, Колыма). Такие территориальные ресурсы необходимо учитывать и выгодно использовать в жизни людей. Соединение городов, которые находятся на берегах рек целесообразно соединить в одну информационную сеть с помощью прокладки оптического кабеля по их дну. Сочетание технологий по прокладке трансокеанских и речных волоконно-оптических линий связи (ВОЛС) дает мощную первичную сеть связи. Это будет самая большая мультисервисная сеть, которая позволит в значительной мере увеличить степень автоматизации в малонаселенных районах России [1].

Ни для кого не секрет, что для выполнения данного глобального проекта необходимо решить ряд проблем.

Одной из них является прокладка кабеля по морскому дну. Огромные глубины, высочайшее давление, малая доступность, сложный подводный рельеф, налагают особые требования на конструкцию кабеля, оптических усилителей, соединительных муфт, разветвителей и прочего оборудования,

но, не смотря на эти недостатки и неудобства, оптические кабели занимают лидирующие позиции. Эти кабели обладают особой прочностью, обеспечивают бесперебойную работу оборудования и самое важное – срок службы составляет не менее 25 лет.

Сегодня, можно сказать, что воплощение идеи построения подводной сети связи на территории РФ уже началась.

Как известно, кабельные линии связи всех операторов России, проложены по югу страны и являются на данный момент единственной линией связи, которая обеспечивает связь абонентов всей страны (рис. 1).



Рис. 1. Магистральная линия связи «РОСТЕЛЕКОМ»

Для того чтобы разгрузить данную линию, предлагается строительство современной, высоко эффективной подводной трансокеанской линии, которая будет проходить по дну Северного Ледовитого и Тихого океанов, связывая между собой города северной территории России (рис. 2).



Рис. 2. Трансокеанская линия связи и линии связи

Данная линия связи будет проходить по дну океанов, а вернее по их морям (Баренцево, Карское, Лаптевых и т. д.), что обеспечит доведение сигналов электросвязи в области северных и восточных районов. Основные из них являются: Архангельская область; Новая Земля; Тюменская область; Красноярский край; Северная Земля; Республика Саха (Якутия); Чукотский автономный округ; Камчатский край; Хабаровский край; Сахалинская область; Курильские острова и Приморский край.

Для прокладки по дну океанов и морей применяется специальный кабель повышенной прочности и эластичности ([рис. 3](#)). Высокое качество кабеля обеспечивает большую длительность его использования под водой, поэтому он не требует частого ремонта или замены. Тем самым практически исключаются или сводятся к минимуму расходы по его поддержанию в эксплуатационном состоянии, что экономит значительные средства и делает подводную связь экономически эффективной. Однако этот вид связи не так уж неуязвим: для него представляют серьезную опасность мутевые потоки на шельфе, штормы в прибрежной зоне, тектонические процессы и донное траение.



Рис. 3. Оптоволоконный подводный кабель

Кабели ВОЛС для прокладки по дну, как правило, состоят из оптического сердечника, токоведущей жилы и внешних защитных покровов. Кабели для бесрепитерных оптоволоконных линий имеют такую же структуру, но у них токоведущая жила отсутствует.

Особые проблемы прокладки ВОЛС через водные препятствия под водой связаны с ремонтом морских линий связи. Так как, находясь, долгое время на морском дне, кабель становится практически невидимым. Кроме того, течения могут отнести оптоволоконный кабель от места его первоначальной прокладки (даже на многие километры), а рельеф дна сложен и разнообразен [2, 3].

Для построения подводной трансокеанской линии связи необходима специальная техника, ею является крупнейший корабль в мире «*CS Cable Innovator*» специально разработанный для прокладки волоконно-оптического кабеля. Он имеет размеры 145 метров в длину и 24 метра в ширину, способен перевозить до 8500 тонн волоконно-оптического кабеля.

Из выше сказанного можно сделать следующие выводы:

1. Прокладка трансокеанской линии связи по северу РФ, которая связывает Мурманск и Владивосток и уже проложенная линия связи по югу страны будут основой для высокозащищенной сети связи на всей территории страны.

2. Построенная, перспективная сеть связи, в основном проложенная в водных бассейнах страны в первую очередь необходима для нужд государственного управления, для организации правительственной связи, для нужд обороны и безопасности государства.

3. Несмотря на большие трудности и недостатки при прокладке и организации связи на северных территориях страны, предлагаемая нами система связи наименьшим образом подвержена средствам информационной разведки, террористическим актам, имеет высокую помехозащищенность и безопасность.

### Список используемых источников

1. **Волоконно**-оптические линии связи : практ. руководство / О. Родина. – М. : Горячая Линия – Телеком, 2009. – 404 с.
2. **Волоконно**-оптические линии связи: учебн. пособие / В. Виноградов, В. Котов, В. Нуприк. – М. : Желдориздат, 2002. – 278 с.
3. **Подводные** кабельные системы связи / С. Беда, А. Катанович. – СПб. : Судостроение, 2009. – 240 с.

## АННОТАЦИИ

### ПЛЕНАРНЫЕ ДОКЛАДЫ

**Распределенная система генерации компьютерной музыки** [Электронный ресурс] / Г. Г. Рогозинский // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб.: СПбГУТ, 2014. – С. 5–9.

*Синергия компьютерной музыки и инфотелекоммуникационных систем производит на свет новые формы искусства, которые открывают новые грани в области применения парадигмы Интернета вещей, пост-NGN сетей и современного информационного пространства.*

**Ключевые слова:** компьютерная музыка, распределенные системы, алгоритмическая композиция.

**Теоретическое и практическое моделирование работы осветительных систем с ик источником излучения** [Электронный ресурс] / А. В. Бахолдин, В. С. Шевкунов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 9–13.

*Работа посвящена исследованию инфракрасных источников излучения и распределению облученности от них при использовании различных оптических систем. Исследование выполнялось в рамках работы по усовершенствованию конструкции игрового оборудования, использующегося в коммерческих целях для имитации боя в полевых условиях. Моделирования проводилось с помощью программы Zemax.*

**Ключевые слова:** LED, инфракрасные источники излучения, Zemax, Лазертаг, распределение облученности, проектирование оптических систем, учебный лабораторный макет.

### РАДИОТЕХНОЛОГИИ СВЯЗИ

**Использование понятий QoS и QoE в оценке IEEE 802.16** / Д. К. Артур // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 14–17.

*Часто в предложении услуг связи термины QoS и QoE используются для описания качества сети и пользовательский опыт, соответственно. Но какие из этих парамет-*

ров должен определять каждый из этих терминов. В этой статье автор объясняет необходимость использования QoE в определении QoS о сети, а не в обратном.

**Ключевые слова:** QoS, QoE, WiMAX и потока обслуживания.

**Проектирование высоконагруженной беспроводной локальной сети Wi-Fi** [Электронный ресурс] / А. С. Лежепёков // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 17–21.

*В данной исследовательской работе рассмотрены проблемы организации высоконагруженной беспроводной Wi-Fi сети, продемонстрированы и визуализированы с помощью вспомогательного ПО выявленные недостатки методов, известных на сегодняшний день, и предложен способ решения выявленной проблемы.*

**Ключевые слова:** Wi-Fi, беспроводные локальные сети.

**Использование фоновой музыки в системе высшего образования** [Электронный ресурс] / Д. А. Парицкая // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 22–26.

*В работе рассмотрены достоинства использования фоновой музыки в высшем образовании. В данной работе сделана попытка проанализировать результаты исследований, выполненных в этой области, и сформулировать выводы о потенциальной пользе использования фоновой музыке в системе высшего образования. Показаны факторы, влияющие на выбор фоновой музыки. Обозначены направления будущей работы, которые привели бы к доказательствам изложенных в работе предположений.*

**Ключевые слова:** фоновая музыка в высшем образовании, польза фоновой музыки.

## ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

**Противодействие атакам методом переполнения буфера** [Электронный ресурс] / А. Д. Алексеев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 27–31.

*В работе рассматриваются основные виды атак с использованием переполнения буфера и причины их реализации. Рассмотрены существующие на сегодняшний день методы противодействия данным атакам, и сделаны выводы об их эффективности.*

**Ключевые слова:** переполнение буфера, стек, анализ исходного кода, DEP, ASLR.

**Актуальность биосистемных технологий и первичный анализ методов защиты информации в биосистемах** [Электронный ресурс] / В. И. Андрианов, Л. А. Виткова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 31–36.

*В работе подчеркивается актуальность использования биосистемных аналогий в процессе разработки и моделирования средств защиты информации. Анализируются методы защиты информации в биосистемах и в естественной иммунной системе, в частности.*

**Ключевые слова:** телекоммуникационные сети, биосистемные технологии, ddos-атака, киберпреступления, биосфера, естественная иммунная система, искусственная иммунная система, ДНК, антиген, клетка, ген.

**Оценка и сравнение существующих концепций построения систем управления телекоммуникационными сетями** [Электронный ресурс] / Э. В. Бенета // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 36–40.

*В работе анализируются распространенные концепции построения систем управления телекоммуникационными сетями. Показаны преимущества и недостатки различных подходов. Данна общая оценка существующих концепций на основе разработанной сравнительной таблицы.*

**Ключевые слова:** система управления, телекоммуникационная сеть связи, СУ ТКС, ITIL, TMN.

**Безопасность беспроводных mesh-сетей. Принцип действия алгоритма CORIDS** [Электронный ресурс] / В. Ю. Бондарев, А. В. Лейкин // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 40–47.

*В данной работе рассматривается принцип действия алгоритма CORIDS, направленного на обеспечение безопасной работы mesh-сетей. В частности, приведены фазы алгоритма, использующиеся параметры и основные формулы для вычисления используемых показателей. Проведен краткий сравнительный анализ со схожим по принципу действия предшественником CORIDS, алгоритмом MDA.*

**Ключевые слова:** алгоритм CORIDS, mesh-сеть, межмашинное взаимодействие, М2М, кластер, атака, вторжение, злонамеренный узел, головной узел кластера, показатель доверия, эффективность.

**Симуляция работы алгоритма маршрутизации AODV при помощи Network Simulator** [Электронный ресурс] / К. С. Варельджян, В. В. Фицов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб.: СПбГУТ, 2014. – С. 47–52.

*Исследовательские работы по протоколам маршрутизации ad hoc сетей являются очень важными, в связи с расширением области применения таких сетей. В этой статье была смоделирована ad hoc сеть и проведена симуляция работы протокола маршрутизации AODV. В качестве инструмента моделирования использовался сетевой симулятор NS-3.*

**Ключевые слова:** Ad hoc, маршрутизация, AODV, симуляция, Network Simulator.

**Анализ способов самоорганизации в роевых структурах** [Электронный ресурс] / Е. В. Васильев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 52–57.

*В работе разбираются и анализируются механизмы и алгоритмы самоорганизации в сетях, образующих роевую структуру. Приведены области применения алгоритмов в мультиагентных системах. Представлено сравнение механизмов самоорганизации по способу и типу взаимодействия элементов в рое.*

**Ключевые слова:** самоорганизация, мультиагентная система, рой.

**Обнаружение и измерение степени сходства кода приложений для ОС ANDROID** [Электронный ресурс] / А. А. Галицкий // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 57–60.

*Android – наиболее распространенная на сегодняшний день платформа для мобильных устройств, и вредоносное программное обеспечение (вредоносные программы) неизбежно существует для него. В этой статье исследуются статические методы анализа вредоносного программного обеспечения для приложений ОС Android. Одним из них является обнаружение и измерение степени сходства кода. Показано, как обнаружить вредоносные программы на основе определения расстояния Дамерау-Левенштейна между блоками кода.*

**Ключевые слова:** сходство программного кода, NCD, расстояние Дамерау-Левенштейна, обнаружение вирусов, ОС Android.

**Оценка вероятностно-временных характеристик сигнального трафика в NGN на базе IMS** [Электронный ресурс] / А. А. Гамиль // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 60–65.

*Вопрос оценки характеристик сигнального трафика в подсистеме IMS остается мало исследованным. В статьи сделаны предварительные оценки времени задержки сигнального трафика во всех узлах сети, как важного параметра качества обслуживания. Построена модель оценки времени ожидания в очереди на узлах подсистемы IMS.*

**Ключевые слова:** NGN, IMS, качество обслуживание, регистрация пользователей, задержка.

**Исследование методов отрицаемого шифрования** [Электронный ресурс] / Л. Р. Гарапова, В. И. Коржик // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 65–69.

*В данной статье описаны методы отрицаемого шифрования: алгебраический шифр на основе шифра Вернама; алгебраический шифр, основанный на применении китайской теоремы об остатках, сформулированной для двоичных многочленов.*

**Ключевые слова:** отрицаемое шифрование, принуждающие атаки, шифр Вернама, китайская теорема об остатках.

**Атаки на протоколы маршрутизации ad hoc сетей** [Электронный ресурс] / В. Ю. Гойхман, Т. Ю. Лушникова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 69–73.

*Широкая популярность беспроводных ad hoc сетей делает их привлекательным объектом для различного рода атак злоумышленников. В составе данных, собираемых сетью, возможно присутствие информации, имеющей конфиденциальный или частный характер.*

*Данная работа классифицирует известные атаки, направленные на протоколы маршрутизации беспроводных ad hoc сетей.*

**Ключевые слова:** ad hoc сети, атаки, безопасность, протоколы маршрутизации.

**Анализ использования при DPI сигнатур потоков сервисов передачи сообщений** [Электронный ресурс] / К. Э. Есалов, Е. В. Золотарев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 73–78.

*В работе освещается технология DPI, ее применение, возможность обнаружения сигнатур различных приложений. Рассмотрены некоторые из полученных при статистическом анализе сигнтуры. Показана идея будущего учебного лабораторного макета, позволяющего попробовать управление системой DPI и дающего возможность применять различные политики к потокам данных различных приложений.*

**Ключевые слова:** DPI, сигнтура, мультимедийные приложения, сервисы, услуги, учебный лабораторный макет.

**Реализация алгоритмов обработки информации и имитационной модели канала передачи данных для беспроводных сетей стандарта 802.11** [Электронный ресурс] / Е. В. Ефимова, И. А. Небаев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 78–83.

*В работе представлена реализация компьютерной имитационной модели канала передачи данных для беспроводных сетей стандарта 802.11. Проведен анализ основных методов и алгоритмов обработки и передачи информации в семействе стандартов IEEE 802.11. Представленные данные и продемонстрированные результаты исполнения модели, могут быть применимы в различных научно-исследовательских и проектных работах данного направления.*

**Ключевые слова:** беспроводные сети, алгоритмы обработки информации, сверточное кодирование, имитационное моделирования.

**Методика выбора эффективной системы видеонаблюдения для идентификации лица** [Электронный ресурс] / Ю. С. Ефремова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 84–89.

*В работе решается задача эффективной записи высококачественного изображения лица человека в зоне видеонаблюдения, которое может быть использовано для доказательства идентичности. Рассмотрен алгоритм Виолы-Джонса, основанный на интегральном представлении, для обнаружения характерных черт лица человека в режиме реального времени.*

**Ключевые слова:** система видеонаблюдения, идентификация, метод Виолы-Джонса, интегральное представление, примитивы Хаара.

**Исследование методов защиты от ошибок в современных широкополосных каналах радиосвязи** [Электронный ресурс] / Д. А. Жукова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 89–94.

*В работе анализируются методы защиты от ошибок в современных широкополосных каналах радиосвязи. Рассматривается процедура каскадного кодирования и декодирования. Приведена структурная схема декодера внутреннего кода. Проведен ряд исследований по обнаружению искаженных блоков и анализ возможности исправления полученных стираний в каналах связи с сильным и слабым группированием ошибок.*

**Ключевые слова:** WiMAX, IEEE 802.16, каскадное кодирование, РС-код, код Хемминга, группирование ошибок, исправление стираний.

**Проект OpenMVL. Компонентные модели и решение больших разреженных систем** [Электронный ресурс] / А. А. Исаков // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 94–98.

*В работе впервые предлагается применение алгоритма Тарьяна применительно к автоматизации процесса вычисления непрерывного потока задач, возникающих в пакетах компьютерного моделирования при моделировании поведения гибридных многокомпонентных систем. Показаны предпосылки для применения данного подхода, связанные со спецификой решаемой задачи. Предложена предварительная схема организации вычислений, которая будет применена в пакете моделирования OpenMVLShell с открытым исходным текстом. Обозначены планируемые результаты, которые будут получены по итогам выполнения сравнительного анализа предлагаемой схемы вычислений и традиционного подхода (для сравнения выбран численный метод MA28), применяемого современными пакетами компьютерного моделирования.*

**Ключевые слова:** визуальные среды моделирования, открытые пакеты, компонентное моделирование, гибридный подход, сложные динамические системы, численные методы.

**Модель междоменного взаимодействия в SDN и с использованием двух контроллеров** [Электронный ресурс] / Ле Чан Дык // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 99–104.

*В работе предлагается новый подход для решения задачи междоменного взаимодействия за счет расширения функционала SDN-контроллеров. В каждом домене предлагается использовать два контроллера: один традиционно отвечает за работу домена, другой выполняет функции взаимодействия с другими доменами. Этот подход позволяет контроллерам избавляться от перегрузки (проблемы «слонов и мышей» и «узкого горлышка»), так как в этом случае один контроллер может поддерживать большее количество коммутаторов в одном домене. Также, один из контроллеров может играть роль резервного для другого, что позволяет реализовывать резервирование ресурсов по схеме 1+1.*

**Ключевые слова:** SDN-программно конфигурируемые сети, SDN-контроллеры, междоменное взаимодействие.

**Контрольно-измерительные материалы для подготовки к олимпиаде по спортивному программированию** [Электронный ресурс] / К. С. Орлов, А. А. Шолохов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 104–107.

*Спортивное программирование приобретает все большую популярность в наши дни. Многие крупные компании, такие как Google, IBM или Yandex, ищут новых сотрудников из числа победителей олимпиад.*

*В статье описываются правила проведения олимпиад для студентов ВУЗов, методические указания для подготовки, составленные на основе личного опыта, а также пример задачи с разбором.*

**Ключевые слова:** спортивное программирование, олимпиадное программирование, правила олимпиад.

**Математическая и программная модель обработки изображений микросрезов кожного покрова** [Электронный ресурс] / А. Г. Радченко // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 108–111.

*Статья посвящена особенностям обработке изображений близко расположенных объектов. Обработка основывается на полевой модели с использованием усреднения и высокочастотных фильтров. Разработана концепция, а также построена математическая модель и алгоритм, поддерживающий эту концепцию.*

**Ключевые слова:** полевая модель, математическая модель, цифровая обработка изображений.

**Разработка предложения по выбору изображений для графического паролирования** [Электронный ресурс] / В. В. Скачкова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 112–116.

*Защита информации от несанкционированного доступа является актуальной проблемой в связи с широким распространением информационных технологий. Системы аутентификации на основе графического пароля стали альтернативой числено-буквенным паролям.*

**Ключевые слова:** аутентификация, системы аутентификации, графический пароль.

**Математическая и программная модель построения поля особых точек на основе уравнения Ляме** [Электронный ресурс] / Л. В. Фролова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 117–125.

*Статья посвящена обработке графической информации на основе её представления в виде векторного поля. Построена математическая модель и разработан алгоритм обработки. Представлены полученные результаты обработки тестовых изображений. основе уравнения и алгоритм, поддерживающий эту концепцию.*

**Ключевые слова:** математическая физика, векторное уравнение, функция Грина, матрица Грина, обработка изображений, особая точка, источники, пиксель.

**Теоретическое исследование кабельных цепей с биметаллическими проводниками** [Электронный ресурс] / П. А. Чаймарданов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 125–129.

*В кабельной промышленности используются различные типы биметаллических проводников. Наиболее широко применяются проводники с сердечником из алюминия или стали и оболочкой из меди. В настоящее время на рынке представлены LAN кабели категории 5е с биметаллическими проводниками. Относительно качества этих изделий у специалистов нет единого мнения. Поэтому актуальной задачей является анализ параметров этих кабелей, который позволит проверять их соответствие международному стандарту. В данной работе получены выражения для расчета распределения электромагнитного поля в биметаллическом проводнике и его полного сопротивления с учетом поверхностного эффекта и эффекта близости.*

**Ключевые слова:** биметаллический проводник, LAN кабель категории 5е, поверхностный эффект, распределение электромагнитного поля, полное сопротивление проводника, эффект близости.

**Разработка программного обеспечения для проверки решений задач по программированию** [Электронный ресурс] / И. Р. Шалин // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 130–132.

*Данная статья предназначена для ознакомления с системой тестирования, рассчитанной для проверки программного кода студентов. Описывается реализация разработки собственного программного обеспечения, которое включает в себя синтаксический анализ исходных текстов программы, стиль написания программы, корректность выполнения задачи и предостережение от потенциально возможных ошибок. Преимущества создания автоматизированной системы проверки однозначны, и для ее осуществления были проведен анализ уже существующего продукта с целью его улучшения, а также выбора основы клиент-серверного приложения. Приведены возникшие трудности, а также путь их решения.*

**Ключевые слова:** автоматизация тестирования, программный код, Node.js, веб-приложение.

**Рациональный агент, решающий задачу поиска в терминах заданных местоположений и переходам по связям между ними** [Электронный ресурс] / Д. А. Шаньгина // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 133–137.

*В агентно-ориентированном подходе в области искусственного интеллекта используются агенты, воспринимающие среду с помощью датчиков и принимающие решения в зависимости от полученной информации. В данной статье приводятся сведения об архитектуре такого агента, а также предложен и промоделирован алгоритм поиска пути для таких агентов.*

**Ключевые слова:** рациональный агент, пространство состояний, искусственный интеллект, функция определения преемника, функция определения пути.

## ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

**Технологии поддержки принятия решения при подготовке ИТ специалистов** [Электронный ресурс] / Е. Е. Андрианова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 138–141.

*Современные информационные технологии, основанные на использовании средств вычислительной техники и связи внедряются во все виды деятельности человека, причем многие из них связаны с принятием решения. Большинство людей убеждены в том, что принимать решения они безусловно умеют. Но, часто решения, принимаемые ими, или очевидны, или просто основаны на их опыте и интуиции. Часто возникают ситуации, когда, вариантов решений несколько и каждый из них имеет свои преимущества и недостатки, то есть выбор не очевиден. В таких случаях, как правило, появляется необходимость посоветоваться с кем-либо из экспертов, квалифицированных специалистов. Возникает потребность в системах поддержки принятия решения (СППР).*

**Ключевые слова:** технологии поддержки принятия решения, базы данных, базы знаний, данные, лицо принимающее решение, системы управления базами данных, системы управления базами знаний.

**Автоматизация процесса сбора и обработки данных с датчиков физических величин с помощью средств визуального программирования** [Электронный ресурс] / Е. А. Бубнова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 141–144.

*В статье объектом исследования является применение беспроводных сенсорных сетей, их эксплуатация, безопасность, а также внедрение в промышленный процесс. В процессе написания работы проводилось исследование беспроводных сенсорных сетей, их организация и построение. Так же были приведены вариации областей применения сенсорных сетей, их реализация и обоснование.*

**Ключевые слова:** беспроводная сенсорная сеть, сенсорная сеть, сенсор, датчик.

**Применение нечеткой искусственной нейронной сети в задаче распознавания эмоций** [Электронный ресурс] / И. А. Васильев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 145–149.

*Непостоянство эмоциональных признаков вызывает определенные сложности формализации модели представления эмоциональных реакций. В работе рассматривается применение нечетких экспертных систем в оценке эмоциональных реакций и возможность расширения критериев оценки, вводиться понятие «дескриптор эмоциональной реакции». Целью данной статьи является определение нечеткой нейронной сети, как основы для построения системы способной обобщить различные дескрипторы эмоци-*

ональных реакций, что позволит сделать многокритериальный вывод о текущем состоянии пользователя.

**Ключевые слова:** дескриптор эмоциональной реакции, нечеткие нейронные сети, эмоции, распознавание, подход определения эмоций.

**Интегрированная технология формализации требований на программный продукт на основе совместного использования двух формальных языков** [Электронный ресурс] / Н. В. Воинов, П. Д. Дробинцев, В. П. Котляров, И. В. Никифоров // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 149–155.

*В работе описывается подход с созданием высокоуровневой формальной модели, понятной заказчику и им контролируемой, и дальнейшим автоматическим преобразованием этой модели в формальную нотацию, с которой работают инструменты верификации и тестирования на основе моделей. Рассматриваются применяемые формальные нотации: высокоуровневая нотация Use Case Maps (UCM) и нотация базовых протоколов, на которой основан мощный инструмент верификации VRS. Также приведены результаты применения разработанного подхода.*

**Ключевые слова:** требования на программный продукт, спецификации, формализация, верификация, UCM.

**Разработка программного модуля автоматизированной маршрутизации внутрицеховых мобильных роботов** [Электронный ресурс] / И. П. Волынкин // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 155–158.

*В работе описываются принципы построения системы автоматизированной маршрутизации внутрицеховых мобильных роботов, алгоритмы маршрутизации, системы позиционирования внутри помещений, внутрицеховой транспорт.*

**Ключевые слова:** автоматизированная система управления, маршрутизация, RTLS, внутрицеховой транспорт.

**Проектирование образовательного модуля автоматизированной системы управления информационно-образовательной средой в сфере инженерных изысканий** [Электронный ресурс] / Н. Н. Горлушкина, Д. А. Денисова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 158–162.

*В работе описывается проектирование образовательного модуля автоматизированной системы управления информационно-образовательной средой в сфере инженерных изысканий, приводятся и анализируются результаты опроса об электронном обучении. Функциональные возможности образовательного модуля описываются с помощью диаграммы вариантов использования. Описываются средства, с помощью которых реализуется образовательный модуль.*

**Ключевые слова:** образовательный модуль, электронное обучение, SCORM, Yii, MySQL.

**Коды с суммированием и их модификации в функциональных системах контроля** [Электронный ресурс] / И. О. Грабко, Т. Х. Черкасова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 162–166.

*В работе анализируется помехоустойчивость классического кода Бергера и приводится ряд модификаций, показывающих лучшие результаты за счет изменения формирования проверочных разрядов.*

**Ключевые слова:** кодирование, код Бергера, помехоустойчивость, модифицированные коды, необнаруживаемые ошибки.

**Исследование аппаратно-программных комплексов Oracle Exadata в компании Japan Tobacco International** [Электронный ресурс] / К. С. Дегтева // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 167–170.

*В работе исследуется программно-аппаратный комплекс Oracle Exadata и процесс его внедрения в компании Japan Tobacco International. Перечисляются проблемы, которые решаются благодаря переходу на Exadata.*

**Ключевые слова:** аппаратно-программные комплексы, Exadata.

**Методика расчета обобщенного параметра функциональной готовности комплекса программно-технических средств** [Электронный ресурс] / Е. В. Катунцов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 171–174.

*В работе представлена методика расчета и прогнозирования обобщенного параметра функциональной готовности, которая позволяет оценить момент достижения предельно допустимого значения по обобщенному параметру в зависимости от фактической функциональной готовности комплекса программно-технических средств.*

**Ключевые слова:** комплекс программно-технических средств, функциональная готовность, прогнозирование, обобщенный параметр.

**Вопросы дизайна и безопасности при модернизации сайта** [Электронный ресурс] / М. А. Квасова // 68-я студенческая научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 175–177.

*В работе анализируются основные недостатки существующего информационного ресурса предприятия гостиничного бизнеса. Предложены решения, позволяющие значительно улучшить оформление, эргономику, а также защищенность существующей информационной системы.*

**Ключевые слова:** информационный ресурс, дизайн, аутентификация, авторизация, распределение ролей, администрирование.

**Разработка локальной версии системы регистрации пользователей в корпоративной системе вуза** [Электронный ресурс] / М. Е. Лю // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 178–180.

*В работе решена задача автоматизации процесса аутентификации студентов при посещении занятий в вузе с использованием индивидуальных пластиковых карт учащихся. Для разработки системы использовался язык программирования высокого уровня C++ и базы данных MSAccess.*

**Ключевые слова:** Корпоративная информационная система, аутентификация, базы данных, язык программирования C++.

**Разработка программного обеспечения дистанционного мониторинга автоматизированного технологического оборудования** [Электронный ресурс] / М. П. Моржаков // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 180–184.

*В работе отображена разработка системы мониторинга технологического оборудования. Рассмотрены существующие системы мониторинга и управления SCADA и их различия с разрабатываемой системой. Рассмотрены возможности программных фреймворков WCF, WPF и их применение в данном проекте. Показаны возможности визуализации информации о состоянии оборудования.*

**Ключевые слова:** система мониторинга оборудования, SCADA, WCF, WPF, C#, визуализация, интерфейс.

**Модель канала связи мультисервисной банковской сети на технологии IP/FRAME RELAY** [Электронный ресурс] / Н. Н. Мошак // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 185–189.

*В работе с позиций системного подхода на базе архитектуры гибридной транспортной системы мультисервисной телекоммуникационной банковской сети на технологии IP/FrameRelay построены сетевые критерии эффективности использования пропускной способности каналов связи речевым трафиком и трафиком данных в режиме установленного соединения с учетом архитектуры транспортной системы сети и требуемого качества сервиса QoS (Quality of Service) – заданных потерь по вызовам для речевого трафика и заданного времени передачи пакета данных. На основе указанных критериев эффективности предложена аналитическая модель типового транспортного канала передачи сети. Приводится пример расчета зависимости параметров канала связи от величины входной речевой нагрузки.*

**Ключевые слова:** мультисервисная сеть связи, транспортная система сети, FrameRelay.

**Разработка системы автоматической трансляции данных из таблиц расписаний занятий, представленных в формате Excel, в таблицы СУБД MySQL** [Электронный ресурс] / М. М. Осипенко // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 189–192.

*В данной работе была решена задача автоматической трансляции данных из таблиц, содержащих расписания занятий в вузе и составленных в формате Excel, в нормированные таблицы реляционной базы данных MySQL. Для решения задачи использовалось открытое свободное программное обеспечение. В качестве языка программирования был выбран язык PHP. Для построения базы данных была выбрана СУБД MySQL, которая позволяет решать задачи любой сложности.*

**Ключевые слова:** автоматическая обработка данных, MS Excel, СУБД MySQL, расписание занятий в вузе.

**Сравнение статистических параметров речевых сигналов гортанной и произносимой вслух речи** [Электронный ресурс] / Е. В. Плотникова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 193–196.

*Исследование речевых функций гортани и возможности снятия и распознавания «закрытой гортанной речи» перспективно для создания устройств, которые позволяют человеку общаться при громких шумах, в местах требующих тишины или при работе в ситуациях без возможности произносить речь «вслух».*

**Ключевые слова:** гортанская речь, распознавание речи, передача речи.

**Разработка генетического алгоритма синтеза электрических цепей** [Электронный ресурс] / И. С. Пономарев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 196–201.

*В работе приводится методология разработки генетического алгоритма для структурно-параметрического синтеза электрических цепей. Рассмотрены возможный способ представления электрической цепи в работе алгоритма, способы применения генетических операторов и генерации решений. Также приведен пример реализации функции выживания для ФНЧ.*

**Ключевые слова:** генетический алгоритм, электрические цепи, лестничные цепи, структурно-параметрический синтез.

**Применение интерполяции для устранения артефактов в кадрах видеопоследовательности** [Электронный ресурс] / И. С. Рубина // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 202–207.

*В работе рассматриваются методы интерполяции изображений и возможность их применения в процессе сжатия видеоданных, для устранения ряда артефактов, связанных, как с динамическими свойствами объектов видеопоследовательности, так и используемыми алгоритмами в последовательности этапов кодирования. Разработан новый метод интерполяции, сущность которого заключается в использовании адаптивного рекурсивного алгоритма с использованием переменного размера ядра интерполяции, позволивший повысить степень сжатия на 30 % и качества восстановленной видеопоследовательности на 2 % по сравнению со сжатием без интерполяции. Результаты исследования найдут широкое применение в задачах обработки видеоданных, кодеках сжатия видео и системах потокового вещания.*

**Ключевые слова:** интерполяция, адаптивный алгоритм, матрица переменного размера, пространственная модель.

**Модель системы аутентификации с использованием QR-кода для доступа к персонализированным данным** [Электронный ресурс] / Е. Е. Семенова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Сту-

денческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 207–211.

*Работа посвящена описанию процедуры аутентификации с использованием QR-кода. В статье сформирован алгоритм системы, приведена модель функционирования системы и описаны основные достоинства предложенного метода.*

**Ключевые слова:** аутентификация, авторизация, QR-код.

**Метод концентрических сфер для послойного определения продуктов горения** [Электронный ресурс] / А. В. Соловьева // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 212–216.

*Для описания процесса распространения горения из центра возгорания до внутренних границ замкнутого пространства сложной конфигурации предлагается использование метода концентрических сфер для послойного определения температуры и давления газа в каждой точке объема в определенный момент времени.*

*Данный метод открывает возможности для детального моделирования процесса горения с различными параметрами точности.*

**Ключевые слова:** концентрические сферы, математическое моделирование, горение и взрывы, замкнутый объем.

**Разработка фрагмента программы для автоматизации учебного процесса** [Электронный ресурс] / С. В. Ушанов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014»: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 216–220.

*В работе рассматривается система АИС «Учета посещаемости и успеваемости» совместно с АИС «Успех» которые позволяет облегчить работу преподавателей различных степеней обучения. Показаны преимущества систем. А так же область их применения.*

**Ключевые слова:** АИС, операционная система, образовательное учреждение, база данных.

**Защита от DDoS-атак методом проксирования** [Электронный ресурс] / Д. В. Шарафанов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 221–224.

*В статье представлен анализ метода построения защиты от распределенных атак на отказ в обслуживании с помощью проксирования трафика. Рассмотрены методы фильтрации входящих пакетов методами автоматического и поведенческого алгоритмов фильтрации, а также указаны основные особенности, преимущества использования сервисов защиты от DDoS-атак, работающих по принципу проксирования входящих запросов.*

**Ключевые слова:** DDoS-атаки, сервис защиты, проксирование, поведенческий метод фильтрации.

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОНИКИ

**Исследование нелинейной динамики однофазных корректоров коэффициента мощности** [Электронный ресурс] / А. И. Андриянов, И. Ю. Бутарев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 225–230.

*Выполнен анализ нелинейных динамических свойств однофазных корректоров коэффициента мощности. Приводятся двухпараметрическая карта динамических режимов, однопараметрическая бифуркационная диаграмма и диаграмма мультипликаторов. На основе полученной информации возможен научно-обоснованный подход к выбору оптимальной силовой части на этапе проектирования, с учетом нелинейных динамических свойств.*

**Ключевые слова:** корректор коэффициента мощности, нелинейная динамика, проектный динамический режим, коэффициент мощности

## ЭКОНОМИКА И УПРАВЛЕНИЕ В СВЯЗИ

**Исследование организационно-экономических проблем регулирования телекоммуникационного рынка связанных со вступлением Российской Федерации в ВТО.** [Электронный ресурс] / Ю. В. Бобрик, Ю. А. Кострикова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 231–235.

*Статья посвящена анализу последствий от вступления Российской Федерации в ВТО для российского телекоммуникационного рынка и их возможностям их сглаживания.*

**Ключевые слова:** телекоммуникационный рынок, ВТО, повышение себестоимости услуг связи, меры поддержки отечественных производителей.

**Рациональные способы начисления оплаты за услугу доступа к сети Интернет** [Электронный ресурс] / М. В. Карпенко // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 236–240.

*В работе рассматривается проблема предоставления услуги доступа к сети Интернет в пунктах общественного питания абсолютно всем группам клиентов независимо от их желания пользоваться данной услугой. Доступ к сети Интернет в пунктах общественного питания предоставляется на основе стандарта IEEE 802.11 (Wi-Fi). Рассмотрен вариант решения данной проблемы путем разделения помещений пунктов общественного питания на залы "С Wi-Fi" и "Без Wi-Fi".*

**Ключевые слова:** идеальная цена потребления, оплата услуги доступа к сети Интернет, беспроводной доступ к сети Интернет, Wi-Fi.

**Инновационный проект: трёхуровневая бизнес-модель телеканала «Молодежная среда»** [Электронный ресурс] / А. И. Копп // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 241–245.

*В статье описан инновационный проект по созданию трёхуровневой бизнес-модели телеканала «Молодёжная среда». Определено влияние телеканала «Молодёжная среда» на качество образования и решение проблемы низкой осведомленности молодежи о требованиях производства и разнообразии видов деятельности. Новизна идеи телеканала «Молодёжная среда» заключается в распределённой работе телередакций образовательных учреждений и централизованном показе на интернет-телеканале «Молодёжная среда» подготовленных ими видеоматериалов по расписанию определённого профиля учебного заведения. Телеканал является интерактивным: предоставляет возможность телезрителям выразить мнение о сюжете, оценить степень новизны темы сюжета, проголосовать за понравившийся сюжет. Информационное содержание телеканала «Молодёжная среда» представляет интерес для студентов и их родителей, школьников, абитуриентов, учёных, преподавателей, факультета повышения квалификации, а также телеканалов.*

**Ключевые слова:** информационное содержание, заинтересованные стороны, телеканал, телередакция.

**Разработка метода формального конструирования сервисов предприятия на основе бизнес-процессов** [Электронный ресурс] / А. И. Копп // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых: материалы конференции. – СПб. : СПбГУТ, 2014. – С. 246–251.

*В работе на основе анализа матриц смежности и матрицы инцидентности процессного графа предложен способ выявления сервисов, возникающих при взаимодействии организационных единиц предприятия. Разработанный метод применён к описанному в нотации BPMN 2.0 бизнес-процессу «Обслуживание авиапассажира после полёта». Статья представляет интерес для специалистов в области архитектуры предприятия, SOA. Читателю рекомендуется обладать знанием построения и чтения матриц смежности и инцидентности графа.*

**Ключевые слова:** бизнес-процесс, взаимодействие ролей, граф, матрица инцидентности, матрица смежности, сервис.

**Эволюция и изучение электронных систем на кристалле** [Электронный ресурс] / У. В. Мальцева // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 252–255.

*Руководители предприятий ежедневно сталкиваются с множеством задач о развитии и движении предприятия. Однако, сложно сказать, как каждое из этих решений может повлиять на продажу или производство продукции, пока не пройдет некоторое время. Потерянное время может дорого обойтись, если ситуацию не контролировать постоянно, анализируя каждое из принятых решений. Предлагается метод, который поможет управляющим принимать решения на любой момент времени.*

**Ключевые слова:** кластерный анализ, алгоритм форель, эталонные значения.

## ГУМАНИРАТНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

**Актуальные философские проблемы современности** [Электронный ресурс] / О. Н. Агеев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 256–260.

*В данной работе анализируются четыре самые важные на мой взгляд философские проблемы современности, а именно: проблема сущности человека, проблема смысла и цели жизни, сознание как философская проблема, проблема свободы человека. Мне кажется рассмотрение данных проблем не должно обходить стороной современных философов, так как они не могут решиться на протяжении нескольких десятков, а может быть даже и сотни лет.*

**Ключевые слова:** проблемы, сущность, смысл и цель жизни, сознание, свобода.

**Золотое сечение** [Электронный ресурс] / Д. Д. Алексеева // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 260–263.

*В работе раскрывается понятие золотого сечения, рассказывается о её истории, об ученых, которые работали над божественной пропорцией. Также раскрывается понятие золотого сечения с философской точки зрения. В ходе работы было проведено исследование, и рассчитано, какой процент учащихся первых курсов СПбГУТ имеет золотые пропорции в лице.*

**Ключевые слова:** золотое сечение, золотая пропорция, философия золотого сечения.

**Дух британских замков в лингвокультурологическом аспекте** [Электронный ресурс] / О. С. Барбир // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 263–267.

*Работа посвящена рассмотрению роли замков в истории и культуре Великобритании. Автор исследует процесс развития и популяризации замков на территории Соединённого Королевства. Описываются характерные черты и основные элементы замка как особого типа архитектурного сооружения, а также типы замков. Делается вывод о том, что замок является неотъемлемой частью культуры Великобритании.*

**Ключевые слова:** норманнский замок, кельтский замок, укрепленный манор, замковая ментальность, замок-поместье, не собственно замок.

**Специфика современного российского телевещания аспекте** [Электронный ресурс] / М. А. Беккер // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 267–272.

*В работе с помощью подсчета статистики выявляются основные черты современного российского телевещания выходного дня: его целевая аудитория, особенности наполнения телевещательной сетки, наиболее широко представленные виды программ, их возрастные ограничения и страны-производители, наиболее и наименее представленные в сетке выходного дня жанры кино.*

**Ключевые слова:** телевещание, телевидение, статистика, Россия.

**Сравнение русской и финской культур: влияние межкультурных различий на ведение бизнеса** [Электронный ресурс] / И. А. Гель // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 272–276.

*В работе приводятся основные характеристики параметров межкультурных различий, выделенных голландским исследователем Гертом Хофтеде. Анализируются деловые культуры России и Финляндии на основе предложенных параметров. Проводится сравнение данных культур и предлагаются рекомендации для финских и российских менеджеров руководящего и исполнительного уровней, работающих соответственно в России и Финляндии.*

**Ключевые слова:** параметры межкультурных различий, Герт Хофтеде, деловые культуры России и Финляндии, рекомендации для менеджеров.

**Аланский вопрос в отношениях Швеции и Финляндии в 1918–1921 гг. как пример решения этнотERRиториального конфликта в Северной Европе** [Электронный ресурс] / А. Б. Гехт // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 277–281.

*В статье рассматривается Аланский вопрос, игравший заметную роль в отношениях Швеции и Финляндии в 1918–1921 гг. Анализируются причины, лежавшие в основе этнотERRиториальных противоречий в отношениях двух стран, перечисляются ключевые этапы в эволюции Аланского вопроса, рассматриваются его основные последствия для шведско-финских отношений в период, предшествующий началу Второй мировой войны.*

**Ключевые слова:** Аланский вопрос, регион Балтийского моря, история шведско-финских политических отношений.

**Персонажи пьес У. Шекспира и историческая реальность** [Электронный ресурс] / О. С. Дерябина // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 281–284.

*Работа посвящена изучению достоверности исторических хроник Уильяма Шекспира. Целью работы было найти грани, где реальность соприкасается с вымыслом.*

**Ключевые слова:** Уильям Шекспир, исторические хроники, английская литература.

**Практики информационного противодействия конкурентам: рекламные войны** [Электронный ресурс] / Е. А. Дорохова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 285–289.

*В работе рассмотрена практика информационного противодействия конкурентам посредством ведения рекламных войн. В рамках практики рекламных войн выделены основные стратегии поведения брендов-конкурентов, а также рассмотрены характеристики данных стратегий.*

**Ключевые слова:** реклама, рекламная война, стратегия, стратегии рекламных войн, бренд, конкуренты, конкуренция.

**Слова-паразиты в современном английском языке** [Электронный ресурс] / М. М. Заливина // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 289–293.

*Данная работа посвящена изменениям в современном английском языке. На примерах аутентичных текстов показано, что ряд лексических единиц, не утратив своего исходного значения, также выполняют в коммуникации новые функции, а именно, функции слов-паразитов. Приводятся данные, иллюстрирующие изменение языкового «престижа», когда развитие языка идет не сверху вниз, а снизу-вверх.*

**Ключевые слова:** слова-паразиты, позитивное мышление, ОК, уровень образования, некатегоричность высказывания, стратегия переоценки.

**Нейтралитет как инструмент шведской внешней политики в период «холодной войны» с 1949 по 1969 гг.** [Электронный ресурс] / Т. А. Захаренко // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 293–297.

*В работе рассматриваются понятие «нейтралитет», его виды и особенности шведского нейтралитета на фоне общепризнанных международно-правовых стандартов прав и обязанностей государства с нейтральным статусом. Приводятся примеры уклонения от провозглашенной политики, как в военное, так и в мирное время. Представлены мнения различных правящих партий Швеции по вопросу о необходимости сохранения и соблюдения нейтралитета.*

**Ключевые слова:** нейтралитет, свобода от альянсов, «холодная война», НАТО, план Marshalla.

**Влияние современного информационного пространства на становление и развитие личности** [Электронный ресурс] / Т. Б. Золотова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 297–300.

*В работе анализируется воздействие современного информационного пространства на становление и развитие личности. Рассматривается положительное и отрицательное влияние современных технологий на ребенка и взрослого человека. Показаны наиболее яркие проблемы современного общества, связанные с информационным пространством, такие как комплексы, прокрастинация, стремление к несуществующим идеалам и так далее.*

**Ключевые слова:** информационное пространство, ребенок, индивидуум, проблемы общества, интернет, телевидение.

**Шахматы как средство воспитания инженерной мысли** [Электронный ресурс] // А. С. Крылов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 301–304.

*В работе рассмотрены особенности мышления и психологического склада, общие для людей, занимающихся шахматами и научно-техническим творчеством, а именно, способность к расчету вариантов, память, эрудиция, интуиция, фантазия, самокритич-*

*ность, смелость в принятии решений. Сделан вывод о пользе занятия шахматами для развития инженерного творчества.*

**Ключевые слова:** шахматы, инженер, наука, мышление.

**Применение методов мотивации в управлении организацией** [Электронный ресурс] / Ю. А. Попова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 304–307.

*В работе рассматривается, что же такое мотивация и её различные методы и виды. Так же различные графики работы, которые способствуют повышению уровня труда. В ходе работы было проведено тестирование и проанализированы результаты и даны соответствующие рекомендации.*

**Ключевые слова:** мотивация, управление, потребности, методы мотивирования.

**Философские проблемы постмодерна** [Электронный ресурс] / А. А. Тарабаев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 307–310.

*В работе анализируются философские проблемы постмодернизма, а именно: проблема хаоса, проблема человека, проблема языка, проблема истины. Мне кажется, современные философы не должны обходить стороной эти проблемы, т.к. мировоззрение будущего во многом зависит от их решения.*

**Ключевые слова:** проблемы, постмодерн, постмодернизм, проблема хаоса, проблема языка, проблема истины, кризис метасценариев.

**Роль Швеции в создании трансатлантической зоны свободной торговли** [Электронный ресурс] / Е. И. Фатькина // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 310–313.

*В работе рассматривается значение деятельности Швеции для развития трансантлантической зоны свободной торговли. Показано двустороннее сотрудничество между США и Швецией в различных областях.*

**Ключевые слова:** Швеция, США, Европейский союз, интеграционные процессы, торгово-экономические отношения, трансантлантическая зона свободной торговли.

**Общественное мнение в социальных сетях: мотивационно-ценостные компоненты** [Электронный ресурс] / А. А. Шарамыгина // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 313–317.

*В статье обосновывается актуальность исследования, дается определение понятию «общественное мнение», описывается специфика выражения общественного мнения в социальных сетях и особенности его мотивационно-ценостных компонентов. Представлен сравнительный анализ результатов теоретических и собственных эмпирических исследований.*

**Ключевые слова:** общественное мнение, социальные сети, ценности, мотивация, влияние.

## СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**Сбор и использование трофеейной техники связи и военно-технического имущества. Эвакуация техники связи и вооружения. Организация учета имущества связи** [Электронный ресурс] / А. А. Асеев, А. Н. Дробяскин, А. Н. Музыкантов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 318–322.

*Под трофеями принято понимать захваченное у противника вооружение, военное имущество, продовольствие, военно-промышленное оборудование, запасы сырья и готовой продукции, предназначенные для обеспечения нужд вооруженных сил воюющего государства. К началу Великой Отечественной Войны Советская Армия не имела самостоятельной трофеейной службы.*

**Ключевые слова:** трофеи, имущество, снабжение, склады.

**Применение оборудования NGN на сетях военной связи** [Электронный ресурс] / Л. В. Воробьев, А. А. Темуров, О. И. Федоровских // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 323–327.

*В работе анализируются тенденции в развитии телекоммуникационных сетей и направление совершенствования сетей военной связи. Показана возможность построения военных сетей на оборудовании гражданского назначения. Рассмотрен вариант состава оборудования узлов связи.*

**Ключевые слова:** развития телекоммуникационных сетей, сети связи следующего поколения, сети военной связи.

**Радиоэлектронная защита станции спутниковой связи** [Электронный ресурс] / С. В. Воронин, А. А. Крючков // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 327–329.

*В работе анализируются меры и мероприятия по радиоэлектронной защите станций спутниковой связи. Показаны технические средства защиты, а также организационные мероприятия по радиоэлектронной защите.*

**Ключевые слова:** станция спутниковой связи, радиоэлектронная защита, помехозащищенность.

**Алгоритм функционирования и предложения по составу аппаратной контроля безопасности связи в сетях связи военного назначения** [Электронный ресурс] / Н. А. Выговская, А. К. Сагдеев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 330–335.

*Обеспечение безопасности связи – одна из важнейших составных частей общей системы мер по сохранению сведений в военной области, составляющих государственную тайну. Оно взаимосвязано с мероприятиями скрытого управления войсками, оперативной маскировки и режимом секретности. Непременным условием достижения*

*безопасности связи является систематическое проведение квалифицированного контроля организации и состояния безопасности связи. В статье разработан алгоритм, позволяющий обосновать состав подвижного комплекса контроля безопасности связи.*

**Ключевые слова:** аппаратная контроля, безопасность связи, сети военной связи.

**Обоснование применения технологии DWDM на сетях специального назначения** [Электронный ресурс] / А. М. Галкин, С. М. Кадашников // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 335–338.

*В работе говориться о развитии и преимуществах применения технологии спектрального мультиплексирования, их классификация, а также возможность применения данной технологии на специальных сетях связи. Представлена компания ООО «Т8», как ведущий отечественный производитель в данном сегменте.*

**Ключевые слова:** спектральное мультиплексирование, DWDM.

**Иновационные чувствительные элементы давления для радиозондирования атмосферы** [Электронный ресурс] / О. А. Гильдеева, В. А. Савостина // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 339–343.

*Предлагается к рассмотрению инновационный датчик воздушного давления для аэрологических радиозондов. Датчик предназначен для преобразования, подаваемого на него избыточного абсолютного давления воздуха, в цифровой код измеряемой величины. Датчик воздушного давления акустоэлектронный интерфейсный ДДАЭ-И относится к измерительной технике и может быть использован в метеорологических радиозондах для измерения вертикального профиля давления в атмосфере.*

**Ключевые слова:** датчик воздушного давления, аэрологический радиозонд, атмосфера.

**Задание исходных данных алгоритма синтеза системы показателей надежности** [Электронный ресурс] / В. П. Грецов, С. В. Дьяков, С. Е. Иванов, А. В. Семизоров // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 344–347.

*Одним из ключевых вопросов при проведении НИОКР является оценивание надежности объекта. Однако методы, применяемые при контрольных испытаниях на надежность, ориентированы на анализ отдельных объектов (изделий) в вышестоящей системе. Основой для решения данных задач могут выступать методы экспериментального анализа с использованием теории искусственных нейронных сетей.*

**Ключевые слова:** Информационное направление, система показателей надежности, экстраполирующая нейронная сеть, когнитивные карты.

**Методологические вопросы синтеза структуры системы синхронизации на основе распределенных информационно-управляющих структур** [Электронный ресурс] / В. В. Дворяков, К. И. Стакеев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 347–351.

*В статье представлена методика формирования структуры системы синхронизации региональной транспортной сети связи специального назначения, основанная на решении оптимизационно-имитационных задач, применяемых для распределенных информационно-управляемых систем. Данная методика включает последовательность решения взаимоувязанных задач синтеза основных элементов и частей системы, которые позволяют произвести выбор наилучшего варианта всей системы по заданным критериям оптимальности. На каждом из этапов синтеза необходимо применять оптимизационно-имитационные процедуры с обязательной проработкой и уточнением вариантов построения отдельных подсистем, с учетом их динамических, а в некоторых и стохастических характеристик функционирования элементов управления и их взаимодействий между собой.*

**Ключевые слова:** система синхронизации, региональная транспортная сеть связи, структура, методика, оптимизационно-имитационные процедуры.

**Процесс радиоконтроля использования радиочастотного спектра** [Электронный ресурс] / В. Г. Ерышов, А. В. Давыдов, А. А. Панкин, П. А. Хайдакин // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 351–354.

*Процесс радиоконтроля использования радиочастотного спектра связан с обеспечением электромагнитной совместимости радиоэлектронных средств. Сам процесс можно представить в виде ориентированного графа состояний и описать в терминах теории Марковских случайных процессов с дискретным состоянием и непрерывным временем. Составляя для него систему обыкновенных дифференциальных уравнений Колмогорова, можно получить модель процесса радиоконтроля использования радиочастотного спектра, позволяющая получить вероятностные и временные характеристики, описывающие состояние анализируемых процессов.*

**Ключевые слова:** радиоконтроль, радиочастотный спектр, электромагнитная совместимость радиоэлектронных средств.

**Морфологическая модель полевой транспортной сети связи специального назначения** [Электронный ресурс] / О. П. Жадан, М. А. Морозов, И. Г. Стажеев // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 354–359.

*Морфологический анализ является весьма эффективным средством для решения задач по построению сетей связи, поскольку он позволяет выявить, систематизировать и изучить всевозможные варианты и способы построения системы, пред назначенной для реализации заданных функций. Он позволяет систематически выявить всю полноту возможных вариантов построения ПТСС СН.*

**Ключевые слова:** морфологическая модель, полевая транспортная сеть связи, система, сеть связи специального назначения.

**Анализ перспектив развития систем технологического управления транспортной сети связи специального назначения** [Электронный ресурс] / С. С. Казаков, С. В. Мельников // 68-я региональная научно-техническая конференция студентов, ас-

пирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 360–364.

*В работе анализируются развитие и текущее состояние систем управления транспортными сетями связи. Показаны преимущества и недостатки различных систем управления, а также их применение.*

**Ключевые слова:** система управления, TMN, CORBA, Java, DCOM.

**Актуальные экологические проблемы Военно-воздушных Сил** [Электронный ресурс] / Д. А. Каспирович, Н. Е. Манвелова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 364–369.

*Статья посвящена современным экологическим проблемам Военно-воздушных сил РФ. Показано, что наиболее значимыми загрязнителями, поступающими в результате деятельности ВВС в окружающую среду, является авиационное топливо, продукты его сгорания, а также утечки авиационного топлива при его длительном хранении (керосиновые линзы) в условиях морально и технически устаревшего складского хозяйства.*

**Ключевые слова:** авиационное топливо, заправка самолетов (наземная и воздушная), склады топлива, керосиновые линзы.

**Система дистанционного питания подводных волоконно-оптических линий связи** [Электронный ресурс] / Е. М. Колесова, М. А. Суранова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 369–374.

*В работе проводится анализ вариантов построения систем дистанционного питания для организации электропитания подводных волоконно-оптических линий связи. Представлен анализ и классификация существующих схем систем дистанционного питания, а также рассмотрены принципы организации цепей дистанционного писания.*

**Ключевые слова:** дистанционное питание, необслуживаемый усилительный пункт, волоконно-оптические линии связи.

**Вулканы. Извержения вулканов и их последствия, способы обеспечения безопасности и оповещения во время извержения** [Электронный ресурс] / В. В. Коптяков, В. А. Феоктистов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 374–379.

*Представлены основные понятия, связанные с извержениями вулканов и их последствиями. Определены способы обеспечения безопасности людей и их оповещения об опасностях извержения вулканов.*

**Ключевые слова:** вулканы, извержения вулканов, безопасность людей, оповещение.

**Применение эллиптических кривых в системах криптографии** [Электронный ресурс] / М. С. Корчагин, А. К. Сагдеев, Ю. А. Фролова // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 379–384.

*Одним из путей решения проблемы защиты информации, а точнее – решения небольшой части вопросов из всего спектра мер защиты, является криптографическое пре-*

*образование информации, или шифрование. В статье предложен новый алгоритм шифрования данных, основанный на использовании эллиптических кривых.*

**Ключевые слова:** криптография, защита информации, асимметричные алгоритмы шифрования, эллиптические кривые.

**О целесообразности использования малоотходных, ресурсосберегающих и экологически безопасных технологий химической переработки древесины** [Электронный ресурс] / Н. П. Куров, С. А. Рудик // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 384–388.

*Статья посвящена проблемам экологически ответственного лесопользования. Показаны преимущества малоотходных технологий химической переработки древесины в сравнении с традиционными сульфатным и сульфитным способами получения целлюлозы.*

**Ключевые слова:** лес РФ, химическая переработка древесины, целлюлозно-бумажная промышленность, негативное воздействие на окружающую среду, загрязнения сточных вод ЦБП.

**Экологические проблемы околоземного космического пространства** [Электронный ресурс] / Н. Е. Манвелова, Д. Г. Никитин, С. А. Панихидников // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 389–394.

*Рассмотрены основные экологические проблемы околоземного космического пространства (ОКП), связанные с деятельностью ракетно-космической техники, выделены наиболее значимые техногенные воздействия: механическое (космический мусор), химическое, электромагнитное и радиоактивное загрязнение ОКП; обозначены возможности уменьшения техногенного воздействия на околоземное космическое пространство.*

**Ключевые слова:** околоземное космическое пространство (ОКП), техногенное воздействие, космический мусор, пути уменьшения техногенного воздействия.

**Некоторые аспекты утилизации химического оружия** [Электронный ресурс] / Н. Е. Манвелова, С. А. Панихидников, К. А. Филиппов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 394–398.

*Рассмотрены основные аспекты проблемы утилизации химического оружия, негативные последствия затопления запасов химоружия времен Второй мировой войны. Приведены сведения о технологии переработки отравляющих веществ, охарактеризовано состояние вопроса утилизации химоружия в РФ.*

**Ключевые слова:** негативные экологические последствия затопления химоружия, технология и предприятия по утилизации отравляющих веществ в РФ.

**Схемотехническое решение по построению приемника дистанционного питания необслуживаемого оптического усилителя** [Электронный ресурс] / И. Ф. Пырву // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых

ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 399–402.

*В работе приводится схемотехническое решение по построению приемника дистанционного питания необслуживаемого оптического усилителя подводной волоконно-оптической линии связи. Представлена функциональная схема приемника дистанционного питания, поясняется назначение его блоков, а также принцип их действий.*

**Ключевые слова:** приемник дистанционного питания, необслуживаемый оптический усилитель, волоконно-оптическая линия связи.

**Проблемы парникового эффекта и способы их решения** [Электронный ресурс] / И. С. Размётова, В. А. Феоктистов // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 403–407.

*В настоящее время проблема парникового эффекта является одним из наиболее глобальных экологических вопросов, стоящих перед человечеством. Суть этого явления состоит в том, что солнечное тепло остается у поверхности нашей планеты в виде оранжерейных газов. Главной причиной парникового эффекта является попадание в атмосферу промышленных газов. Решить проблему парникового эффекта возможно, но надо, чтобы все люди приложили максимум усилий для предотвращения последствий уже существующих и будущих.*

**Ключевые слова:** парниковый эффект, парниковые газы, киотский протокол.

**Анализ реализации оптических коммутаторов на основе эффекта Поккельса** [Электронный ресурс] / Д. С. Самаркин, Н. Г. Строева // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 408–412.

*Применение электронных преобразователей в оптических сетях приводит к двойному преобразованию сигнала – из оптического в электрический и обратно. В результате сеть становится неоднородной, что ведет к существенному удорожжанию оборудования. Построение однородных оптических сетей возможны с применением оптических коммутирующих устройств.*

**Ключевые слова:** коммутатор, ячейка Поккельса, эффект Поккельса, оптический коммутатор.

**Построение подводной трансокеанской линии связи России** [Электронный ресурс] / А. И. Симоненко, И. Г. Стакеев А. А. Яхункина, // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. – СПб. : СПбГУТ, 2014. – С. 412–416.

*В статье рассматривается вопрос построения трансокеанской линий связи, в частности по Северной части Российской Федерации. Данная линия в перспективе должна соединиться с существующей линией связи, которая проходит по югу страны. В статье особое внимание уделяется возможным проблемам, которые могут возникнуть для выполнения данного проекта. Несмотря на большие трудности и недостатки при прокладке и организации связи на северных территориях страны, предлагаемая система связи наименьшим образом подвержена средствам информационной разведки, террористическим актам, имеет высокую помехозащищенность и безопасность.*

**Ключевые слова:** трансокеанская линия связи, ВОЛС, подводный кабель связи.

## АВТОРЫ СТАТЕЙ

АЛЕКСЕЕВ  
Антон Дмитриевич

студент группы МБИ 22-м Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [me@talleyran.ru](mailto:me@talleyran.ru)

АГЕЕВ  
Олег Николаевич

студент группы ИКТ-303 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [assassin93409@gmail.com](mailto:assassin93409@gmail.com)

АНДРИАНОВ  
Владимир Игоревич

кандидат технических наук, доцент кафедры «Защищенных систем связи» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [Vladimir.i.andrianov@gmail.com](mailto:Vladimir.i.andrianov@gmail.com)

АНДРИАНОВА  
Екатерина Евгеньевна

старший преподаватель кафедры «Безопасность информационных систем» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [chikaleva1@rambler.ru](mailto:chikaleva1@rambler.ru)

АНДРИЯНОВ  
Алексей Иванович

кандидат технических наук, доцент кафедры «Электронные, радиоэлектронные и электротехнические системы» Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Брянский государственный технический университет», [ahaos@mail.ru](mailto:ahaos@mail.ru)

АРТУР  
Джозеф Квеку

аспирант кафедры «Радиопередающие устройства и средств подвижной связи» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [ajkweku@yahoo.com](mailto:ajkweku@yahoo.com)

АСЕЕВ  
Алексей Андреевич

студент группы ИКТВ-31 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [aleeeses@mail.ru](mailto:aleeeses@mail.ru)

**БАРБИР**  
Ольга Сергеевна  
студентка группы ЗР-32 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [barbir.o@mail.ru](mailto:barbir.o@mail.ru)

**БАХОЛДИН**  
Алексей Валентинович  
кандидат технических наук, доцент, заведующий кафедрой «Прикладная и компьютерная оптика» Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», [bakholdin@aco.ifmo.ru](mailto:bakholdin@aco.ifmo.ru)

**БЕККЕР**  
Маргарита Андреевна  
студентка группы ЗР-31 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [margaritabk2226@gmail.com](mailto:margaritabk2226@gmail.com)

**БЕНЕТА**  
Элина Валерьевна  
аспирант кафедры «Электрическая связь» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет путей сообщения», [elinabeneta@yandex.ru](mailto:elinabeneta@yandex.ru)

**БОБРИК**  
Юлия Владимировна  
студентка группы ЭМ-27 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [julia.vl.mil@gmail.com](mailto:julia.vl.mil@gmail.com)

**БОНДАРЕВ**  
Владислав Юрьевич  
студент группы СК-92 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [1992bondarev@gmail.com](mailto:1992bondarev@gmail.com)

**БУБНОВА**  
Елена Алексеевна  
студентка группы ТСС-31м Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [ele.bubnova@gmail.com](mailto:ele.bubnova@gmail.com)

**БУТАРЕВ**  
Игорь Юрьевич  
аспирант кафедры «Электронные, радиоэлектронные и электротехнические системы» Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Брянский государственный технический университет», [igorbutarev@gmail.com](mailto:igorbutarev@gmail.com)

ВАРЕЛЬДЖЯН  
Каринэ Степановна  
студентка группы СК-91 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [karisha.var@gmail.com](mailto:karisha.var@gmail.com)

ВАСИЛЬЕВ  
Евгений Владимирович  
аспирант кафедры «Сети связи» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[jimmbraddock@gmail.com](mailto:jimmbraddock@gmail.com)

ВАСИЛЬЕВ  
Иван Андреевич  
старший преподаватель кафедры «Информатика и компьютерный дизайн» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[Ivan3Dgraphic@yandex.ru](mailto:Ivan3Dgraphic@yandex.ru)

ВИТКОВА  
Лидия Андреевна  
студентка группы МБИ-22м Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [lidia@iskin.spb.ru](mailto:lidia@iskin.spb.ru)

ВОИНОВ  
Никита Владимирович  
кандидат технических наук, доцент кафедры «Информационные и управляющие системы» института Информационных технологий и управления Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный политехнический университет»,  
[voinov@ics2.ecd.spbstu.ru](mailto:voinov@ics2.ecd.spbstu.ru)

ВОЛЫНКИН  
Иван Павлович  
студент группы ТСС-95 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [jonasas@mail.ru](mailto:jonasas@mail.ru)

ВОРОБЬЕВ  
Леонид Васильевич  
кандидат технических наук, доцент, начальник цикла – старший преподаватель военной кафедры института военного образования Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[lv.vorobjev@yandex.ru](mailto:lv.vorobjev@yandex.ru)

- ВОРОНИН**  
Сергей Владимирович  
кандидат технических наук, доцент, начальник цикла военной кафедры – старший преподаватель института военного образования Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [wsw1@yandex.ru](mailto:wsw1@yandex.ru)
- ВЫЮГОВСКАЯ**  
Наталья Александровна  
студентка группы ИКТВ-32 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[natasha14-23@mail.ru](mailto:natasha14-23@mail.ru)
- ГАЛИЦКИЙ**  
Александр Анатольевич  
студент группы СП-91 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[galexant@yandex.ru](mailto:galexant@yandex.ru)
- ГАЛКИН**  
Анатолий Михайлович  
кандидат технических наук, доцент кафедры «Сетей Связи» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[galkinam@inbox.ru](mailto:galkinam@inbox.ru)
- ГАМИЛЬ**  
Абдуллах Абдулрахман  
аспирант кафедры «Инфокоммуникационные системы» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[obad-85a@mail.ru](mailto:obad-85a@mail.ru)
- ГАРАПОВА**  
Луиза Рамилевна  
студентка Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[garapova.l@ya.ru](mailto:garapova.l@ya.ru)
- ГЕЛЬ**  
Ирина Александровна  
студентка группы Э-01 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[eskada93@mail.ru](mailto:eskada93@mail.ru)

- ГЕХТ  
Антон Борисович  
аспирант кафедры «История и регионоведение» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[a.geht@yandex.ru](mailto:a.geht@yandex.ru)
- ГОЙХМАН  
Вадим Юрьевич  
кандидат технических наук, доцент кафедры «Инфокоммуникационные системы» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[vg@sotsbi.ru](mailto:vg@sotsbi.ru)
- ГОРЛУШКИНА  
Наталия Николаевна  
кандидат технических наук, доцент, заведующая кафедрой «Интеллектуальные технологии в гуманитарной сфере» Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»,  
[nagor.spb@mail.ru](mailto:nagor.spb@mail.ru)
- ГРАБКО  
Илья Олегович  
Студент Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный политехнический университет»,  
[ilya4041@yandex.ru](mailto:ilya4041@yandex.ru)
- ГРЕЦЕВ  
Валерий Петрович  
доцент кафедры Федерального государственного казенного военного образовательного учреждения высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного»,  
[vgrescev@yandex.ru](mailto:vgrescev@yandex.ru)
- ДАВЫДОВ  
Александр Викторович  
начальник кафедры Федерального государственного казенного военного образовательного учреждения высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного»,  
[alex\\_dav2001@mail.ru](mailto:alex_dav2001@mail.ru)
- ДВОРЯКОВ  
Виталий Викторович  
кандидат технических наук, доцент военной кафедры Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Московский государственный технический университет радиотехники, электроники и автоматики»,  
[confsut@gmail.com](mailto:confsut@gmail.com)
- ДЕГТЕВА  
Ксения Сергеевна  
студентка группы 53506/10 Федерального государственного образовательного бюджетного учреждения высшего

профессионального образования «Санкт-Петербургский государственный политехнический университет»,  
[ksedeg@yandex.ru](mailto:ksedeg@yandex.ru)

ДЕНИСОВА  
Дарья Александровна

студентка группы 4707 Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», denisovadasha@mail.ru

ДЕРЯБИНА  
Ольга Сергеевна

студентка группы ЗР-22 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [gartemora@hotmail.com](mailto:gartemora@hotmail.com)

ДОРОХОВА  
Екатерина Алексеевна

студентка группы РСО-11 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [kate-d\\_07@rambler.ru](mailto:kate-d_07@rambler.ru)

ДРОБИНЦЕВ  
Павел Дмитриевич

кандидат технических наук, доцент кафедры «Информационные и управляющие системы» института Информационных технологий и управления Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный политехнический университет», [drob@ics2.ecd.spbstu.ru](mailto:drob@ics2.ecd.spbstu.ru)

ДРОБЯСКИН  
Андрей Николаевич

начальник учебной части – заместитель начальника отдела Учебного военного центра Института военного образования Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [dan8@mail.ru](mailto:dan8@mail.ru)

ДЬЯКОВ  
Сергей Вячеславович

доцент кафедры Федерального государственного казенного военного образовательного учреждения высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного», [srgdyakov@rambler.ru](mailto:srgdyakov@rambler.ru)

ЕРЫШОВ  
Вадим Георгиевич

старший преподаватель кафедры Федерального государственного казенного военного образовательного учреждения высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного», [eryshov@mail.ru](mailto:eryshov@mail.ru)

- ЕСАЛОВ  
Кирилл Эдуардович** ассистент кафедры «Инфокоммуникационные системы», начальник Научно-образовательного центра «Исследование проблем инфокоммуникационных технологий и протоколов» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [yesalov@gmail.com](mailto:yesalov@gmail.com)
- ЕФИМОВА  
Елена Викторовна** студентка группы СК-91 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [efimo-ele@yandex.ru](mailto:efimo-ele@yandex.ru)
- ЕФРЕМОВА  
Юлия Сергеевна** студентка группы СК-01, Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Поволжский государственный университет телекоммуникаций и информатики», [7.07.1992@mail.ru](mailto:7.07.1992@mail.ru)
- ЖАДАН  
Олег Павлович** преподаватель кафедры «Многоканальные электропроводные и оптические системы связи» Федерального государственного казенного военного образовательного учреждения высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного», [gadan\\_op@mail.ru](mailto:gadan_op@mail.ru)
- ЖУКОВА  
Дарья Александровна** студентка группы СИС-22м Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [zukovkapro@gmail.com](mailto:zukovkapro@gmail.com)
- ЗАЛИВИНА  
Мария Михайловна** студентка группы СР-12 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [confsut@gmail.com](mailto:confsut@gmail.com)
- ЗАХАРЕНКО  
Татьяна Алексеевна** студентка группы СР-01 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [zakharenko.tatjana2011@yandex.ru](mailto:zakharenko.tatjana2011@yandex.ru)
- ЗОЛОТАРЕВ  
Евгений Витальевич** студент группы ИКТК-19 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский госу-

дарственный университет телекоммуникаций им. проф.  
М. А. Бонч-Бруевича», [mischa.archer@gmail.com](mailto:mischa.archer@gmail.com)

КОЛЕСОВА  
Екатерина Михайловна  
студентка группы ИКТВ-32 Федерального государствен-  
го образовательного бюджетного учреждения высшего  
профессионального образования «Санкт-Петербургский  
государственный университет телекоммуникаций им.  
проф. М. А. Бонч-Бруевича,  
[katya.kolesova2014@mail.ru](mailto:katya.kolesova2014@mail.ru)

КОПП  
Анастасия Ильинична  
студентка магистры группы БИ-33м Федерального госу-  
дарственного образовательного бюджетного учреждения  
высшего профессионального образования «Санкт-  
Петербургский государственный университет телекомму-  
никаций им. проф. М. А. Бонч-Бруевича»,  
[aikopp@mail.ru](mailto:aikopp@mail.ru)

КОПТЯКОВ  
Валерий Владимирович  
студент группы МС-22 Федерального государственного  
образовательного бюджетного учреждения высшего про-  
фессионального образования «Санкт-Петербургский госу-  
дарственный университет телекоммуникаций им. проф.  
М. А. Бонч-Бруевича»,  
[valkoptyakovkop@gmail.com](mailto:valkoptyakovkop@gmail.com)

КОРЖИК  
Валерий Иванович  
доктор технических наук, профессор, профессор кафедры  
«Защищенные системы связи» Федерального государ-  
ственного образовательного бюджетного учреждения выс-  
шего профессионального образования «Санкт-  
Петербургский государственный университет телекомму-  
никаций им. проф. М. А. Бонч-Бруевича»,  
[val-korzhik@yandex.ru](mailto:val-korzhik@yandex.ru)

КОРЧАГИН  
Мстислав Сергеевич  
студент группы ИКТВ-33 Федерального государственного  
образовательного бюджетного учреждения высшего про-  
фессионального образования «Санкт-Петербургский госу-  
дарственный университет телекоммуникаций им. проф.  
М. А. Бонч-Бруевича», [gerl22@list.ru](mailto:gerl22@list.ru)

КОСТРИКОВА  
Юлия Александровна  
аспирант кафедры «Экономика и управление в связи» Фе-  
дерального государственного образовательного бюджетно-  
го учреждения высшего профессионального образования  
«Санкт-Петербургский государственный университет теле-  
коммуникаций им. проф. М. А. Бонч-Бруевича»,  
[ariadnna91@gmail.com](mailto:ariadnna91@gmail.com)

КОТЛЯРОВ  
Всеволод Павлович  
кандидат технических наук, доцент, профессор кафедры  
«Информационные и управляющие системы» института  
Информационных технологий и управления Федерального  
государственного бюджетного образовательного учрежде-  
ния высшего профессионального образования «Санкт-

дарственный университет телекоммуникаций им. проф.  
М. А. Бонч-Бруевича», [jen.zolotarev@gmail.com](mailto:jen.zolotarev@gmail.com)

**ЗОЛОТОВА**  
Татьяна Борисовна

студентка группы ИКТ-304 Федерального государствен-  
го образовательного бюджетного учреждения высшего  
профессионального образования «Санкт-Петербургский  
государственный университет телекоммуникаций им.  
проф. М. А. Бонч-Бруевича»,  
[tatjana.zolotowa2011@yandex.ru](mailto:tatjana.zolotowa2011@yandex.ru)

**ИВАНОВ**  
Сергей Евграфович

Заместитель начальника кафедры Федерального государ-  
ственного казенного военного образовательного учрежде-  
ния высшего профессионального образования «Военная  
академия связи имени Маршала Советского Союза  
С. М. Буденного», [evgrafiy@rambler.ru](mailto:evgrafiy@rambler.ru)

**ИСАКОВ**  
Андрей Алексеевич

аспирант кафедры «Распределенные вычисления и компь-  
ютерные сети» Федерального государственного бюджетно-  
го образовательного учреждения высшего профессиональ-  
ного образования «Санкт-Петербургский государственный  
политехнический университет», [isak239@mail.ru](mailto:isak239@mail.ru)

**КАДАШНИКОВ**  
Самсон Михайлович

студент группы СКВ-93 Федерального государственного  
образовательного бюджетного учреждения высшего про-  
фессионального образования «Санкт-Петербургский госу-  
дарственный университет телекоммуникаций им. проф.  
М. А. Бонч-Бруевича», [samason@yandex.ru](mailto:samason@yandex.ru)

**КАЗАКОВ**  
Сергей Сергеевич

студент группы ИКТС-31 Федерального государственного  
образовательного бюджетного учреждения высшего про-  
фессионального образования «Санкт-Петербургский госу-  
дарственный университет телекоммуникаций им. проф.  
М. А. Бонч-Бруевича», [serega160595@yandex.ru](mailto:serega160595@yandex.ru)

**КАРПЕНКО**  
Максим Викторович

студент Федерального государственного образовательного  
бюджетного учреждения высшего профессионального об-  
разования «Санкт-Петербургский государственный уни-  
верситет телекоммуникаций им. проф. М. А. Бонч-  
Бруевича», [maxer94@mail.ru](mailto:maxer94@mail.ru)

**КАТУНЦОВ**  
Евгений Владимирович

кандидат технических наук, доцент кафедры «Безопасность  
информационных систем» Федерального государственного  
образовательного бюджетного учреждения высшего про-  
фессионального образования «Санкт-Петербургский госу-  
дарственный университет телекоммуникаций им. проф.  
М. А. Бонч-Бруевича», [katuntsov.sut@gmail.com](mailto:katuntsov.sut@gmail.com)

**КВАСОВА**  
Мария Александровна

студентка группы ИСТ-91 Федерального государственного  
образовательного бюджетного учреждения высшего про-  
фессионального образования «Санкт-Петербургский госу-

Петербургский государственный политехнический университет», [vpk@ics2.ecd.spbstu.ru](mailto:vpk@ics2.ecd.spbstu.ru)

КРЫЛОВ  
Александр Сергеевич

студент группы МТ-01 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [www.krylov.pskov-spb@mail.ru](mailto:www.krylov.pskov-spb@mail.ru)

КРЮЧКОВ  
Артём Александрович

студент группы СП-22 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [tomganchos@mail.ru](mailto:tomganchos@mail.ru)

ЛЕ ЧАН  
Дык

студент группы МТ-95 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [letranduc.telecom@gmail.com](mailto:letranduc.telecom@gmail.com)

ЛЕЖЕПЁКОВ  
Антон Сергеевич

студент группы РМ-12 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [anton.lezhepekov@mail.ru](mailto:anton.lezhepekov@mail.ru)

ЛЕЙКИН  
Антон Владиславович

старший преподаватель кафедры «Инфокоммуникационные системы» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [a.v.leykin@gmail.com](mailto:a.v.leykin@gmail.com)

ЛУШНИКОВА  
Татьяна Юрьевна

студентка группы СП-91 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [t.yu.lushnikova@gmail.com](mailto:t.yu.lushnikova@gmail.com)

ЛЮ  
Максим Евгеньевич

студент группы РТ-32 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [maksim.lyu@gmail.com](mailto:maksim.lyu@gmail.com)

МАЛЬЦЕВА  
Ульяна Владимировна

аспирант кафедры «Экономика и управление в связи» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет

тет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[taxav@bk.ru](mailto:taxav@bk.ru)

МЕЛЬНИКОВ  
Сергей Васильевич

кандидат технических наук, доцент, заведующий кафедрой «Специальные средства связи» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [msv0909@yandex.ru](mailto:msv0909@yandex.ru)

МОРЖАКОВ  
Максим Павлович

студент группы ТСС-95 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [drakon.dark@yandex.ru](mailto:drakon.dark@yandex.ru)

МОРОЗОВ  
Максим Александрович

курсант группы 2941 Федерального государственного казенного военного образовательного учреждения высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного», [gadan\\_op@mail.ru](mailto:gadan_op@mail.ru)

МОШАК  
Николай Николаевич

студент группы ИСТ-91 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [mg123mg@mail.ru](mailto:mg123mg@mail.ru)

МУЗЫКАНТОВ  
Алексей Николаевич

заместитель начальника Учебного военного центра Института военного образования Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [muzal@mail.ru](mailto:muzal@mail.ru)

НЕБАЕВ  
Игорь Алексеевич

кандидат технических наук, ассистент кафедры «Обработка и передача дискретных сообщений» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [ingg@radiocoder.net](mailto:ingg@radiocoder.net)

НИКИФОРОВ  
Игорь Валерьевич

ассистент кафедры «Информационные и управляющие системы» института Информационных технологий и управления Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный политехнический университет», [igor.nikiforov@gmail.com](mailto:igor.nikiforov@gmail.com)

- ОРЛОВ Константин Сергеевич** студент группы СП-01 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [kostyaorlov92@gmail.com](mailto:kostyaorlov92@gmail.com)
- ОСИПЕНКО Михаил Михайлович** студент группы ИСТ-341 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [osipenko-mihail@mail.ru](mailto:osipenko-mihail@mail.ru)
- ПАНКИН Андрей Алексеевич** преподаватель кафедры Федерального государственного казенного военного образовательного учреждения высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного», [Andrey85000@yandex.ru](mailto:Andrey85000@yandex.ru)
- ПАРИЦКАЯ Диана Алексеевна** студентка группы Р-05 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [dipari91@gmail.com](mailto:dipari91@gmail.com)
- ПЛОТНИКОВА Елена Вячеславовна** аспирант кафедры «Информатики и компьютерного дизайна» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [E\\_Plotnikova@russia.ru](mailto:E_Plotnikova@russia.ru)
- ПОНОМАРЕВ Иван Сергеевич** студент группы ИСТ-341м Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [ivan15-91@mail.ru](mailto:ivan15-91@mail.ru)
- ПОПОВА Юлия Александровна** студентка группы ИКТ-307 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [popovka\\_95@mail.ru](mailto:popovka_95@mail.ru)
- ПЫРВУ Ирина Филипповна** студентка группы ИКТВ-32 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [irina\\_pyrvu@mail.ru](mailto:irina_pyrvu@mail.ru)

- РАДЧЕНКО**  
Анна Геннадьевна      студентка группы СП-92 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [radanngen@gmail.com](mailto:radanngen@gmail.com)
- РАЗМЁТОВА**  
Ирина Сергеевна      студентка группы МС-22 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [razmetova.irina94@gmail.com](mailto:razmetova.irina94@gmail.com)
- РОГОЗИНСКИЙ**  
Глеб Генрихович      кандидат технических наук, руководитель направления аудиотехнологий Научно-образовательного центра «Медиацентр» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [gleb.rogozinsky@gmail.com](mailto:gleb.rogozinsky@gmail.com)
- РУБИНА**  
Ирина Семеновна      кандидат технических наук, доцент кафедры «Вычислительной техники» Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», [rubren@mail.ru](mailto:rubren@mail.ru)
- САГДЕЕВ**  
Александр Константинович      кандидат технических наук, преподаватель Учебного военного центра Института военного образования Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [brother-aks@yandex.ru](mailto:brother-aks@yandex.ru)
- САМАРКИН**  
Денис Сергеевич      старший преподаватель Учебного военного центра Института военного образования Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [denst2006@yandex.ru](mailto:denst2006@yandex.ru)
- СЕМЕНОВА**  
Елена Евгеньевна      студентка группы 6709 Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский национальный исследовательский университет информационных технологий механики и оптики», [elena.semenova\\_2012@mail.ru](mailto:elena.semenova_2012@mail.ru)

СЕМИЗОРОВ  
Андрей Викторович

курсант группы 1021 Федерального государственного казенного военного образовательного учреждения высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного»,  
[semizorov@mail.ru](mailto:semizorov@mail.ru)

СКАЧКОВА  
Виктория Витальевна

студентка группы МБИ-22м Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[feya.v.kedax@gmail.com](mailto:feya.v.kedax@gmail.com)

СОЛОВЬЕВА  
Александра Владимировна

старший преподаватель кафедры «Информатика и компьютерный дизайн» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[alexandrakhiznyak@gmail.com](mailto:alexandrakhiznyak@gmail.com)

СТАХЕЕВ  
Иван Геннадьевич

кандидат технических наук, доцент Учебного военного центра Института военного образования Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[kisasig@yandex.ru](mailto:kisasig@yandex.ru)

СТАХЕЕВ  
Константин Иванович

студент группы ИКТВ-33 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[kisasig@yandex.ru](mailto:kisasig@yandex.ru)

СТРОЕВА  
Надежда Геннадьевна

студентка группы МТВ-93 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[saffatty1@mail.ru](mailto:saffatty1@mail.ru)

СУРАНОВА  
Марина Александровна

студентка группы ИКТВ-32 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,  
[ya.marinasuranova2014@yandex.ru](mailto:ya.marinasuranova2014@yandex.ru)

ТАРАБАЕВ  
Антон Александрович

студент группы ИКТ-303 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский госу-

дарственный университет телекоммуникаций им. проф.  
М. А. Бонч-Бруевича», [anton200895@mail.ru](mailto:anton200895@mail.ru)

**ТЕМУРОВ  
Амир Арифович** студент группы СК-02 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [amirtemurov@gmail.com](mailto:amirtemurov@gmail.com)

**УШАНОВ  
Станислав Валентинович** студент группы ТСС-17с Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [sc591sv@mail.ru](mailto:sc591sv@mail.ru)

**ФАТЬКИНА  
Елизавета Игоревна** студентка группы СР-91 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [lizzza92@mail.ru](mailto:lizzza92@mail.ru)

**ФЕДОРОВСКИХ  
Олег Игоревич** студент группы СК-02 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [oleg.fedorovskih@gmail.com](mailto:oleg.fedorovskih@gmail.com)

**ФЕОКТИСТОВ  
Валерий Александрович** кандидат военных наук, доцент, старший преподаватель кафедры «Экология и безопасность жизнедеятельности» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [miwaleri@mail.ru](mailto:miwaleri@mail.ru)

**ФИЦОВ  
Вадим Владленович** ассистент кафедры «Инфокоммуникационные системы» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [noldi@bonch-ikt.ru](mailto:noldi@bonch-ikt.ru)

**ФРОЛОВА  
Лариса Владимировна** студентка группы СП-92 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича» [laro4ka.f@yandex.ru](mailto:laro4ka.f@yandex.ru)

**ФРОЛОВА  
Юлия Аркадьевна** студентка группы ИКТВ-33 Федерального государственного образовательного бюджетного учреждения высшего

профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [fr95juli@mail.ru](mailto:fr95juli@mail.ru)

**ХАЙДАКИН**  
Павел Алексеевич

курсант учебной группы Федерального государственного казенного военного образовательного учреждения высшего профессионального образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного», [haidakin@mail.ru](mailto:haidakin@mail.ru)

**ЧАЙМАРДАНОВ**  
Павел Александрович

студент группы МТ-03 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [pchai@yandex.ru](mailto:pchai@yandex.ru)

**ЧЕРКАСОВА**  
Танзила Халитовна

кандидат физико-математических наук, преподаватель Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный политехнический университет», [cherkasova.tnz@yandex.ru](mailto:cherkasova.tnz@yandex.ru)

**ШАЛИН**  
Иван Родионович

студент группы СП-91 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [shalin.ivan@gmail.com](mailto:shalin.ivan@gmail.com)

**ШАНЬГИНА**  
Дарья Александровна

студентка группы СП-02 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича» [lshangina.da@gmail.com](mailto:lshangina.da@gmail.com)

**ШАРАМЫГИНА**  
Анна Алексеевна

студентка группы РСО-31м Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [lickerish@list.ru](mailto:lickerish@list.ru)

**ШАРАФАНОВ**  
Денис Витальевич

аспирант кафедры «Безопасность информационных систем» Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [sharafanov@wesk-group.ru](mailto:sharafanov@wesk-group.ru)

**ШЕВКУНОВ**  
Вячеслав Сергеевич

студент магистратуры Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский наци-

ональный исследовательский университет информационных технологий, механики и оптики»,  
[slava473@mail.ru](mailto:slava473@mail.ru)

ШОЛОХОВ  
Артём Андреевич

студент группы СП-01 Федерального государственного образовательного бюджетного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», [sholokhov\\_aa@gmail.com](mailto:sholokhov_aa@gmail.com)

## АВТОРСКИЙ УКАЗАТЕЛЬ

- Агеев О. Н. **256**  
Алексеев А. Д. **27**  
Алексеева Д. Д. **260**  
Андринов В. И. **31**  
Андринова Е. Е. **138**  
Андрянов А. И. **225**  
Артур Д. К. **14**  
Асеев А. А. **318**  
Барбир О. С. **263**  
Бахолдин А. В. **9**  
Беккер М. А. **267**  
Бенета Э. В. **36**  
Бобрик Ю. В. **231**  
Бондарев В. Ю. **40**  
Бубнова Е. А. **141**  
Бутарев И. Ю. **225**  
Варельджян К. С. **47**  
Васильев Е. В. **52**  
Васильев И. А. **145**  
Виткова Л. А. **31**  
Воинов Н. В. **149**  
Волынкин И. П. **155**  
Воробьев Л. В. **323**  
Воронин С. В. **327**  
Выюговская Н. А. **330**  
Галицкий А. А. **57**  
Галкин А. М. **335**  
Гамиль А. А. **60**  
Гарапова Л. Р. **65**  
Гелль И. А. **272**  
Гехт А. Б. **277**  
Гильдиева О. С. **339**  
Гойхман В. Ю. **69**  
Горлушкина Н. Н. **158**  
Грабко И. О. **162**  
Грецов В. П. **344**  
Давыдов А. В. **351**  
Дворяков В. В. **347**  
Дегтева К. С. **167**  
Денисова Д. А. **158**  
Дерябина О. С. **281**  
Дорохова Е. А. **285**  
Дробинцев П. Д. **149**  
Дробяскин А. Н. **318**  
Дьяков С. В. **344**  
Ерышов В. Г. **351**  
Есалов К. Э. **73**  
Ефимова Е. В. **78**  
Ефремова Ю. С. **84**  
Жадан О. П. **354**  
Жукова Д. А. **89**  
Заливина М. М. **289**  
Захаренко Т. А. **293**  
Золотарев Е. В. **73**  
Золотова Т. Б. **297**  
Иванов С. Е. **344**  
Исаков А. А. **94**  
Кадашников С. М. **335**  
Казаков С. С. **360**  
Карпенко М. В. **236**

- Касперович Д. А. **364**  
Катунцов Е. В. **171**  
Квасова М. А. **175**  
Колесова Е. М. **369**  
Копп А. И. **241, 246**  
Коптяков В. В. **374**  
Коржик В. И. **65**  
Корчагин М. С. **379**  
Кострикова Ю. А. **231**  
Котляров В. П. **149**  
Крылов А. С. **301**  
Крючков А. А. **327**  
Куров Н. П **384**  
Ле Чан Даңк **99**  
Лежепёков А. С. **17**  
Лейкин А. В. **40**  
Лушникова Т. Ю. **69**  
Лю М. Е. **177**  
Мальцева У. В. **252**  
Манвелова Н. Е. **364, 389, 394**  
Мельников С. В. **360**  
Моржаков М. П. **180**  
Морозов М. А. **354**  
Мошак Н. Н. **185**  
Музыкантов А. Н. **318**  
Небаев И. А. **78**  
Никитин Д. Г. **389**  
Никифоров И. В. **149**  
Орлов К. С. **104**  
Осипенко М. М. **189**  
Панихидников С. А. **389, 394**  
Панкин А. А. **351**  
Парицкая Д. А. **22**  
Плотникова Е. В. **193**  
Пономарев И. С. **196**  
Попова Ю. А. **304**  
Пырву И. Ф. **399**  
Радченко А. Г. **108**  
Размётова И. С. **403**  
Рогозинский Г. Г. **5**  
Рубина И. С. **202**  
Рудик С. А. **384**  
Савостина В. А. **339**  
Сагдеев А. К. **330, 379**  
Самаркин Д. С. **408**  
Семенова Е. Е. **207**  
Семизоров А. В. **344**  
Симоненко А. И. **412**  
Скачкова В. В. **112**  
Соловьева А. В. **212**  
Стахеев И. Г. **354, 412**  
Стахеев К. И. **347**  
Строева Н. Г. **408**  
Суранова М. А. **369**  
Тарабаев А. А. **307**  
Темуров А. А. **323**  
Ушанов С. В. **216**  
Фатькина Е. И. **310**  
Федоровских О. И. **323**  
Феоктистов В. А. **374, 403**  
Филиппов К. С. **394**  
Фицов В. В. **47**  
Фролова Л. В. **117**  
Фролова Ю. А. **379**  
Хайдакин П. А. **351**  
Чаймарданов П. А. **125**  
Черкасова Т. Х. **162**  
Шалин И. Р. **130**

Шаньгина Д. А. **133**

Шарамыгина А. А. **313**

Шарафанов Д. В. **221**

Шевкунов В. С. **9**

Шолохов А. А. **104**

Яхункина А. А. **412**

## НАУЧНОЕ ИЗДАНИЕ

68-я региональная научно-техническая конференция  
студентов, аспирантов и молодых ученых  
«Студенческая весна – 2014»

Сборник научных статей конференции

Под редакцией  
Заслуженного деятеля науки РФ,  
доктора технических наук, профессора С. М. Доценко

Составители А. Г. Владыко, Е. А. Аникеевич, Л. М. Минаков  
Литературное редактирование, корректура Е. А. Аникеевич  
Оформление Л. М. Минаков  
Верстка Е. М. Аникеевич

Неисключительные права на все материалы, опубликованные в данном издании принадлежат СПбГУТ.

Все материалы, авторские права на которые принадлежат СПбГУТ, могут быть воспроизведены

при наличии письменного разрешения от СПбГУТ. Ссылка на первоисточник обязательна.

По вопросам приобретения неисключительных прав и использования сборника обращайтесь

по тел. (812) 312-83-79, e-mail: telecomsut@gmail.com

Тип компьютера, процессор, сопроцессор, частота: Pentium IV и выше / аналогичное; оперативная память (RAM): 256 Мб и выше; необходимо на винчестере: не менее 64 Мб; ОС MacOS, Windows (XP, Vista, 7) / аналогичное; видеосистема встроенная; дополнительное ПО: Adobe Reader версия от 7.X или аналогичное. Защита от незаконного распространения: реализуется встроеннымми средствами Adobe Acrobat.

Подписано в печать 30.06.2014. Вышло в свет 30.06.2014.  
Формат 60x90 1/8. Уст. печ. л. 57,875. Заказ № 011-ИТТ-2014.  
Россия, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1.