

Журнал включен в перечень периодических научных изданий, рекомендуемых ВАК Минобрнауки России для публикации научных работ, отражающих основное научное содержание кандидатских и докторских диссертаций и рекомендован УМО по образованию в области телекоммуникаций для студентов высших учебных заведений.

Учредитель

ООО "Издательский дом Медиа Паблшер"

Главный редактор

В.О. Тихвинский

Издатель

С.С. Дымкова

ds@media-publisher.ru

Редакционная коллегия

А.С. Аджемов, А.А. Гоголь, Е.А. Голубицкая,
В.Л. Горбачев, Ю.А. Громаков,
А.И. Демьянов, Б.В. Зверев, Е.П. Зелевич,
Ю.Б. Зубарев, В.Р. Иванов,
Т.А. Кузюкова, В.Н. Лившиц,
С.Л. Мишенков, С.В. Рабовский,
И.В. Парфенов, Ш.Ж. Сеилов,
В.О. Тихвинский, В.В. Фронтов

Редакция

Выпускающий редактор

Андрей Волков

va@media-publisher.ru

Редактор

Наталья Беяева

Отдел маркетинга и PR

Наталья Ременникова,

директор по маркетингу и PR

natrem@media-publisher.ru

Кристина Маркарова,

менеджер по маркетингу и PR

kristina@media-publisher.ru

Ольга Дорошкевич,

менеджер по маркетингу и PR

ovd@media-publisher.ru

Отдел распространения и подписки

info@media-publisher.ru

Предпечатная подготовка

ООО "ИД Медиа Паблшер"

СОДЕРЖАНИЕ

НОВОСТИ

В рубрике представлена информация компаний:

"Энвижн Групп", "Синтерра", "PyCat", Axis Communications, Cisco Systems, Nortel, HP, Yota, МТС, "ВымпелКом", Aladdin, NXP, Intel, Microsoft, "Аэрофлот-Карго"

4

ТЕХНОЛОГИИ

Видеосвязь, дающая конкурентные преимущества вашему бизнесу (по материалам компании Tandberg)

8

Скрынников В.Г.

Предварительная оценка параметров сети UMTS/HSDPA при статическом распределении мощности базовой станции

14

Фокин Г.А.

Особенности функционирования территориально-распределенных самоорганизующихся сетей радиосвязи с адаптивными антенными системами

20

Альтер Л.Ш., Подманков И.И., Свириденко М.В.

Расчет взаимных помех между проектируемыми и действующими радиосредствами на локальном объекте

23

Зелевич Е.П.

Технологии современных систем контроля и управления доступом

26

ЭКОНОМИКА

Артемьева Г.С., Резникова Н.П., Тихвинский В.О.

Позиционирование оператора связи на телекоммуникационном рынке на основе метода Уолша

30

ТРАНСПОРТ

Суслин Ю.И.

Технология структурообразования средств механизации технологического процесса ремонта тележек грузовых вагонов, разработанная НПФ "Промтехника"

38

БЕЗОПАСНОСТЬ

Даннави М.Н.

Последствия воздействия некоторых несанкционированных сообщений ОКС-7 на сети связи общего пользования

42

Годовой отчет Symantec по безопасности MessageLabs Intelligence

45

УСЛУГИ

Степанова И.В., Кондратов А.Г.

Результаты разработки метода расчета пропускной способности сетей подвижной связи

46

Сеилов Ш.Ж., Жуманов Ж.М.

Развитие казахоязычного Интернет-пространства

50

В период с 18 по 20 марта 2009 г. на базе Московского технического университета связи и информатики (МТУСИ) будет проходить
**III Отраслевая научная конференция-форум
“Технологии информационного общества”,
посвященная 150-летию со дня рождения А.С. Попова.**

**Организаторы конференции: МТУСИ, ФГУП ЦНИИС, ФГУП НИИР,
ФГУП НИИ “Восход” и ФГУП ВНИИПВТИ.**

На конференцию приглашены представители регионов России, а также зарубежные участники (в т.ч. из стран СНГ).

Конференция традиционно направлена на объединение усилий отраслевых НИИ, ВУЗов, предприятий и операторов связи для расширения задач по развитию перспективных технологий связи и совершенствованию инфокоммуникационной инфраструктуры регионов России. В ходе конференции также предполагается обсудить проблемы развития науки и определить приоритетные направления научных исследований отрасли.

На конференции будут заслушаны доклады руководителей отрасли, ведущих ученых, специалистов предприятий и ВУЗов связи.

Предполагается проведение работы конференции по следующим научно-техническим направлениям:

- сетевые технологии электросвязи следующего поколения;
- инфокоммуникационные технологии и услуги информационного общества;
- системы цифрового телерадиовещания;
- системы подвижной связи;
- направляющие среды и системы связи;
- цифровые телевизионные технологии и видеоинформатика;
- электродинамика полей и излучателей в системах связи и вещания, распространение радиоволн;
- защита информации и защищенные системы связи;
- идентификационные технологии в телекоммуникационных системах;
- математическое моделирование систем и средств связи;
- системы и аппаратно-программные средства приема и обработки радиосигналов;
- системно-метрологические вопросы информационного общения;
- технологии почтовой связи;
- системы спутниковой связи и вещания;
- подтверждение соответствия современных средств связи;
- компьютерная графика и автоматизированное проектирование;
- математическая стеганография.

В составе конференции-форума будут также работать научно-методические секции.

По результатам конференции будет опубликован сборник трудов, статьи в который должны быть рекомендованы научно-техническими секциями конференции после обсуждения и в ходе их работы.

Полную информацию о конференции можно получить в отделе ИРИС МТУСИ
по тел.: +7 (495) 362-25-25, e-mail: iris@srd.mtuci.ru

УВАЖАЕМЫЕ ЧИТАТЕЛИ

Продолжается подписка на журнал
“Т-Сотт - Телекоммуникации и Транспорт” на 2009 год.

Подписной индекс журнала в агентстве “Роспечать” 80714.

Открыта также подписка через редакцию info@media-publisher.ru

Стоимость подписки: на первое полугодие — 450 руб.; на год — 1050 руб.

Заказ журналов:

- по каталогу “Роспечать” (индекс 80714)
- по каталогу “Интерпочта” (индекс 15241)
- “Деловая пресса” (www.delpress.ru)
- в редакции (info@media-publisher.ru)

Возможен также заказ через региональные альтернативные подписные агентства
<http://www.media-publisher.ru/raspr.shtml>

Периодичность выхода — шесть номеров в год
Стоимость одного экземпляра 150 руб.

Целевая аудитория по распространению

- Телекоммуникационные компании;
- Дистрибьюторы телекоммуникационного оборудования и услуг;
- Контент-провайдеры;
- Разработчики и производители абонентского оборудования;
- Предприятия и организации нефтегазового комплекса;
- Энергетические компании;
- Авто-транспортные предприятия;
- Крупные организации с собственным автомобильным автопарком;
- Компании, занимающиеся железнодорожными, воздушными и морскими перевозками;
- Логистические и экспедиционные компании;
- Провайдеры охранно-поисковых услуг;
- Геодезические и картографические организации;
- Государственные ведомства и организации;
- Строительные компании;
- Профильные учебные заведения

Тираж 5000 экз. + Интернет-версия

Адрес редакции

101990, Россия, Москва,
ул. Авиамоторная, д. 8, корп. 1, офис 209
e-mail: info@media-publisher.ru
Тел.: +7 (495) 957-77-43

Журнал зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия. Свидетельство о регистрации: ПИ № ФС77-27364

Мнения авторов не всегда совпадают с точкой зрения редакции. За содержание рекламных материалов редакция ответственности не несет

Материалы, опубликованные в журнале — собственность ООО “ИД Медиа Паблишер”. Перепечатка, цитирование, дублирование на сайтах допускаются только с разрешения издателя. *All articles and illustrations are copyright. All rights reserved. No reproduction is permitted in whole or part without the express consent of Media Publisher Joint-Stock Company*

Вниманию авторов!

Для начисления авторского гонорара необходимо указать ваши ФИО, почтовый адрес (с индексом), паспортные данные (серия, номер, кем и когда выдан), ИНН, номер свидетельства пенсионного страхования, дату и место рождения, номер телефона.

Плата с аспирантов за публикацию рукописи не взимается

© ООО “ИД Медиа Паблишер”, 2009

www.media-publisher.ru

"Энвижн Груп" и "Синтерра" провели полномасштабную трансляцию для Первого Международного Форума по нанотехнологиям

Компания "Энвижн Груп" и компания "Синтерра", национальный оператор связи, организовали полномасштабную трансляцию в режиме реального времени для Первого Международного Форума по нанотехнологиям, который проходил с 3 по 5 декабря 2008 г. в московском "Экспоцентре".

В мероприятии приняли участие более трех тысяч ученых и бизнесменов из десятка стран, прошли выступления членов правительства, в том числе заместителя Председателя Правительства РФ Сергея Иванова, а также генерального директора РОСНАНО Анатолия Чубайса, и лауреата Нобелевской премии Жореса Алферова. На форуме представлено более 300 проектов в области нанотехнологий начинающих российских исследователей.

В среднесрочной перспективе на развитие нанотехнологий в России планируется потратить 10 млрд. долл.

Для организации мероприятия "Энвижн Груп" организовала полномасштабную он-лайн трансляцию через интернет 12 тематических каналов на русском и английском языках и Wi-Fi связь на всей территории выставки и форума.

Для обеспечения отказоустойчивости решения компанией "Энвижн Груп" был разработан и внедрен программно-аппаратный комплекс с реализацией дублирования и резервирования основных компонентов системы для обеспечения непрерывности трансляции.

Партнерство с компанией "Синтерра" позволило обеспечить мероприятие основным и резервным каналами, связывающими "Экспоцентр" с московским ЦОД компании, и связь сетевого сегмента Интернет-трансляции с сетями нескольких российских и зарубежных провайдеров интернет. Таким образом, была обеспечена возможность просмотра Интернет-трансляции российскими и зарубежными пользователями без наличия "узких мест" в транспортной сети.

"Вычислительный Центр Якутавиа" расширяет спутниковую сеть на базе SkyWire

Оператор спутниковой связи "РyСaт" объявляет о создании первой в России спутниковой сети связи по технологии SkyWire, не требующей строительства центральной земной спутниковой станции (hub). Сеть по заказу ОАО "Вычислительный Центр Якутавиа" создается на основе спутникового модема SkyWire производства компании Radyne (с 2008 г. входит в состав ComTech EF Data, США). Проект телекоммуникационного оснащения объектов авиационного назначения на северо-востоке Якутии планируется завершить в I кв. 2009 г.

На сегодняшний день введены в эксплуатацию две малые земные станции спутниковой связи (МЗССС), расположенные в центральном офисе компании в Якутске и в аэропорту поселка Чукурдах. Пропускная способность канала связи в каждом направлении составляет до 256 кбит/с. Всего в рамках проекта услуги связи будут предоставляться на

основе организованной сети с пропускной способностью 64 кбит/с для авиапредприятий в городе Среднеколымске, поселках Депутатский, Зырянка, Белая Гора, Черский, Нижнеякск.

Специалисты "РyСaт" организовали поставку оборудования со склада в Москве, провели пусконаладочные и инсталляционные работы, обеспечили допуск данных МЗССС к космическому сегменту, организовали и успешно протестировали космический канал связи по направлению Якутск-Чокурдах с использованием спутникового ресурса "Экспресс-АМЗ" (140° в.д.) в период с 24 по 28 ноября 2008 г., сдали станции заказчику для дальнейшей эксплуатации.

Основные преимущества сети, организованной на основе модема SkyWire, — сокращение расходов на строительство центральной станции и более эффективное использование спутникового ресурса за счет исключения из цепочки свя-

зи (VSAT — satellite — центральная станция — satellite — VSAT) одного звена — центральной станции — и сокращения времени задержки сигнала в два раза.

В течение трех лет с начала сотрудничества с "Вычислительным Центром Якутавиа" построена сеть из 25 спутниковых станций по технологии LinkStar для обеспечения услугами связи аэровокзальных комплексов, функционирования системы бронирования и продажи авиационных билетов в Республике Саха (Якутия). Географическое положение и площадь республики более 3000 тыс. км² определяют развитие воздушное сообщение и применение современных спутниковых технологий для предоставления услуг связи бизнесу и частным пользователям. Успешный запуск в эксплуатацию канала связи между Якутском и Чокурдахом стал первым опытом использования новой технологии SkyWire в России, практически сразу же после дебюта на зарубежном рынке.

Сетевая камера с полной поддержкой формата HDTV

Компания Axis Communications представляет сетевую камеру с полной поддержкой формата HDTV (в соответствии со стандартом SMPTE в части разрешения, цветопередачи и частоты кадров). AXIS Q1755, подключенная к монитору с поддержкой HDTV, идеально подходит для обеспечения безопасности мест, где требуются детализированные изображения, например в аэропортах, пунктах паспортного контроля и в казино.

Камера обеспечивает разрешение 1080i или 720 (HDTV), соотношение сторон 16:9 и поддерживает сжатие H.264 или Motion JPEG при максимальной частоте кадров. Наряду с прогрессивной разверткой и эффективной работой в дневном и ночном режиме, она обеспечивает исключительное качество передачи изображений, в том числе быстро движущихся объектов при лю-

бом освещении без размытости изображения. 10-кратное оптическое и 12-кратное цифровое увеличение в сочетании с автоматической фокусировкой обеспечивает четкость просмотра необходимого поля обзора.

Камера оснащена встроенным разъемом для карт памяти SD/SDHC, позволяющим сохранять записи без использования внешнего оборудования. Технология Power over Ethernet (IEEE 802.3af) обеспечивает питание камер через сеть.

AXIS Q1755 обладает интеллектуальными возможностями: усовершенствованные функции обнаружения движения, звука и попыток воздействия на камеру, например ее накрывания или закрасивания распылителем. Камера AXIS Q1755 оснащена новой функцией привратника, автоматически увели-

чивающей масштаб при наличии движения в зоне наблюдения и уменьшающей масштаб по истечении установленного интервала времени. Эта сетевая камера содержит самый современный в отрасли набор возможностей по обеспечению безопасности и сетевому управлению, включая шифрование HTTPS, аутентификацию IEEE 802.1X, поддержку протоколов IPv4 и IPv6, а также функции Quality of Service.

Сетевая камера AXIS Q1755 поддерживается самой большой в отрасли базой ПО для управления видеонаблюдением, созданной партнерами Axis по разработке программных приложений, а также программой AXIS Camera Station. Камера поступит в продажу в январе 2009 г. и будет распространяться через дистрибьюторскую сеть компании Axis.

Ряд крупнейших национальных ЖД-операторов объявили о внедрении GSM-Railway решений от Nortel

Испанская национальная железнодорожная компания ADIF выбрала Nortel для внедрения, эксплуатации и обслуживания системы GSM-R на новой высокоскоростной линии Барселона-Фигуерас. А турецкая строительная компания Yapı Merkezi отдала предпочтение Nortel в качестве поставщика телекоммуникационного решения для магистрали передачи данных на основе сетей GSM-R и SDH в рамках реализации

проекта высокоскоростной железнодорожной магистрали на участке Полатли-Конья. Nortel выпустила решение All-IP Voice Core для железнодорожных операторов на базе платформы ATCA (Advanced Telecommunications Computing Architecture), которое будет развернуто ЖД-операторами в Алжире и Литве.

Компания Nortel уже более 15 лет занимается разработками на основе технологии мобильных коммуникаций

GSM-R. Nortel является ведущим поставщиком решений на основе технологии GSM-R, которыми оснащено 60% из более чем 115 тыс. км линий, использующих эту систему. Nortel имеет контракты по национальным сетям GSM-R в Алжире, Австрии, Франции, Германии, Литве, Алжире и Великобритании и принимает участие в развитии сетей GSM-R в Китае, Чехии, Италии, Индии, Словакии, Испании и Турции.

Nortel и IEEE работают над разработкой нового высокоскоростного стандарта

Компания Nortel разработала экономически эффективную технологию передачи данных по сетям Ethernet со скоростью 100 Гбит/с, которая обеспечит сервис-провайдерам и корпоративным пользователям полосу пропускания необходимую в эпоху Гиперподключенности. Демонстрация передачи 100-гигабитного трафика в сети Ethernet со скоростью 100 Гбит/с на одной длине волны была проведена в научно-исследовательском центре компании Nortel в Оттаве.

Одноканальная оптическая сеть стандарта 100 Гбит/с позволит операторам просто и экономически эффективно обеспечить пропускную способность, в десять раз превышающую возможности стандартных сетей.

Решение Nortel объединяет пропускную способность в 100 Гбит/с со скоростью и простотой сетей Ethernet. На демонстрации были показаны возможности прототипа устройства стандарта 100 Гбит/с, разработанного Nortel при использовании системы

100 GE Development Accelerator System от Ixia для моделирования и контроля трафика в сети.

Для демонстрации как Ixia, так и Nortel использовали сигнал стандарта 100 Гбит/с, соответствующий техническим требованиям IEEE для сети длиной 100 м на физическом уровне. Nortel позволяет осуществлять безошибочную передачу сигнала через единственный оптический модуль передачи данных (OTU4), соответствующий каналу стандарта 100 Гбит/с, который передает данные со скоростью 112 Гбит/сек через 800-километровый оптоволоконный кабель, используя инновационное решение 100G Adaptive Optical Engine.

Ведущее положение компании Nortel в предоставлении широкополосного доступа стандарта 100 Гбит/с возможно благодаря успешному решению 40G/100G Adaptive Optical Engine, которое позволяет поставщикам услуг удовлетворять постоянно увеличивающиеся потребности клиентов в

пропускной способности сети. Решения Nortel стандарта 40 и 100 Гбит/с — это технологии, которые легко внедряются на любых оптических сетях.

В июле 2006 г. при IEEE была создана группа по исследованию возможностей высокоскоростной передачи данных для разработки требований к стандартам сетей Ethernet выше 10 Гбит/с через 3-7 лет. Эта группа пришла к заключению, что необходимо рассмотреть решения стандарта как 100, так и 40 Гбит/с, и подали запрос об утверждении проекта по увеличению скорости Ethernet в соответствии со стандартом IEEE 802.3. После утверждения проекта и планируемых целей в декабре 2007 г. была создана специализированная группа по разработке высокоскоростного стандарта IEEE 802.3ba. На ее совещаниях обсуждаются технические предложения, результатом которых должно стать появление стандарта к 2010 г. Nortel является активным участником специализированной группы IEEE 802.3ba.

Международный аэропорт Квебек модернизирован на базе решений Cisco и HP

С помощью решений компаний Cisco и HP завершена модернизация терминала в расположенном в канадском городе Квебек международном аэропорту имени Жана Лесажа. Развернутая в аэропорту сетевая инфраструктура Cisco® и интегрированные с ней решения для мобильности и унифицированных коммуникаций расширили возможности пользователей и привлекли новых пассажиров.

В этом проекте компания HP выступила в роли комплексного системного интегратора и поставщика услуг технической поддержки для сетевой инфраструктуры. Сотрудничество Cisco с HP помогло внедрить все новые функции менее чем за год.

Ежегодно через аэропорт имени Жана Лесажа проходит более миллиона пассажиров. Каждую неделю оттуда совершается около 400 рейсов в города Северной и Южной Америки и Европы. В ходе подготовки к торжествам, посвященным 400-летию Квебека (прошли летом 2008 г.), в аэропорту была развернута работающая по стандарту 802.11n беспроводная сеть Cisco, которая создала основу для дальнейшей модернизации этого

авиапредприятия в следующих областях:

- **Модернизация обслуживания пассажиров у стоек регистрации.** Мобильные сетевые технологии Cisco и внедренческие услуги HP превратили стойки регистрации в гибкие многофункциональные терминалы, с помощью которых разные авиакомпании могут управлять пассажиропотоком.

- **Совершенствование связи между всеми мобильными сотрудниками аэропорта.** С помощью компании HP аэропорт Квебека развернул проводную и беспроводную сетевую инфраструктуру Cisco с системой Cisco Unified Communications Manager.

- **Бесплатный доступ к беспроводной широкополосной сети Wi-Fi для всех пассажиров.**

Аэропорт Квебека развернул сеть Cisco 802.11n на базе точек доступа Cisco Aironet®1250, чтобы создать основу для поддержки будущих мобильных приложений, способных объединить операции, которые раньше были разрозненными и неэффективными.

- **Регистрация пассажиров и багажа в режиме самообслуживания.** В аэропорту установлены киоски самообслуживания, подключенные к унифицированной беспроводной сети Cisco.

цированной беспроводной сети Cisco. Эти киоски можно свободно перемещать в любую точку аэропорта.

- **Инспекция взлетно-посадочных полос.** В аэропорту испытывается мобильное IP-приложение, собирающее информацию о состоянии покрытия взлетно-посадочных полос и передающее данные в центр управления. Это приложение повысит эффективность связи с пилотами и устранил проблемы, возникающие при передаче данных по переполненным радиоканалам. В результате сократятся задержки в передаче информации пилотам, управляющим воздушными средствами в зоне ответственности аэропорта.

- **Использование наземного оборудования.** Руководство аэропорта Квебека рассматривает возможность использования сети 802.11n для поиска и мониторинга грузовиков, снегоуборочной техники и другого подвижного оборудования.

- **Обработка багажа.** Чтобы сократить случаи потери багажа, аэропорт Квебека планирует установить систему радиочастотной идентификации (RFID), которая позволит отслеживать каждый чемодан или сумку при входе в аэропорт и выходе из него.

Первый российский спорткар подключен к Yota

В декабре 2008 г. в "Новом Манеже" состоялась презентация первого российского серийного спорткара MARUSSIA. Yota, разработчик и поставщик мобильных сервисов, оснастила автомобиль беспроводным быстрым доступом в интернет на базе самой современной технологии связи — 4G.

Спорткар представили известный шоумен и автогонщик, чемпион мира по автогонкам в классе GT, а теперь и автомобильный дизайнер Николай Фоменко и продюсер MARUSSIA Ефим Островский.

Автомобили MARUSSIA российской компании Е.М.М. — радикальная инновация в области серийного автомобилестроения. Ключевые приемы конструктивного дизайна MARUSSIA позволяют на порядки повысить безопасность вождения для пилота и добиться радикального снижения веса автомобиля. Эти инновационные разработки роднят российский автомобиль с болидами "Формулы 1". Однако применение многих технологий в серийном производстве сдерживалось высокими ценами. В новой разработке это препятствие удалось преодолеть, поэтому создатели автомобиля рассчитывают, что спорткар станет доступным обычному покупателю, подобно тому, как перестали быть предметом роскоши мобильные телефоны.

Спорткар оснащен видеокамерами, тремя ЖК-мониторами и другими электронными устройствами. Выход в интернет по технологии 4G обеспечивает Yota. Водителю и пассажирам доступны система навигации и карты, а также такие развлекательные сервисы, как онлайн-музыка и видео. Подключение к интернету поддерживается на скорости до 120 км/ч, а скорость передачи данных достигает 10 Мбит/с, поэтому фильмы и музыку можно не скачивать, а проигрывать онлайн.

Бренд Yota объединяет компании, занимающиеся развитием сети, разработкой собственного программного обеспечения и агрегацией контента.

Дочерние компании "ВымпелКом" в Украине, Узбекистане и Армении внедряют решения Intec

Компания Intec объявила о внедрении биллинговых систем на базе трех дочерних структур компании "ВымпелКом", работающих в Украине, Узбекистане и Армении, ЗАО "Украинские радиосистемы", "Юнител" Узбекистан и "АрменТел" в Армении.

В прошлом году Intec подписала стратегическое групповое лицензионное соглашение с компанией "ВымпелКом", одним из лидирующих операторов мобильной связи на территории России. Это соглашение укрепило статус компании Intec как ведущего поставщика биллинговых систем для межсетевых соединений в России и странах СНГ. На лицензионной территории группы компаний "ВымпелКом" проживает 240 млн. человек, что делает "ВымпелКом" одним из важнейших операторов мобильной связи в мире. Географически, лицензии "ВымпелКом" покрывают 78 регионов России с населением 136,5 млн. человек (94% населения страны). Помимо России, компания "ВымпелКом" предоставляет услуги мобильной связи в Украине, Узбекистане, Армении, Казахстане, Таджикистане и Грузии.

Национальные клиенты МТС

Компания МТС во второй раз победила в конкурсе на право обеспечить мобильной связью Государственную Думу. Новый контракт будет подписан на три года — до конца 2011 г. Госдума является национальным клиентом МТС с 1 января 2008 г.

В настоящее время в МТС статус национального клиента имеют государственные органы власти различных уровней и около 400 компаний, четверть миллиона сотрудников которых во всех регионах РФ ежедневно пользуются в своей работе услугами связи МТС. В число национальных клиентов МТС входят Государственная Дума и Совет Федерации Федерального Собрания РФ, другие государственные ведомства, а также крупнейшие российские и международные корпорации — Роснефть, ТНК-ВР, Alcoa, ВТБ, АвтоВАЗ, WV, Philips, DHL, Metro, Ikea, Еврохим, Nissan и др.

Новая сетевая медиа-платформа Cisco

Компания Cisco анонсировала новую медиаплатформу, которая упрощает прямую трансляцию медиаданных и получение медиаинформации по требованию с помощью персональных компьютеров, мобильных устройств и других цифровых экранных средств. Новая платформа (Cisco Media Processing) автоматически форматирует видео и мультимедиа для просмотра на любом устройстве. Платформа, позволяющая создать контент и затем использовать его на любых устройствах, поддерживает создание медиаинформации в реальном времени, а также ее редактирование, форматирование и распределение по сети в рамках единого сетевого решения.

Первым продуктом в линейке Cisco Media Processing стала модель Cisco Media Experience Engine (MXE) 3000, которая трансформирует контент, поступающий из единого источника, для воспроизведения на любом устройстве.

Renesas и NXP объявляют о лицензионном соглашении на бесконтактную технологию MIFARE

NXP и Renesas Technology Corp. объявили о расширении лицензионного соглашения на технологию NXP MIFARE™. Это соглашение направлено на стимулирование внедрения инновационных систем оплаты и систем с поддержкой технологии Near Field Communication (NFC) в инфраструктуру бесконтактных коммуникаций.

Компания Renesas уже является держателем лицензии MIFARE и теперь получает более широкий доступ ко всему семейству микросхем NXP MIFARE. MIFARE, наиболее распространенная технология бесконтактных коммуникаций в мире, обеспечивает

высочайшие уровни производительности, гибкости и безопасности в области автоматических систем оплаты, контроля доступа, билетных систем и программ лояльности клиентов.

Лицензионное соглашение направлено на поддержку запросов отрасли по расширению возможностей бесконтактных приложений за счет внедрения новых форм-факторов и еще более укрепит глобальные позиции Renesas в области микроконтроллеров с функцией защиты данных, использующихся в hi-end мобильных устройствах и в банковских приложениях, использующих дуальный интерфейс.

Эта модель также поддерживает функции создания и обработки медиаконтента в реальном времени, включая добавление "водяных знаков", редактирование голоса и видео, работу с оверлейными слоями текста и графики и подавление шумов.

Стратегия Cisco в области корпоративных видеотехнологий включает разработку систем и услуг и использование сети как платформы для максимального повышения качества абонентских сетевых видеослужб, доставляемых на различные устройства.

Media Processing — последняя из растущего списка новых технологий Cisco. Эти новаторские технологии, сочетающие новые технологические решения с бизнес-моделями, опира-

ются на богатый опыт Cisco в области IP-сетей. Примерами таких технологий можно назвать Cisco TelePresence, цифровые медиа-системы Cisco DMS и системы физической безопасности. Услуги удаленного управления DMS для Cisco Media Experience Engine включены в число удаленных услуг Cisco Remote Operations Services (ROS). Услуги ROS, доставляемые через сервисный отдел Cisco, помогают заказчикам устанавливать тесно интегрированные комплексные решения с гибкими вариантами обслуживания.

Модель Cisco Media Experience Engine доступна уже сегодня.

Более подробную информацию о ней можно получить на странице www.cisco.com/go/mxe.



ются на богатый опыт Cisco в области IP-сетей. Примерами таких технологий можно назвать Cisco TelePresence, цифровые медиа-системы Cisco DMS и системы физической безопасности.

Услуги удаленного управления DMS для Cisco Media Experience Engine включены в число удаленных услуг Cisco Remote Operations Services (ROS). Услуги ROS, доставляемые через сервисный отдел Cisco, помогают заказчикам устанавливать тесно интегрированные комплексные решения с гибкими вариантами обслуживания.

Модель Cisco Media Experience Engine доступна уже сегодня.

Более подробную информацию о ней можно получить на странице www.cisco.com/go/mxe.

NXP поставляет 100-миллионную микросхему для электронных паспортов

Решения NXP работают более чем в 80% систем электронных паспортов по всему миру, 55 из 67 стран мира используют технологию NXP SmartMX, включая США, Великобританию, Францию, Германию, Турцию и Сингапур.

Целью внедрения биометрических паспортов, впервые представленных в 2004 г, было повышение уровня безопасности в зонах пограничного контроля и обеспечение защиты от подделок и мошенничества. В 2005 г. компания NXP стала первым производителем микросхем, представившим бесконтактный защищенный чип P5CD072к электронным паспортам и

сертифицированный Федеральным Управлением Информационной безопасности Германии в соответствии с требованиями Общего Критерия уровня EAL5+. В продолжение развития своего успеха, в 2007 г. компания выпустила новую микросхему семейства SmartMX (P5CD080), которая стала первой микросхемой в отрасли, получившей сертификацию уровня EAL5+ и полностью поддерживающей спецификацию EAC (Extended Access Control) ICAO. В сентябре 2008 г. NXP выпустила передовую микросхему SmartMX P5CD081. Новый чип установил отраслевой рекорд, обеспечив выполнение операций считывания

данных биометрического паспорта с использованием технологии расширенного контроля доступа (EAC) всего за 3,5 с, с учетом того, что считываемая информация содержала полный набор данных гражданина, включая отпечатки пальцев. Новая микросхема SmartMX стала также первым контроллером для смарт-карт с технологией Secure Fetch™, существенно увеличивающей степень защиты самого чипа.

Эта технология обеспечивает повышенный уровень защиты против атак с использованием излучения и лазеров, способствуя разработке приложений с высоким уровнем безопасности.

Виртуальный офис Cisco "закрывает" на ключ eToken

В комплексе Cisco Virtual Office реализована поддержка eToken для сохранения конфигурации сетевых систем и защищенного мобильного доступа к корпоративным данным.

Получившая широкое распространение концепция *any time, in any place, from any device* (возможность работы сотрудников компании в любое время, в любом месте, с любого устройства) нашла свое отражение в новом комплексном решении технологических партнеров Cisco и Aladdin. Комплекс Cisco Virtual Office (CVO) поддерживает работу с аппаратным средством аутентификации и хранения ключевой информации Aladdin eToken, используемым для сохранения параметров сетевых систем, а также автоматической загрузки и настройки конфигурации CVO. В составе поставки Cisco Virtual Office USB-ключ eToken содержит логотип Cisco.

К структурным компонентам CVO относятся: абонентская станция, центральный узел и соответствующий комплекс услуг, гарантирующий корректную интеграцию, дальнейшую поддержку и оптимизацию решения в процессе эксплуатации. В рамках комплекса CVO на каждой абонентской станции устанавливаются маршрутизаторы Cisco серий 870, 880, 1800, 2800 и 3800 Integrated Services Router (ISR) и IP-телефоны из серии Cisco Unified IP Phones 7900. Центральный узел является соединительным звеном для всех абонентских станций и реализован на базе VPN-маршрутизатора, который выполняет роль конвергентной платформы, объединяющей возможности защищенного соединения с удаленными офисами, централизован-

ное управление политиками, настройками и параметрами идентификационных данных.

Использование на абонентской станции электронного ключа eToken позволяет обеспечить удаленным сотрудникам безопасный доступ к широкому пакету корпоративных сервисов с возможностями их гибкой настройки под свои нужды. Защищенное подключение удаленного сотрудника к корпоративному серверу может быть реализовано, только когда eToken подсоединен к компьютеру или маршрутизатору на абонентской станции. Без такого подключения абонентская станция, через которую мобильный сотрудник получает доступ к необходимым ему ресурсам, не сможет обеспечить защищенное соединение с центральным офисом.

Существует три сценария использования eToken в рамках решения Cisco Virtual Office: в качестве физического носителя, на котором хранятся ключи шифрования RSA, в качестве носителя для настройки удаленного клиента (в этом случае на eToken хранятся RSA-ключи и небольшой файл с настройками CVO), а также для хранения полной конфигурации Cisco Virtual Office.

Первый сценарий является наиболее приемлемым в силу удобства внедрения и простого решения главной задачи: для подключения к CVO нужен только eToken. В этом случае маршрутизатор указанных серий может поставляться сразу вместе с eToken. Благодаря такому комплексу поставки клиент получает готовый к использованию "коробочный" вариант. Кроме того, этот сценарий позволяет эконо-

мить на внедрении.

Второй сценарий предполагает загрузку маршрутизатора с минимальными настройками, достаточными для защищенного соединения с центральным сервером. На eToken сохранены сертификат корневого центра сертификации, ключевая пользовательская пара, конфигурация PSec (для установления защищенного соединения с центральным офисом, механизм синхронизации времени и агент Cisco CNS, который отвечает за обработку событий на уровне ядра Cisco Configuration Engine.

Если же предполагается, что eToken будет использоваться для автонстройки или для хранения всей конфигурации Cisco Virtual Office, то предварительно необходимо скопировать все параметры конфигурации ПО Cisco IOS и цифровые сертификаты в память eToken, используя для этого систему управления средствами аутентификации - Aladdin Token Management System (TMS).

Одна из наиболее привлекательных характеристик использования Cisco Virtual Office совместно с eToken — это полностью автоматизированная настройка "zero-touch setup", позволяющая в автоматическом режиме выполнять установку и настройку параметров сетевых систем, используемых в CVO. Автоустановка позволит компаниям экономно и оперативно распределять своих сотрудников по тысячам удаленных рабочих мест, и при этом быть в полной уверенности в том, что все процессы будут работать корректно и не потребуют услуг технической поддержки.

"Аэрофлот-Карго" выбирает систему CHAMP Cargospot нового поколения

"Аэрофлот-Карго" переходит на Cargospot — новую систему бронирования для грузовых перевозок, поставляемую дочерней компанией SITA

ЗАО "Аэрофлот-Карго", 100% дочернее предприятие ОАО "Аэрофлот", объявило о подписании контракта сроком на 5 лет с CHAMP Cargosystems, мировым лидером в области предоставления IT-решений по управлению грузовыми перевозками на воздушном транспорте. Сотрудничество с CHAMP позволит авиакомпании одной из первых в России приступить к использованию системы нового поколения Cargospot. Данная технология обеспечит полный контроль над продажами и управлением грузовыми перевозками путем интеграции всех соответствующих бизнес-процессов авиакомпании.

Заключение контракта проходит в период проведения программы по обновлению парка самолетов "Аэрофлот-Карго", в соответствии с которой компания планирует в 2009 г. увеличить парк до шести самолетов Mc Donnell Douglas MD-11F и значительно нарастить перевозки грузов на пассажирских рейсах "Аэрофлота".

Система Cargospot, разработанная на базе Java-Oracle, предоставляет широкие возможности по дистрибуции системы через каналы Web-Интернет и доработке системы согласно текущим требованиям ЗАО "Аэрофлот Карго". Персонал компании получит доступ к оперативным и статистическим данным об объемах грузопотоковых перевозок.

Миграцию из действующей системы бронирования проведет CHAMP Cargosystems, что обеспечит бесперебойный переход на новое приложение, включая извлечение и перенос информации с гарантированным сохранением данных и минимальным влиянием на работу компании.

Cisco, Intel и Microsoft — сотрудничество в преобразовании глобальных методов оценки знаний

На Всемирном форуме "Обучение и технология" (Лондон) три ведущие технологические компании анонсировали планы реализации разностороннего исследовательского проекта, нацеленного на поиск новых способов, методов и технологий оценки знаний в современных системах очного обучения для всех стран мира. Проведя обширное исследование, Cisco, Intel и Microsoft сделали вывод о том, что большинство систем образования не успевают за быстро меняющейся экономикой и не дают ученикам необходимых навыков. (Такими навыками принято считать способность к критическому, творческому мышлению, к совместной работе и адаптации к постоянно меняющейся технологии, используемой в быту и на производстве).

Cisco, Intel и Microsoft объявили о назначении доктора наук Барри Макгоу,

директора Мельбурнского института исследований в области образования, исполнителем совместного проекта. Он будет руководить работой исполнительного комитета, проектной группой и группой из 50 ведущих специалистов в области образования и государственного управления, которые займутся совместной разработкой международных и национальных методов оценки знаний учащихся.

Исследовательский проект, который возглавили компании Cisco, Intel и Microsoft, получил поддержку ряда ведущих международных организаций. Так, например, ОЭСР и Международная ассоциация по оценке результатов учебы (IEA) проявили интерес к использованию объективных и проверяемых оценок "навыков XXI века" в новых версиях программы PISA и международных тестов TIMSS, используемых для оценки ма-

тематических и научных знаний.

Группы преподавателей и ученых будут разрабатывать методологии и технологии обучения, создавать эффективную обучающую среду и формировать воспроизводимые методы обучения и оценок с помощью информационных и коммуникационных технологий, стимулирующих развитие навыков, необходимых ученикам для успешной работы. Чтобы ускорить реализацию проекта и получить результаты до выхода в свет новых версий PISA и TIMSS, его участники проанализируют ряд успешных экспериментов по развитию и тестированию навыков XXI в. и рассмотрят возможности широкого распространения полученных результатов.

Информацию о проекте, можно получить у Барри Макгоу (Barry McGow) по адресу: bmcgow@animelb.edu.au.

Видеосвязь, дающая конкурентные преимущества вашему бизнесу

Видеосвязь — это сеанс "живой" связи между людьми, находящимися в разных местах, которым необходимо личное общение, включающее в себя обычную речь, обмен текстовой и визуальной информацией.

В ходе недавних исследований, проведенных Roger ASW и TANDBERG, было установлено, что методы связи, активно используемые бизнесом сегодня — электронная почта и телефон, не являются эффективными и достаточными инструментами для принятия серьезных бизнес-решений (56% бизнесменов считают, что они теряют более 30 минут каждый день, пользуясь неэффективными методами связи). Результаты этого исследования четко указали на то, что в сегодняшнем мире технологий проводной связи "личное" присутствие стало более важным, чем когда-либо.

Видеосвязь обеспечивает доступ к должностным лицам или специалистам, недоступным иным образом. Совместная работа над документами и приложениями в реальном времени сокращает количество согласований и утверждений, значительно ускоряя процесс принятия решений.

Как выбрать поставщика и систему

Существует несколько факторов, которые следует учесть при выборе поставщика оборудования для видеоконференцсвязи:

- стабильные финансовые показатели и оптимальная модель бизнеса;
- успешная история развития компании;
- проверенная временем система обслуживания и поддержки клиентов;
- экономически эффективные программы технического обслуживания;
- прогрессивные методы исследований и разработок;
- соблюдение деловой этики;
- присутствие в различных странах мира
- клиенты довольные качеством оборудования и сервиса;
- комплексное решение.

Важно найти решение, соответствующее требованиям вашего бизнеса. Имеются различные категории систем видеосвязи, и особенно важным является понимание ограничений и преимуществ каждой из них. Компания TANDBERG предлагает полный ассортимент продуктов, следуя принципу "для

каждой ситуации есть свое решение". Например, в удаленном офисе может потребоваться лишь небольшая система, в то время как в головных офисах требуется полнофункциональная, высококачественная система, рассчитанная на большие переговорные комнаты.

При покупке систем видеоконференцсвязи следует учесть:

- системы, которые работают стабильно, без сбоев;
- стандарты, внедренные для обеспечения наибольшей эффективности;
- инновационный инженерный дизайн;
- соответствие сертификату ISO 9002;
- высокий показатель среднего времени между отказами;
- четкий и лаконичный язык меню и интуитивно понятный пользовательский интерфейс;
- простота инсталляции, поддержки и обслуживания систем;
- стандарты, обеспечивающие функциональную совместимость во всем мире;
- нестандартные решения, дающие наивысшее качество звука и видео;



Пользователи технологий визуальных коммуникаций

Вертикальные рынки

Области применения	Преимущества	
Образование	<ul style="list-style-type: none"> • Курсы повышения квалификации • Специальное образование • Дистанционное использование знаний и опыта учителей находящихся далеко • Сотрудничество с другими образовательными учреждениями • Выступления экспертов • Виртуальные путешествия • Тренинги для инструкторов и персонала • Административные совещания 	<ul style="list-style-type: none"> • Связывает удаленные сельские районы с образовательными учреждениями, делая образование доступным всем • Расширяет доступ учреждений и студентов к образовательным ресурсам • Обеспечивает доступ к экспертам-практикам • Дает возможность электронных путешествий по миру • Расширяет возможности учебного плана • Предоставляет возможности для корпоративного обучения и тренинга
Финансы	<ul style="list-style-type: none"> • Сотрудничество - выработка ежедневных стратегий, обмен новостями, информацией о состоянии рынка при максимальной ясности и отсутствии недопонимания • Стратегическое взаимодействие — незамедлительное реагирование на изменения рынка в обстановке ясности и высокой степени доверия • Тактическое взаимодействие — улучшение процесса получения и хранения информации благодаря преимуществам и оперативности видеосвязи • Разработка более эффективных процессов с привлечением большого числа людей, как со стороны, так и собственных сотрудников 	<ul style="list-style-type: none"> • Повышает степень удержания клиентов • Вносит большую ясность в отношения корпоративной культуры, понимание миссии и целей • Улучшает процесс принятия решений и качества сделок • Формирует доверительные отношения и стимулирует работу в команде • Обеспечивает снижение расходов и более высокую маржу операционной прибыли • Создание видеозаписей с конвергенцией данных и связями для передачи речи, видео и данных в реальном масштабе времени
Здравоохранение	<ul style="list-style-type: none"> • Удаленная диагностика пациентов из районов сельской местности • Телеконсультации; использование технологий видеосвязи в ходе традиционного приема у врача • Телемониторинг - позволяет связаться двум медикам для наблюдения процедуры оказываемой пациенту в режиме реального времени и выработки дальнейших медицинских указаний • Административные совещания для связи с персоналом • Курсы повышения квалификации для врачей - обеспечивает общий доступ к специализированной медицинской базе знаний, совместное использование ресурсами и передачу опыта 	<ul style="list-style-type: none"> • Сокращение расходов на транспортировку пациентов • Обеспечение доступа пациентов из сельской местности к специализированным медицинским услугам • Позволяет врачам наряду с контрольной информацией, хранить результаты обследований • Сокращает необходимость проведения лишних исследований • Обеспечивает возможность получения второго мнения в реальном времени по данному пациенту • Сокращает время на диагностику и лечение • Обеспечивает доступ к международным ресурсам
Судебно-правовая область	<ul style="list-style-type: none"> • Изучение документации и вещественных доказательств • Проведение слушания дела • Допрос свидетелей и консультации с экспертами • Взятие показаний у свидетелей и экспертов в особо сложных случаях • Удаленное посещение • Юридические консультации 	<ul style="list-style-type: none"> • Способствует более продуктивному использованию времени • Более эффективное планирование и проведение слушаний • Уменьшает время и расходы на поездку • Обеспечивает доступ к экспертам • Обеспечивает возможность текущей записи заседания для последующего документирования
Производство	<ul style="list-style-type: none"> • Обсуждение дизайна продукта и его корректировка с коллегами • Контроль качества • Удаленный ремонт производственного оборудования 	<ul style="list-style-type: none"> • Дает возможность совместной работы всех сторон • Ускоряет процесс сбора информации • Сокращает простои машинного оборудования • Снижает время вывода на рынок нового продукта • Обеспечивает постоянную обратную связь
Общественная безопасность	<ul style="list-style-type: none"> • Организации по чрезвычайным ситуациям и обеспечению безопасности страны используют видео в зонах бедствий • Органы обеспечения правопорядка используют видеосистемы для создания мобильных полевых командных пунктов • Персонал, отвечающий за военную подготовку, и полевые специалисты проводят учения и брифинги по видео 	<ul style="list-style-type: none"> • Специалисты могут оценить ситуацию и выявить потенциальные угрозы и принять верное решение без потерь времени • Связи с местными больницами и специалистами позволяют оценить состояние раненых и назначить им лечение моментально • Правительственные органы, организации обеспечения безопасности могут делать публичные заявления

Горизонтальные рынки

Маркетинг	<ul style="list-style-type: none"> • Просмотр рекламных текстов и макетов для рекламной компании • Опрос фокус-групп для проведения маркетингового исследования • Запуск новых продуктов 	<ul style="list-style-type: none"> • Ускоряет процесс согласования и утверждения • Позволяет получать оценки и мнения в короткий временной интервал из нескольких точек • Дает возможность вовлекать специалистов, находящихся далеко от офиса
Продажи	<ul style="list-style-type: none"> • Обсуждение ежемесячных результатов, прогнозов и целей • Стратегическое финансовое планирование • Выпуск новых продуктов и программ 	<ul style="list-style-type: none"> • Сокращается время вывода товара на рынок и рост продаж • Улучшается взаимопонимание благодаря визуальному контакту • Снижаются расходы на проведение совещаний и переезды • Транслирование информации о новых продуктах во все точки происходит одновременно • Обеспечивает согласованную и своевременную информацию

TANDBERG И HP

Решение Halo Gateway разработано в рамках программы партнерства компаний TANDBERG и HP, стартовавшего в январе 2007 г. Целью данного партнерства является достижение полной совместимости разработок и решений обеих компаний в области видеосвязи, видеоконференцсвязи и телеприсутствия. В итоге, заказчики получают возможность беспрепятственного видеообщения с использованием всего спектра видеорешений — от студий телеприсутствия HP Halo Collaboration до разнообразных систем ВКС компании TANDBERG для конференц-залов, переговорных комнат и персонального использования. В состав Halo Gateway входят: кодек TANDBERG 6000 MXP, устройство подключения TANDBERG Video Switch, система Halo compositor, сервер HP ProLiant и программное обеспечение, разработанное компанией Hewlett-Packard.

HP и TANDBERG представили также новый комплексный управляемый сервис для пользователей традиционных систем видеоконференцсвязи — HP Halo Video Collaboration Service, а также расширили рамки действующего агентского соглашения. Об этом было объявлено в ходе ежегодной конференции HP Annual Imaging and Printing Conference. Услуга HP Halo Video Collaboration Service позволит значительно улучшить качество и надежность связи, повысить эффективность работы компании и снизить расходы на переезды. Сервис будет поддерживать все системы TANDBERG, включая решения по телеприсутствию, а также видеосистемы других производителей. Видеотерминалы пользователей HP Halo Video Collaboration Service смогут подключаться напрямую к глобальной оптоволоконной сети Halo Video Exchange Network (HVEN), разработанной специально для ВКС. HVEN позволяет легко устанавливать связь между системами разных компаний и не требует распределения ресурсов полосы пропускания, ее зона покрытия охватывает весь мир. Для построения инфраструктуры сети используется технология TANDBERG.

Результатом совместной деятельности HP и TANDBERG стал наиболее полный из представленных на мировом рынке набор продуктов и сервисов для ВКС, помогающих покупателям значительно повысить производительность при экономии ресурсов.

TANDBERG И IBM

Movi для IBM Lotus Sametime позволяет пользователям инициировать видео звонки со своих компьютеров, как через программу коротких сообщений (IM) Sametime, так и через приложения для web-конференций. Movi для IBM Lotus Sametime — это часть общего интеграционного решения, предлагаемого TANDBERG для IBM Lotus Notes и Lotus Sametime. Продукты TANDBERG просты в эксплуатации и безупречно интегрируются в коммуникационные решения IBM.

- многофункциональные продукты по конкурентоспособным ценам;
- системы, оптимизированные как для высокой, так и для низкой пропускной способности;
- программное обеспечение с возможностью обновления;
- характеристики и функциональные возможности.

Стандарты и совместимость

С середины 1990-х гг. Международный союз телекоммуникаций (ITU) определил международные стандарты на видеосвязь. Эти стандарты были созданы для того, чтобы гарантировать совместимость между системами различных производителей. При выборе системы, очень важно гарантировать ее совместимость с этими стандартами и то, что она не предлагает собственный метод связи. Системы, основанные на собственных методах, могут работать лишь с системами той же конструкции. Инвестиции в оборудование для видеоконференций, которое соответствует международным стандартам, гарантирует, что:

- оборудование будет совместимо и восприимчиво к новейшим технологиям;
- инвестиции не окажутся в течение короткого времени вложенными в устаревшие технологии;
- система будет обеспечивать высококачественное изображение при всех скоростях передачи данных и свободно взаимодействовать с другими системами, основанными на промышленных стандартах.

Некоторые системы видеосвязи могут быть совместимы со стандартами ITU и в то же время с другими стандартами. Эти системы могут поддерживать не все характеристики и скорости или предоставлять то же качество изображения в обоих режимах передачи. Важно разобраться, как будет работать система при соединении с оборудованием, изготовленным другой компанией-производителем средств видеосвязи. Эти требования являются первоочередными в случае, если вы хотите обеспечить наивысшее качество соединения со всеми типами систем (все системы компании TANDBERG основываются на стандартах и поддерживают все основные стандарты видеосвязи ITU).

IP H.323 — это стандарт для передачи аудио и видеoinформации, а также данных по IP-сетям (Internet Protocol), который становится все более и более распространенным в среде бизнеса любого масштаба. В особенности, он описывает то, как происходит мульти-

медийное взаимодействие между терминалами, сетевым оборудованием, службами в локальных сетях (LAN), глобальных сетях (WAN) и в сети Internet.

ISDN или цифровая сеть с комплексными услугами — это международный стандарт связи для отправки голосовых, видео- и других данных по цифровым телефонным линиям или по обычным телефонным проводам. Она также известна как BRI — базовый интерфейс обмена. ISDN поддерживает скорости передачи данных, кратные 64 кбит/с (64000 бит/с), и наиболее часто используется физическими лицами и малым бизнесом. Каждая линия ISDN состоит из двух В-каналов (каналов информационного обмена для передачи речи, группового потока данных) и одного D-канала (телеметрического канала). Каждый В-канал может нести до 64 кбит/с данных. PRI — первичный интерфейс обмена — это вид услуг ISDN, разработанный для более крупных организаций. PRI включает в себя 23 В-канала (в Европе — 30) и один D-канал.

Качество связи

Основными факторами, влияющими на качество изображения, являются качество кодека и ширина полосы пропускания.

Видеосвязь опирается на "дискретизацию" и "сжатие" при генерировании изображения и звукового сигнала, которые направляются от одной точки к другой во время сеанса связи. Видеосигнал состоит из большого объема данных. В большинстве случаев, передача всей этой информации не эффективна с точки зрения затрат. Решением является то, что кодек получает видеосигнал на вход и выполняет "дискретизацию" или делает снимки видеосигнала через четко определенные интервалы времени, каждый из которых составляет доли секунды. Кроме того, на выходе видеоданные подвергаются дальнейшей оптимизации при помощи "сжатия". Сжатие снижает дублирование данных, связанных с изображением.

Например, поскольку фоновая информация в типовом конференц-зале изменяется редко, нет необходимости непрерывно передавать снова и снова эту часть изображения. Экономия полосы, не используемую для такой повторяющейся информации, кодек может уделить больше внимания движущимся или изменяющимся элементам, и передать больший объем данных по сети. Если во время сеанса связи имеет место существенное передвижение или изменения, кодек выполняет большой объем обработки данных. Кодек бо-

лее высокого качества лучше обрабатывает движущиеся объекты. Кроме того, кодек отвечает за частоту обновления экрана монитора. Она измеряется количеством кадров в секунду, при этом оптимальное значение составляет 30 кадров/с.

Для успеха видеоконференции особую важность имеет хорошее качество звука. Аудиосистема состоит из различных элементов: микрофон, эхоподавитель, баланс и максимизация доступной полосы частот для аудиоданных относительно видеоданных, а также колонки для воспроизведения звука. Как и во всех других областях видеосвязи, соблюдение международных стандартов является обязательным условием.

Решения TANDBERG по видеоконференцсвязи

Существуют пять самых важных компонентов, которые составляют систему для проведения видеоконференций: камера, микрофон, монитор, динамик и кодек. Камера и микрофон улавливают изображение и звук на одном конце линии. Кодек преобразовывает видео и звук в цифровой сигнал и сжимает его прежде, чем отправить по сети. На другом конце кодек распаковывает сигнал и подает изображение на вход монитора, а звук — на звуковые колонки. Это может звучать сложно, но зритель этого не видит.

Все, что необходимо сделать пользователю, — это набрать номер и нажать "Connect" (установить связь). Комплексное решение TANDBERG предлагает видеосистемы и сетевое оборудование для разнообразных нужд бизнеса и сфер рынка, сохраняя при этом общую платформу. Масштабируемые и гибкие решения способны расти вместе с потребностями сетей для видеосвязи.

Ядром данного решения является TANDBERG Management Suite (TMS). Эта система централизованного управления оборудованием ВКС является основой любой видеосети, базой для наращивания структуры видеоконференцсвязи в рамках организации. TMS позволяет легко добавлять новые устройства и управлять ими, причем устройства могут быть как производства TANDBERG, так и других вендоров. Инфраструктурные продукты TANDBERG созданы для обеспечения интеграции видео с существующей инфраструктурой компании. Они поддерживают полный набор функций видеосвязи, гарантируя безупречное качество видеокommunikаций.

Программное обеспечение TANDBERG для планирования видео встреч позволяет пользователям планировать и проводить со-

вещания с использованием простых и знакомых интерфейсов, включая IBM Lotus Notes® и Microsoft Outlook®.

Мультимедийное качество определило создание платформы MXP TANDBERG. Живой звук и видео, совместное использование презентаций одним нажатием кнопки и расширенные возможности проведения многоточечных конференций — это лишь некоторые из функций, делающих работу с оборудованием незабываемой.

Анализ примеров использования видеосвязи организациями

Видеосвязь преобразовывает мир связи для бизнеса. Эта технология может оказать помощь компаниям в повышении эффективности их работы, а также предоставить стратегические преимущества в конкурентной борьбе. Видеосвязь также оказала сильное воздействие на медицину и образование, улучшив возможности доступа к важнейшим ресурсам, таким как обучение и лечение для тех, кто проживает в отдаленных районах. Внедрение программ интерактивного обучения на расстоянии в учебных заведениях различных стран мира поднимает уровень знаний и объединяет студентов, факультеты и штатных сотрудников, создает атмосферу, способствующую учению, преподаванию, исследовательской работе и управлению учебными заведениями. Успех любого комплекса видеосвязи зависит от высокого качества, надежности и легкости в использовании товаров и услуг, демонстрирующих совершенное качество.

Commerzbank AG — одна из лидирующих европейских компаний на рынке финансовых услуг, активы которой составляют 425 млрд. евро, количество сотрудников 32820 чел., а число клиентов превышает 8 млн. по всему миру. Когда немецкая финансовая корпорация решила сесть на "бескомандировочную диету", используя визуальные коммуникации, выбор был сделан в пользу TANDBERG как единого корпоративного стандарта для всех подразделений. Торговцы акциями и валютой в Лондоне, Франкфурте и Сингапуре, например, сейчас используют систему для видеоконференций целый день, не выключая, для обеспечения координации продаж и покупок в различных временных поясах.

На данный момент Commerzbank установил около трех десятков видеосистем TANDBERG в Европе, Северной Америке, Африке и Азии, заменив старое оборудование других производителей там, где это было необходимо.

TANDBERG И BARCO

Преимущества от интеграции многооконной системы отображения Barco и решений TANDBERG в области видеосвязи высокой четкости получают территориально-распределенные предприятия, углубленно изучающие большие объемы разноформатных данных в режиме реального времени. Такая работа типична для сферы госуправления, нефтегазовой отрасли, автомобилестроения и др. При этом удаленные команды могут видеть полную картину и реагировать как одно целое, а их компетенции могут быть незамедлительно подключены к анализу и обсуждению с помощью любой стандартной видеосистемы через единый интерфейс.

Совместный продукт включает новый кодек телеприсутствия TANDBERG's C90 и камеры высокой четкости, интегрированные с дружественным пользователю комплексом программного обеспечения Barco XDS Control Center. Это многооконное ПО работает на множестве платформ Barco, включая LCD-панели, проекторы, одно- и многоканальные проекционные системы. Последняя и наиболее впечатляющая из них — это однопроекторная десятимегапиксельная система отображения XDC-3000, позволяющая пользователям одновременно визуализировать множество источников информации — каждый в своем разрешении.

TANDBERG И MICROSOFT

ВКС терминалы семейства TANDBERG MXP могут напрямую регистрироваться и проходить авторизацию в Office Communications Server 2007 и, соответственно, — отображаться в списках контактов пользователей Office Communicator 2007. Пользователи этого ПО смогут, просто выбрав имя в списке контактов, установить сеанс видеосвязи с любым устройством TANDBERG MXP, зарегистрированным в Office Communications Server 2007. Для этого необходимо лишь обычный апгрейд встроенного ПО видеосистемы. Также пользователи получают все преимущества единой идентификации, свойственной системе Microsoft Office Communications Server. Например, когда сотрудник находится в офисе, для видеосвязи с ним будет автоматически выбрана настольная видеосистема высокой четкости (HD), а когда он в поездке — web-камера, зарегистрированная в Office Communications Server 2007.

Также, семейство серверов многоточечной видеоконференцсвязи TANDBERG Codian MCU 4500 расширяет модель совместимости видеосистем TANDBERG с Microsoft Office Communications Server 2007, позволяя многоточечным сеансам ВКС, контролируемым TANDBERG MCU, появляться в списке контактов. Это дает возможность пользователям Office Communicator 2007 подключаться к любой стандартизированной видеосистеме. При этом в сеансе ВКС пользователи видеосистем HD будут по-прежнему получать видеоизображение высокой четкости.



Неограниченный доступ к новым доходам



Условный доступ для цифрового вещания. Когда Вы можете предоставить клиенту то, что он хочет, у вас всегда появляется дополнительная прибыль. В течение последних 10 лет Conax предоставлял системы условного доступа для вещателей и производителей контента, защищая и контент, и доходы своих партнеров. Наша технология доказала свою надежность, выгодность и требует минимальных начальных вложений для развертывания системы.



У Conax есть опыт поддержки самых разных бизнес-моделей, в том числе таких прибыльных, как Видео по запросу (VOD), NVOD, трансляции отдельных событий, IPTV, заказа услуг через мобильный телефон и других замечательных новых технологий цифрового телевидения. Войдите в мир условного доступа с Conax и воспользуйтесь преимуществом неограниченных возможностей для нового бизнеса.

Conax – одна из первых компаний, придумавших систему условного доступа. Дух первооткрывателей все еще живет. Сегодня наш опыт и зрелость технологий постоянно превращает новые возможности бизнеса в новые доходы. Основанная на открытых технологиях модульная система Conax'a позволяет вещателям и производителям контента запускать услуги платного ТВ и затем расширять и усложнять их за счет добавления новых компонентов. Подобно нашим клиентам из более чем 70 стран Вы можете открыть для себя новые возможности в бизнесе.

Предварительная оценка параметров сети UMTS/HSDPA при статическом распределении мощности базовой станции

ОПИСАНЫ ОСОБЕННОСТИ РАДИОИНТЕРФЕЙСА HSDPA, ОБУСЛОВЛЕННЫЕ РАСПРЕДЕЛЕНИЕМ ПОЛНОЙ МОЩНОСТИ БАЗОВЫХ СТАНЦИЙ МЕЖДУ СЛУЖЕБНЫМИ ФИЗИЧЕСКИМИ КАНАЛАМИ И ТРАФИКОВЫМИ КАНАЛАМИ HSDPA. ПРИВЕДЕНЫ ТИПОВЫЕ ЗНАЧЕНИЯ ПАРАМЕТРОВ, ОПРЕДЕЛЯЮЩИХ ЭНЕРГЕТИЧЕСКИЙ БЮДЖЕТ КАНАЛОВ CPICH, PDPCH И HS-PDSCH, ПРОИЗВЕДЕНА ОЦЕНКА ПРОПУСКНОЙ СПОСОБНОСТИ ЯЧЕЙКИ HSDPA.



В.Г. Скрынников,
независимый эксперт,
руководитель Рабочей группы
по ЭМС отделения РАЕН

Введение

В [1] были приведены строгие аналитические соотношения между основными параметрами радиointерфейса системы UMTS. Эти соотношения могут служить методологической базой для дальнейших исследований, связанных с планированием радиосетей UMTS и определением требуемых условий электромагнитной совместимости. На основе полученных соотношений были оценены некоторые показатели радиосети UMTS/HSDPA в упрощенной форме лишь для того, чтобы показать, насколько сильная взаимосвязь параметров радиointерфейса отличает планирование радиосетей UMTS от GSM. В свою очередь режим высокоскоростной пакетной передачи данных в UMTS (режим HSDPA) имеет свои характерные отличия от UMTS (Rel'99, Rel'4). К таким отличиям можно отнести: наличие специального нисходящего высокоскоростного канала с мультикодовой передачей данных; отсутствие мягкого хэндовера; постоянство мощности излучения базовой станции ввиду замены быстрой регулировки мощности при HSDPA адаптивным выбором схем модуляции и кодирования совместно с процедурой быстрого запроса повторений пакетов передаваемых данных.

При упрощенной оценке показателей радиосети UMTS/HSDPA в [1] считалось, что вся мощность излучения базовой станции (БС) UMTS выделена для высокоскоростных каналов HSDPA. На самом же деле, вопрос о распределении полной мощности БС между различными каналами радиointерфейса является одним из важных при планировании радиосетей UMTS/HSDPA, особенно, когда

полная мощность базовых станций ограничена по условиям ЭМС.

В продолжение [1] рассмотрены особенности предварительной оценки параметров радиосети UMTS/HSDPA при различном распределении полной мощности базовой станции между конфигурациями каналов UMTS (Rel'99) и HSDPA и ограничениях этой мощности, введенных по условиям электромагнитной совместимости.

Особенности радиointерфейса UMTS/HSDPA. Оборудование радиоподсистемы UMTS, поставляемое сегодня для строительства сетей в России, соответствует Техническим спецификациям 3GPP Rel'5 [4,5]. В соответствии с Rel'5 радиointерфейс UMTS/HSDPA является промежуточным решением и представляет собой комбинацию обычного режима UMTS (Rel'99) и режима высокоскоростной пакетной передачи данных HSDPA. Применительно к рассматриваемой задаче необходимо выделить в данной конфигурации основные физические каналы. В обычном режиме UMTS (Rel'99) организуются общие контрольные каналы доступа в сеть CPICH (Common Pilot Channel), S-SCH (Synchronization Channel), PCCPCH (Primary Common Control Physical Channel), SCCPCH (Secondary Common Control Physical Channel), AICH (Acquisition Indicator Channel), PICH (Paging Indicator Channel) и выделенные каналы: контрольный канал DPCCCH (Dedicated Physical Control Channel) и канал передачи данных DPDCCH (Dedicated Physical Data Channel). Для режима HSDPA организуются специальные каналы: выделенный высокоскоростной канал HS-PDSCH (High-Speed Physical Downlink I Shared Channel) и кон-

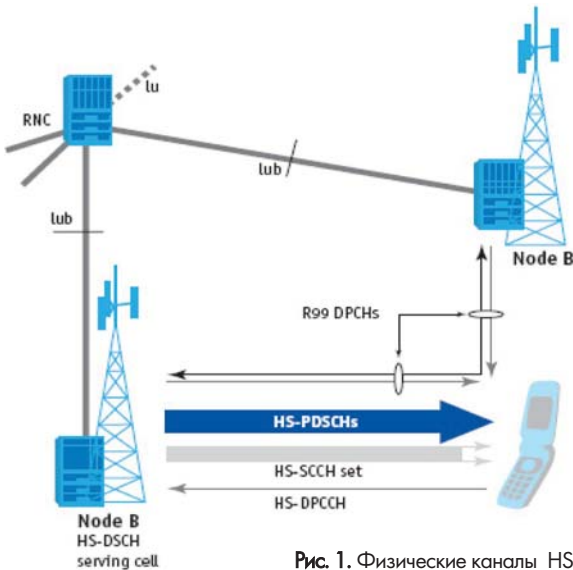


Рис. 1. Физические каналы HSDPA

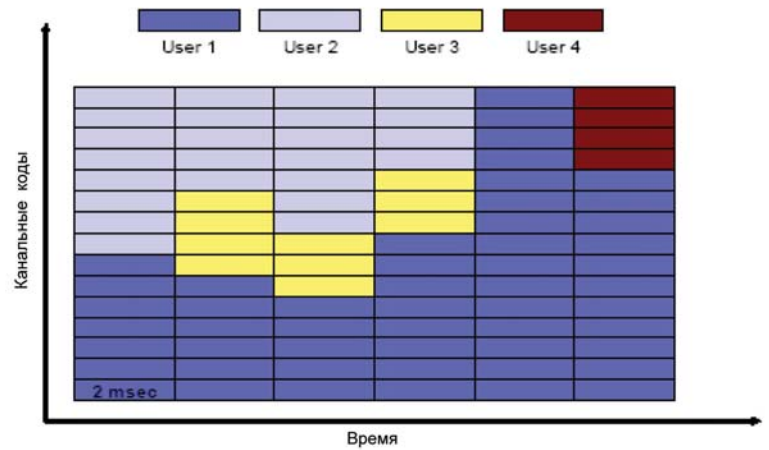


Рис. 2. Мультиплексирование пользовательских данных в канале HS-PDSCH

трольные каналы HS-SCCH (High-Speed Shared Control Channel), HS-DPCCH (High-Speed Dedicated Physical Control Channel), как показано на рис.1.

Нисходящий высокоскоростной канал HS-PDSCH имеет фиксированный коэффициент расширения спектра сигнала (SF), равный 16, что потенциально может обеспечить до 15 пользовательских каналов и один контрольный канал [1]. Наряду с манипуляцией QPSK в канале при хорошем его качестве используется адаптивно модуляция более высокого уровня 16 QAM (16-позиционная квадратурная амплитудная манипуляция). Передаваемые пользовательские данные мультиплексируются по времени на укороченном интервале передачи TTI = 2 мс (TTI – Transmission Time Interval) и далее на каждом TTI подвергаются кодовому мультиплексированию (рис.2).

Дополнительный контрольный канал от абонентского терминала к базовой станции HS-DPCCH служит для передачи информации о состоянии (CQI) нисходящего канала HS-PDSCH и подтверждения приема пакетов данных (ACK/NAK).

Общая характеристика энергетических соотношений при распределении полной мощности БС между режимами. В коммерческих сетях UMTS приоритет одного из режимов UMTS (Rel'99) и HSDPA зависит от планирования их целевого предназначения и в соответствии с этим определяется распределением полной мощности базовых станций между ними. Как было отмечено ранее, HSDPA работает совместно с UMTS (Rel'99) и обе эти схемы должны получать соответствующую требуемую мощность для обязательных общих контрольных и выделенных каналов, рассмотренных выше. Однако следует

иметь в виду, что механизм такого распределения мощности не определен стандартом Rel'5, хотя на практике могут применяться два возможных решения фиксированного и статического распределения (рис. 3а,б).

Динамическое распределение мощности ориентировано на адаптацию к современному рынку, где пока преобладает спрос на речевые и низкоскоростные услуги, и предполагает приоритет режима UMTS (Rel'99), а мощность для HSDPA распределяется по остаточному принципу. Для оценки параметров сетей UMTS/HSDPA логично рассматривать статическое распределение, чтобы получить реальное представление, как о параметрах обычного режима, так и о параметрах HSDPA, при разных соотношениях выделенных мощностей. Соотношения пропускной

способности двух схем (режимов) при различном распределении мощности показаны в табл.1 и на рис. 4 [2].

Особенность энергетических соотношений при распределении полной мощности БС между физическими каналами. В табл. 2 приведены рекомендуемые соотношения мощностей, выделяемых для описанных выше общих контрольных каналов доступа (P1 на рис.3) [2,3].

Особую значимость среди перечисленных контрольных каналов имеет нисходящий пилотный канал CPICH, по которому передается последовательность пилот-символов, в канале отсутствуют информационная модуляция и регулировка мощности, коэффициент расширения SF постоянен и равен 256. Канал не ассоциирован с логическими и транспортными каналами. Выделенная мощность в

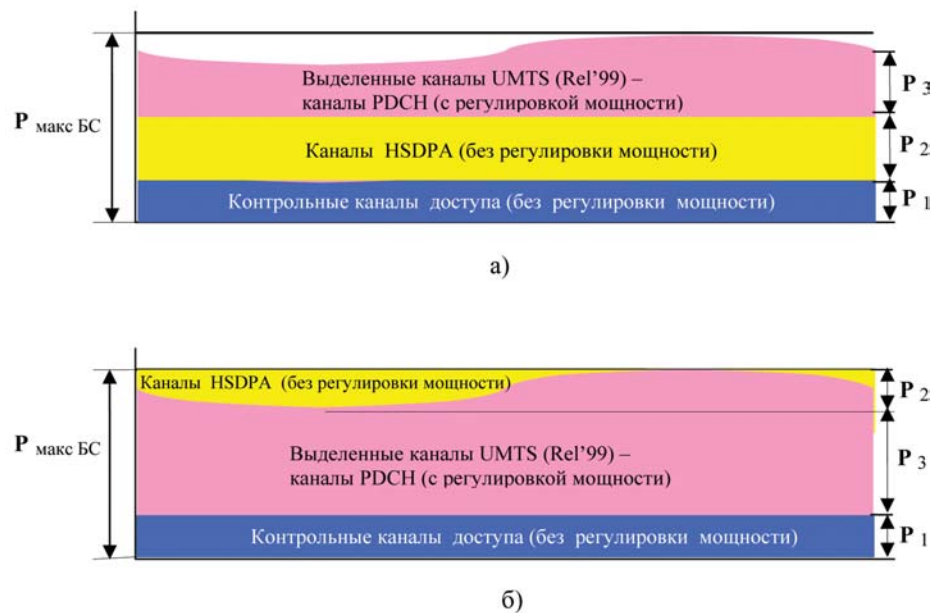


Рис. 3. Распределение полной мощности БС между каналами

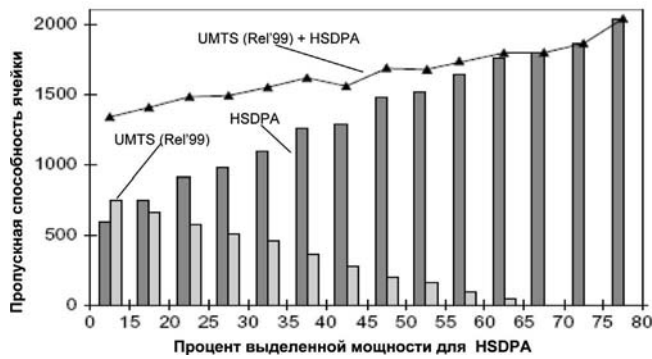


Рис. 4. Соотношение пропускной способности UMTS (Rel'99) и HSDPA

Таблица 1

Пропускная способность UMTS (Rel'99) при разной выделенной мощности для HSDPA

Сервис	Средняя пропускная способность ячейки	Среднее число пользователей в ячейке
20% полной мощности БС выделено для HSDPA		
384 кбит/с (PS)	594.0	1.7
64 кбит/с (PS)	388.9	5.6
64 кбит/с (CS-видео-телефония)		3.7
12,2 кбит/с (AMR)		63.0
50% полной мощности БС выделено для HSDPA		
384 кбит/с (PS)	200.83	0.7
64 кбит/с (PS)	169.12	2.1
64 кбит/с (CS-видео-телефония)		0.8
12,2 кбит/с (AMR)		29.9
80% полной мощности БС выделено для HSDPA		
384 кбит/с (PS)	0.0	0.0
64 кбит/с (PS)	0.0	0.0
64 кбит/с (CS-видео-телефония)		0.0
		0.7

Таблица 2

Распределение мощности БС (20 Вт) между контрольными каналами доступа

Каналы	Типовая мощность, дБм/Вт	Мощность относительно канала CPICH, дБ	Активность использования, %	Среднее значение мощности, дБм/Вт	Комментарии
CPICH	33/2	-	100	33/2	10% от полной мощности БС
SCH	30/1	-3	10	20/0.1	на практике 28-33 дБм
PCCPCH	30/1	-3	90	29,5/0.9	на практике 30-33 дБм
SCCPCH	30/1	0	10	20/0.1	для SF = 128
AICH	27/0.5	-6	-	-	активны только при передаче трафика
PICH	27/0.5	-6	-	-	
Суммарная мощность, Вт				3.1 (15,5%)	

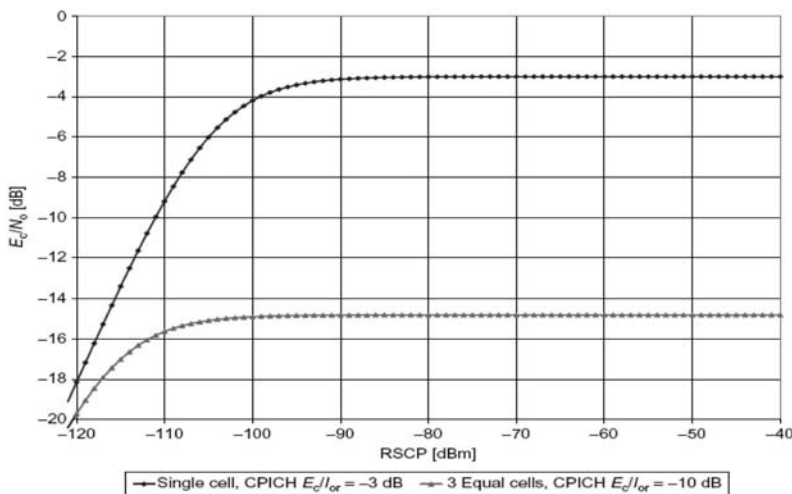


Рис. 5. Зависимость уровня пилот-сигнала в канале CPICH от отношения сигнал/(шум+помеха) на входе приемника AT

канале CPICH остается постоянной и не зависит от передаваемого трафика. Уровень сигнала в канале задает размер зоны покрытия ячейки и в процессе соединения контролируется постоянно абонентским терминалом независимо от режима. По соотношению уровней сигнала в контролируемых каналах CPICH от других ячеек в абонентском терминале принимается решение о мягком хэндовере. Энергетический бюджет CPICH определяется факторами, указанными в табл. 3 [2].

Приведенные параметры характеризуют энергетический бюджет канала CPICH и позволяют по допустимым потерям в радиоканале (поз. (w) в табл. 3) осуществить контроль покрытия зоны обслуживания и оценить условия для мягкого хэндовера при работе в режиме UMTS R'99. Одним из определяющих параметров при этом является минимальный требуемый уровень пилот-сигнала RSCP на входе приемника AT (поз. (n) в табл.3). На его значение влияют ЭИММ передатчика БС в канале CPICH (поз. (f) в табл.3), параметр $CPICH_{loc}/I_{or}=1/Geometry$ (поз. (l) табл. 3), где $Geometry$ — параметр "геометрия ячейки" характеризует распределение мощности БС в определенной точке в пределах зоны обслуживания ячейки, I_{or} — спектральная плотность суммарной мощности каналов всех ячеек, не связанных с абонентским терминалом (не входящих в активный набор) и создающих помеху, I_{or} — спектральная плотность суммарной мощности каналов всех ячеек, связанных с абонентским терминалом в мягком хэндовере (входящих в активный набор), а также отношение $CPICH_{Ec}/No$ энергии принимаемого пилот-сигнала к суммарному помеховому сигналу на входе приемника AT (поз. (m) в табл.3). На рис. 5 показана зависимость параметра RSCP от этого отношения при разной мощности, выделяемой в БС для пилотного канала CPICH (параметр $CPICH_{Ec}/I_{or}$) [2].

В отличие от служебного канала CPICH в трафиковых каналах энергетический бюджет имеет ряд существенных особенностей. Во-первых, бюджет восходящего канала UL зависит от мощности излучения абонентского терминала и планируется для класса терминалов с минимальной мощностью. Следует заметить, что в стандарте UMTS по мощности излучения различают 4 класса терминалов: 1 класс — 33 дБм, 2 класс — 27 дБм, 3 класс — 24 дБм и 4 класс — 21 дБм. Во-вторых, для обычного режима UMTS (R'99) скорость передачи данных в терминале ограничивается при планировании значением 64 Кбит/с, для режима HSDPA — 384 Кбит/с (табл. 4). В-

Таблица 3

Энергетический бюджет канала CPICH

Параметры	Значение	Формула расчета
передатчик БС		
(a) полная мощность БС (P_T)	43 дБм	определена
(b) мощность, выделенная для канала CPICH (P_{CPICH})	33 дБм	определена
(c) $CPICH_{Ec/Ior}$ (P_{CPICH}/P_T)	-10 дБ	(b)-(a)
(d) потери в антенно-фидерном тракте	3 дБ	3 дБ
(e) коэффициент усиления антенны (без учета потерь в фидере)	18 дБ	определен
(f) ЭИИМ передатчика в канале CPICH	48 дБм	(b)-(d)+(e)
приемник АТ		
(g) спектральная плотность тепловых шумов (линейные элементы)	-174 дБм/Гц	определена
(h) полоса пропускания приемника	65,8 дБГц	$10\log(3840000)$
(i) коэффициент шума приемника	7 дБ	определен
(k) мощность теплового шума в приемнике	-101,2 дБм	(g)+(h)+(k)
(l) $CPICH_{Ioc/Ior}$	3 дБ	определено
(m) $CPICH_{Ec/No}$	-14,8 дБ	определено [2]
(n) мин. требуемый уровень пилот-сигнала RSCP	-111 дБм	определен [2]
(o) коэффициент усиления антенны	0 дБ	определен
(p) потери в антенном фидере	0 дБ	определены
(q) усиление и ослабление в антенне	0 дБ	(0)+(p)
радиоканал		
(r) логнормальный фединг	10,3 дБ	определен экспериментально
(s) выигрыш от хэндовера	4,1 дБ	определен экспериментально
(t) ослабление сигнала зданиями	20 дБ	определено экспериментально
(u) ослабление сигнала телом человека (body loss)	3 дБ	определено экспериментально
(v) компонент распространения	29,2 дБ	(r)+(t)+(u)-(s)
(w) допустимые максимальные потери в радиоканале	159 дБ	(f)-(n), включая (v)
(aa) допустимые максимальные потери на трассе распространения сигнала	129,8 дБ	(w)-(v)
(ab) максимальный радиус зоны обслуживания ячейки	0,75 км дБ	модель E-Nata (город)

третьих, энергетический бюджет HSDPA (нисходящие каналы DL) зависит от допустимых максимальных потерь на трассе распространения сигнала в восходящем канале UL (табл. 5). Эти потери определяют возможный размер ячейки для абонентского терминала, который не имеет смысла превышать в каналах DL при двухстороннем соединении. Как было отмечено в [1], энергетический бюджет каналов UL при планировании сетей HSDPA определяет размер зоны обслуживания, а бюджет нисходящих каналов HSDPA — пропускную способность ячейки в пределах этой зоны. При таком планировании размер ячейки в трафиковых каналах необходимо сопоставлять с возможным размером ячейки в канале пилот-сигнала CPICH.

При планировании энергетического бюджета каналов UL должны учитываться коэффициент загрузки сети (как правило, 75%), требуемое отношение сигнал/шум и выигрыш при обработке сигнала для выбранного сервиса (см. табл. 4).

Энергетический бюджет каналов DL при HSDPA характеризуется рядом специфических параметров:

— HSDPA Power Allocation — доля мощности БС, выделенной для режима HSDPA. Суть данного параметра была пояснена выше;

— E_c/N_t — отношение уровня сигнала (энергии чип) к общему уровню внутрисистемных помех и теплового шума. В отличие от UMTS R'99 данный параметр не приводится к скорости передачи данных в конкретном соединении, ибо использование параметра E_b/N_t , описанного ранее в [1], затруднено в силу его зависимости от состояния радиоканала и непрогнозируемого количества перезапросов на повтор передачи, которые используются при HSDPA. В качестве примера на рис. 6 показано соответствие параметра E_c/N_t скорости передачи данных, полученное посредством статистического моделирования [2];

— Operating Margin — некоторый запас энергии, предназначенный для компенсации потерь в радиоканале, связанных с отличиями характера помех от белого шума и повторениями передачи данных. Данный параметр задается, главным образом, требуемым коэффициентом ошибок SPER (Sub-Packet Error Rate). Для выбранной модели канала VA30 (см. табл. 5) параметр имеет значение 1,3 дБ для одной передачи и -2,2 дБ для двух передач [2].

Ранее отмеченный параметр "геометрия ячейки" Geometry остается для HSDPA важным, хотя и имеет особенности. Отсутствие

Таблица 4

Энергетический бюджет трафикового канала UL для HSDPA

Параметры	Значение	Формула расчета
передатчик АТ		
(a) максимальная мощность	21 дБм	определена
(b) потери в антенно-фидерном тракте	0 дБ	определены
(c) коэффициент усиления антенны	0 дБ	определен
(d) ЭИИМ передатчика	21 дБм	(a)-(b)+(c)
приемник БС		
(e) спектральная плотность тепловых шумов (линейные элементы)	-174 дБм/Гц	определена
(f) скорость передачи данных	55,8 дБГц	$10\log(384000) - \text{для } 384 \text{ Кбит/с}$
(g) коэффициент шума приемника	5 дБ	определен
(h) мощность теплового шума в приемнике	-113,2 дБм	(e)+(f)+(g)
(i) коэффициент загрузки сети	75%	определен
(j) превышение шума внутрисистемными помехами в приемнике	6 дБ	определено
(k) требуемое отношение сигнал/суммарная помеха, включая шумы приемника	3,2 дБ	определено [TS 25.101]
(l) выигрыш при обработке сигнала	10 дБ	$10\log(3,84 \cdot 10^6/384 \cdot 10^3)$
(m) чувствительность приемника	-114 дБм	(h)+(j)+(k)-(l)
(n) коэффициент усиления антенны	18 дБ	определен
(o) потери в антенно-фидерном тракте	3 дБ	определены
радиоканал		
(p) логнормальный фединг	10,3 дБ	определен экспериментально
(q) выигрыш от хэндовера	4,1 дБ	определен экспериментально
(r) ослабление сигнала зданиями	20 дБ	определено экспериментально
(s) ослабление сигнала телом человека (body loss)	3 дБ	определено экспериментально
(t) компонент распространения	29,2 дБ	(p)+(r)+(s)-(q)
(u) допустимые максимальные потери в радиоканале	150 дБ	(d)+(n)-(o)-(m), включая (t)
(v) допустимые максимальные потери на трассе распространения сигнала	120,8 дБ	(u)-(t)
(w) максимальный радиус зоны обслуживания ячейки	0,3 км дБ	модель E-Nata (город)

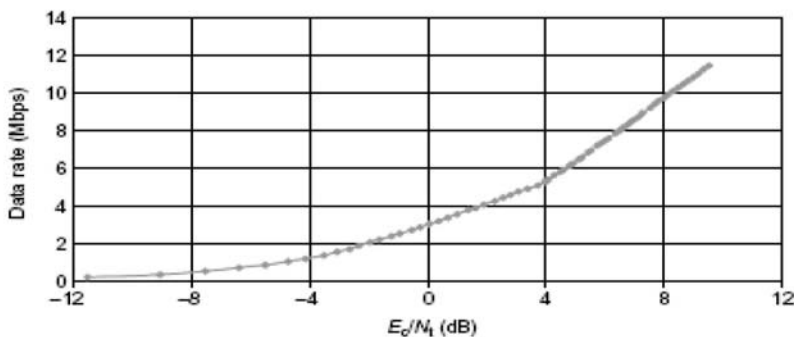


Рис. 6. Соответствие параметра E_b/N_t скорости передачи данных

мягкого хэндовера приводит к более низкой конфигурации ячейки, в особенности в области перехода между смежными ячейками. Это приводит к тому, что деградация этого параметра при переходе к активному набору, состоящему из одной ячейки при HSDPA, по сравнению с UMTS R'99, может составлять до 3 дБ.

С учетом описанных особенностей энергетических соотношений в радиointерфейсе HSDPA произведем оценку параметров сети HSDPA.

Оценка параметров сети HSDPA. Для

оценки параметров сети воспользуемся аналитическими соотношениями и некоторыми исходными данными, описанными в [1]. Исходные данные, особенность которых описана в данной статье, при расчетах были взяты из табл. 5. При планировании сети важно оценить пропускную способность ячейки HSDPA на краю ее зоны обслуживания. Поэтому результаты расчетов, приведенные ниже, соответствуют этому случаю.

1. Максимально допустимое количество пользовательских каналов. Как показано в [1], выражение (13), при выборе конкретных

параметров сети и, прежде всего, вида предоставляемых услуг (требуемого отношения сигнал/шум), вида (модели) радиоканала (параметр α), существует некий предел допустимого количества пользовательских каналов N_d

$$N_o < \frac{1}{(1+i)} \cdot \left[\frac{16}{\alpha \cdot \left(\frac{E_b}{N_o}\right) \cdot v} + 1 \right]. \quad (1)$$

Этот предел обусловлен необходимостью соблюдения энергетического баланса в ячейке и ограничивает возникновение недопустимого уровня внутрисистемных помех, как от собственной ячейки, так и от смежных ячеек, за счет появления в них избыточных пользовательских каналов. Параметром, устанавливающим этот предел, является коэффициент загрузки сети [1]

$$\eta_{DL} = \sum_{j=1}^N \frac{\alpha \cdot (1+i)}{\frac{G_{pj}}{\left(\frac{E_b}{N_o}\right)_j \cdot v_j} + \alpha}. \quad (2)$$

Этот коэффициент характеризует в большей степени превышение на входе приемника абонентских терминалов шума внутрисистемными помехами от пользовательских каналов собственной и смежных ячеек, нежели пропускную способность сети. В этом смысле при планировании сети UMTS η_{DL} задает допустимый уровень внутрисистемных помех в каждой ячейке для планируемых конкретных условий и, следовательно, ограничивает количество пользовательских каналов (см. (1)).

Расчет по формуле (1) проведем для следующих значений исходных параметров: коэффициент ортогональности кода $\alpha = 0,5$, параметр $i = \text{loc}/\text{lor}(1/\text{Geometry}) = 1,25$ (см. табл.5), $E_b/N_o = 6$ дБ (для модели канала VA30 см. табл.5) [4,5], $v=1$ (при передаче данных). Результат расчета — 4 пользовательских канала с суммарной пропускной способностью 4×720 Кбит/с = 2,88 Мбит/с при кодировании данных со скоростью 3/4. Этот результат будет учтен при последующих расчетах.

2. Зависимость суммарной пропускной способности от полной мощности излучения базовой станции. Приведем соотношение (14) [1] в соответствие с логикой данной ста-

Таблица 5

Энергетический бюджет трафикового канала DL для HSDPA

Параметры	Значение	Формула расчета
передатчик БС		
(a) полная мощность БС	43 дБм	определена
(b) доля мощности, выделенной для служебных каналов R'99 (от полной мощности БС)	15,5% (35 дБм)	определены (табл.2)
(c) доля мощности, выделенной для HSDPA (от оставшейся мощности БС)	50% (39,3 дБм)	$10 \log [20 \cdot (1-b) \cdot 0,5]$
(d) доля мощности, выделенной для служебных каналов HS-SCCH (HSDPA) (от мощности, выделенной для HSDPA)	8% (28,3 дБм)	$10 \log [0,08 \cdot (c)]$ определена [2]
(e) доля мощности, выделенной для трафиковых каналов HS-PDSCH (HSDPA) (от мощности, выделенной для HSDPA)	82% (38,9 дБм)	$10 \log [0,82 \cdot (c)]$
(f) потери в антенно-фидерном тракте	3 дБ	3 дБ
(g) коэффициент усиления антенны (без учета потерь в фидере)	18 дБ	определен
(h) ЭИИМ передатчика в каналах HSDPA	53,9 дБм	(e)-(f)+(g)
приемник АТ		
(i) спектральная плотность тепловых шумов (линейные элементы)	-174 дБм/Гц	определена
(j) полоса пропускания приемника	65,8 дБГц	$10 \log (3840000)$
(k) коэффициент шума приемника	7 дБ	определен
(l) мощность теплового шума в приемнике	-101,2 дБм	(i)+(j)+(k)
(m) коэффициент усиления антенны	0 дБ	определен
(n) потери в антенном фидере	0 дБ	определены
(o) усиление и ослабление в антенне	0 дБ	(n)+(o)
радиоканал		
(p) модель канала	VA30	определена
(q) $\text{loc}/\text{lor}(1/\text{Geometry})$	1 дБ	определен [2]
(r) коэффициент ортогональности кода	0,5	определен
(s) Operating Margin	1,3 дБ	определен [2]
(t) допустимые максимальные потери в радиоканале	150 дБ	определены (табл. 4)
(u) допустимые максимальные потери в радиоканале с учетом Operating Margin	148,7 дБ	(t)-(s)

ти, для чего заменим суммарную мощность БС P_{Σ} в данном соотношении суммарной мощностью $P_{\Sigma \text{ HSDPA}}$, выделенной для трафиковых каналов HSDPA (поз. (е) в табл. 5). В соответствии с табл. 5 $P_{\Sigma \text{ HSDPA}} = 0,35 P_{\Sigma}$, следовательно,

$$N = \frac{0,35 \cdot P_{\Sigma} \cdot (1 - \eta_{DL}) G_{BS}}{P_N \cdot L(d)} \cdot \left[\frac{16}{\left(\frac{E_b}{N_0}\right) \cdot v} + \alpha \right], \quad (3)$$

где N — количество пользовательских каналов HS-PDSCH.

Результат расчета по формуле (3), пересчитанные в скорость передачи данных, для используемых выше исходных условий при коэффициенте усиления антенны G_{BS} , равном 15 дБи (с учетом потерь в фидере, см. табл. 5), мощности теплового шума P_N в приемнике, равной минус 101,2 дБм (см. табл.5), допустимых максимальных потерях в радиоканале $L(d)=148,7$ дБ (см. табл. 5) и близком к предельному коэффициенту загрузки ячейки HSDPA $\eta_{DL} = 85\%$ приведен на рис. 7. Представленная на рис. 7 зависимость соответствует случаю, когда "дыхание" соты отсутствует.

3. Зависимость суммарной пропускной способности от распределения мощности для HSDPA. По мере смещения акцента в пользу предоставления в сети UMTS услуг высокоскоростной передачи данных для HSDPA будет выделяться большая часть мощности БС. В данном случае рассматривается характер поведения пропускной способности ячейки от перераспределения мощности БС, оставшейся от общих служебных каналов. Результаты расчета представлены на рис. 8.

Приведенные результаты свидетельствуют о сравнительно низкой пропускной способности на краю ячейки в силу плохой ее "геометрии" ($Geometry = 1$ дБ), в результате чего имеет место значительное помеховое влияние смежных ячеек на абонентский терминал. Следует напомнить, что при HSDPA отсутствует активный набор ячеек (или активный набор состоит лишь из одной собственной ячейки) и все смежные ячейки являются источниками внутрисистемных помех. "Геометрия" ячейки (параметр "Geometry") — есть параметр, обратно пропорциональный параметру i в выражении (2), т.е. $Geometry = 1/i$. Для сравнения на рис. 8 приведена зависимость пропускной способности при несколько лучшей "геометрии" ячейки ($Geometry = -1$ дБ).

Заключение

Полученные результаты позволяют сделать несколько важных выводов.

1. Необходимость перераспределения мощности базовой станции между режимами низкоскоростной (UMTS R'99) и высокоскоростной (HSDPA) передачи данных увеличивает чувствительность сети UMTS/HSDPA к ограничениям мощности излучения БС по условиям ЭМС. Эта чувствительность в большей степени проявляется при преобладании в сети UMTS/HSDPA речевых услуг и услуг низкоскоростной передачи данных.

2. При статическом распределении мощности в интересах HSDPA степень влияния этого распределения на пропускную способность во многом зависит от "геометрии" ячеек, что необходимо учитывать при планировании сетей UMTS/HSDPA.

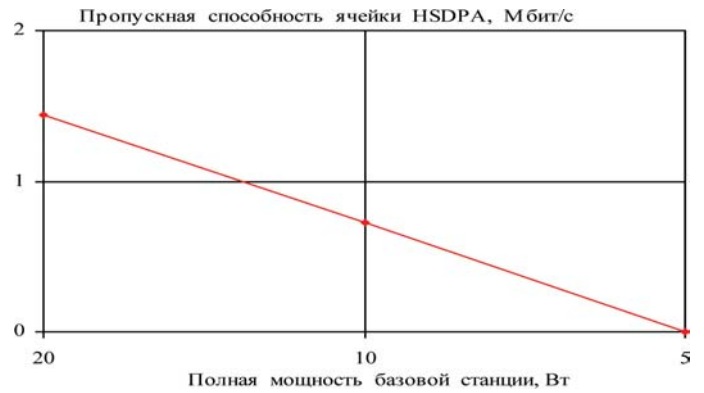


Рис. 7. Зависимость пропускной способности ячейки HSDPA от полной мощности базовой станции

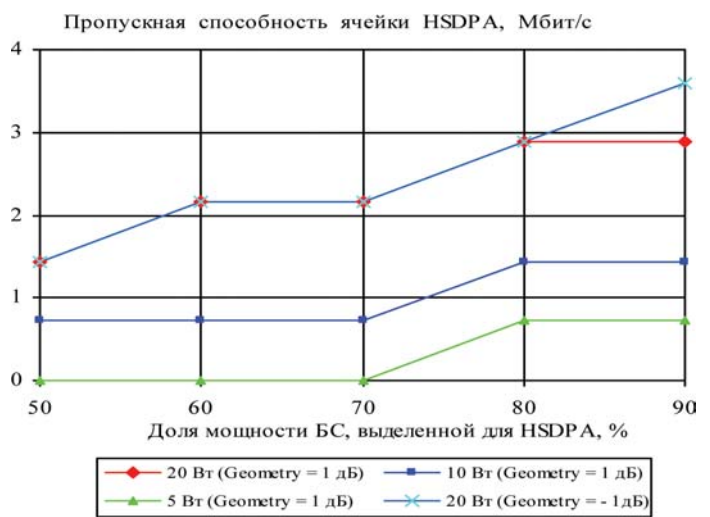
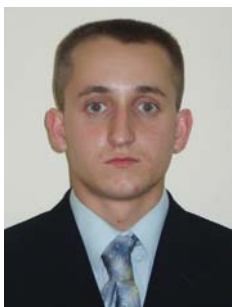


Рис. 8. Зависимость пропускной способности ячейки HSDPA от распределения полной мощности базовой станции

Литература

1. Скрынников В.Г. Предварительная оценка параметров сети UMTS/HSDPA. — Электросвязь. — №3. — 2008.
2. Ch. Chevallier, Ch. Brunner, A. Garavaglia, Kenn P. Murray, Kenneth R. Baker. WCDMA (UMTS). Deployment Handbook. Planning and Optimization. — Wiley, 2006.
3. J. Laiho, A. Wacker, T. Novosad. Radio Network Planning and Optimisation for UMTS. — Wiley, 2002.
4. 3GPP TS 25.104. v.5.9.0 (2004-09). Technical Specification Group Radio Access Network; Base Station (BS) radio transmission and reception (FDD) (Release 5). 2004-09.
5. 3GPP Technical Specification TS25.101 (Release 7), User Equipment (UE) radio transmission and reception (FDD), 2005-12.

Особенности функционирования территориально-распределенных самоорганизующихся сетей радиосвязи с адаптивными антенными системами



Фокин Г.А.,
инженер отдела развития
ОАО "Гипросвязь СПб",
аспирант СПбГУТ

Интерес к распределенным сетям радиосвязи, организованным по принципу "равный с равным" (ad-hoc сеть), зародился во второй половине прошлого века. Главной особенностью этих сетей является децентрализованная схема организации радиосвязи на территории, где использование фиксированной связанной инфраструктуры нецелесообразно или невозможно. На протяжении последних десятилетий интерес к этой проблематике возрастал, о чем свидетельствуют многочисленные публикации [1-4] и формирование рабочей группы MANET (Mobile Ad-hoc Networks) по мобильным ad-hoc сетям в составе специальной комиссии IETF (Internet Engineering Task Force). Масштабы проектов, где востребованы мобильность и сетевая самоорганизация, выросли до уровня локальных (LAN) и городских (MAN) сетей, легко интегрируемых в глобальные сети (WAN).

В настоящее время для построения территориально-распределенных самоорганизующихся сетей радиосвязи используются стандарты IEEE 802.11 (a,b,g), работающие по принципу контроля несущей с предотвращением коллизий CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance). Радиостанции работают со всенаправленными антеннами в общем диапазоне частот на базе технологии TDM (Time Division Multiplex) и ведут передачу в режиме распределенного управления доступом к разделяемой среде DCF (Distributed Coordination Function). Процесс передачи в режиме DCF складывается из обмена четырьмя кадрами: запрос на передачу (RTS), разрешение на передачу (CTS), передача пакета информации (DATA) и подтверждения успешной передачи (ACK).

Недостатком режима DCF в территориально-распределенных самоорганизующихся сетях радиосвязи со всенаправленными антеннами являются известные про-

блемы так называемых "скрытых" и "засвеченных" радиостанций [5]. Их происхождение следует из того, что образование полносвязной территориально-распределенной сети радиосвязи, как правило, невозможно в силу высокого уровня ослабления радиосигнала при распространении радиоволн.

При использовании направленных передач в территориально-распределенных самоорганизующихся сетях радиосвязи с адаптивными антенными системами известные проблемы "скрытых" и "засвеченных" радиостанций приобретают направленный характер [6-8].

Произведем сопоставительный анализ достоинств и недостатков применения адаптивных антенных систем в самоорганизующихся распределенных сетях радиосвязи и определим пути повышения эффективности их использования.

Рассмотрим проблемы направленных передач в режиме DCF на примерах, изображенных на рис. 1. Будем считать, что в режиме приема радиостанции принимают ненаправленно. Допустим, радиостанция А ведет направленную передачу информации радиостанции В. Тогда имеют место следующие ситуации.

"Направленно-засвеченная" радиостанция (рис. 1а). При передаче радиостанцией А информации радиостанции В, радиостанция С попадает в зону обслуживания радиостанции А и будет вынуждена откладывать передачу информации в направлении радиостанции D, хотя это несколько не препятствует радиоприему В.

"Направленно-скрытая" радиостанция (рис. 1б). Радиостанция Е находится вне зоны обслуживания радиостанции А, и считает среду свободной для передачи. Допустим, радиостанция Е начнет передачу в направлении F. В связи с тем, что радиостанция В попадает в зону обслуживания радиостан-

ции E, радиоприем на B будет искажен вследствие коллизии одновременных передач.

Несмотря на рассмотренные выше проблемы, пропускная способность территориально-распределенной самоорганизующейся сети радиосвязи с адаптивными антенными системами в базовом режиме DCF может быть увеличена при определенной ширине ДНА. На рис. 2 представлена зависимость нормированной пропускной способности C от ширины ДНА радиостанции в горизонтальной плоскости Q, при различном числе соседних радиостанций N [9]. Для сравнения пропускной способности направленных и ненаправленных передач на рис. 2 представлена нормированная пропускная способность для случая всенаправленных антенн.

Анализ графиков на рис. 2 позволяет сделать следующие выводы:

1. Без модификации базового режима DCF использование направленных передач позволяет увеличить пропускную способность при ширине ДНА радиостанции $Q < 40^\circ$.

2. С увеличением количества радиостанций-соседей N пропускная способность уменьшается. Это отражает очевидное противоречие между связностью и пропускной способностью: чем больше радиостанций-соседей N находится в зоне обслуживания передающей радиостанции, тем реже ей следует вести передачу для соблюдения зон занятости радиоканала.

В рассмотренных на рис. 1 ситуациях направленных передач в режиме DCF мощность, излучаемая каждой радиостанцией, предполагалась одинаковой.

При использовании адаптивных антенных систем в направлении соседней станции формируется узконаправленный лепесток. При этом:

- Мощность передатчиков и чувствительность приемников концентрируется в более узком луче, и, следовательно, увеличивается дальность радиосвязи.
- Область интерференции одновременных передач уменьшается, и, следовательно, увеличивается пространственная избирательность радиосети.

Если мощность, излучаемая радиостанцией в режиме ненаправленной передачи равна направленно излучаемой мощности, то зоны обслуживания определяются равенством:

$$\frac{1}{d_0^\alpha} = \frac{2\pi}{Q} \frac{1}{d(Q)^\alpha} \quad (1)$$

где d_0 — радиус зоны обслуживания в режиме ненаправленной передачи;

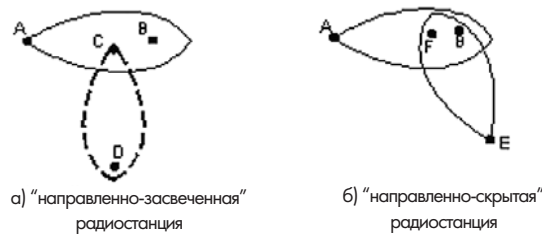


Рис. 1. Ситуации направленных передач в режиме DCF

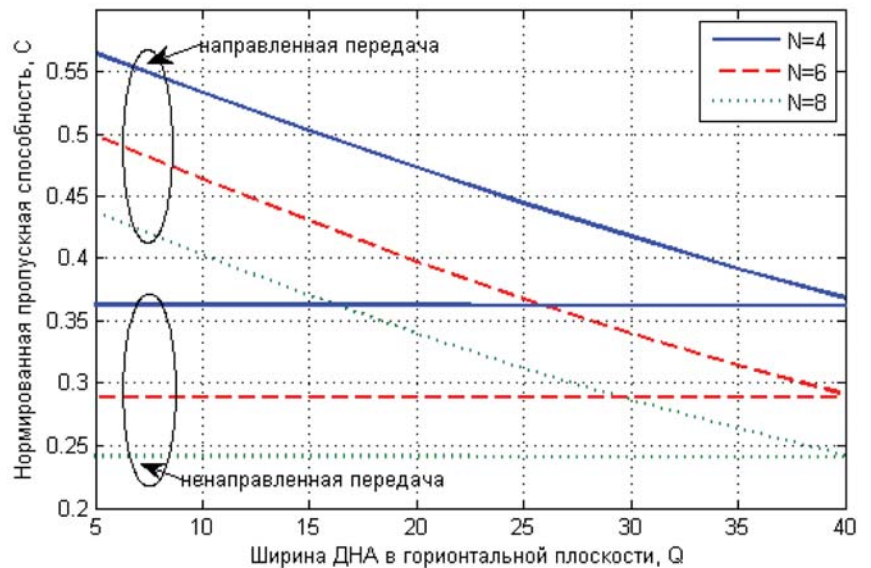


Рис. 2. Зависимость нормированной пропускной способности C от ширины ДНА в горизонтальной плоскости Q



Рис. 3. Преимущества адаптации направления и мощности излучения

$d(Q)$ — дальность зоны обслуживания в режиме направленной передачи;

Q — ширина ДНА в горизонтальной плоскости;

α — показатель затухания.

Из соотношения (1) можно определить дальность зоны обслуживания в режиме направленной передачи:

$$d(Q) = d_0 \left(\frac{2\pi}{Q} \right)^{1/\alpha}. \quad (2)$$

С точки зрения уменьшения зон занятости радиоканала, а, следовательно, повышения пропускной способности, использование одинаковых мощностей приводит к недоиспользованию возможностей пространственной избирательности в разделяемой среде передачи. Оценим возможность уменьшения зон занятости радиоканала за счет управления направлением и мощностью излучения на примерах, изображенных на рис. 3.

Рассмотрим случай, когда $\alpha = 4$, $Q = 10^\circ$. Тогда по формуле (2) можно определить зоны занятости радиоканала S_p , изображенные на рис. 3. Из рис. 3в видно, что при адаптации направления и мощности излучения можно существенно (в десятки раз) локализовать зоны занятости радиоканала,

и, таким образом, увеличить пропускную способность. Дополнительное преимущество управления направлением и мощностью излучения заключается в скрытности радиосредств.

Таким образом, для реализации возможностей пространственной избирательности, предоставляемых адаптивными антенными системами, на уровне доступа к среде передачи радиостанциям следует:

- обнаруживать соседей, число которых не превышает значения N_{\min} , минимально-необходимого для связности радиосети;
- устанавливать в процессе приема кадров запроса на передачу RTS и ответа на передачу CTS такую мощность направленной передачи P_{\min} , которая необходима для радиопокрытия не более одной соседней радиостанции.

Литература

1. M. Sanchez, T. Giles, and J. Zander, CSMA/CA with Beam Forming Antennas in Multi-Hop Packet Radio // in Proceedings of the Swedish Workshop on Wireless Ad Hoc Networks, March 2001.
2. M. Takai, J. Martin, A. Ren, and R. Bagrodia, Directional Virtual Carrier Sensing for Directional

Antennas in Mobile Ad Hoc Networks // in Proceedings of ACM MOBIHOC, Lausanne, Switzerland, June 2002.

3. A. Nasipuri, S. Ye, and R. E. Hiroto, A MAC Protocol for Mobile Ad Hoc Networks Using Directional Antennas // in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), 2000.

4. Y. B. Ko and N. H. Vaidya, Medium Access Control Protocols Using Directional Antennas in Ad Hoc Networks, in Proceedings of IEEE INFOCOM, March 2000.

5. Hekmat R. Ad-Hoc Network: Fundamental properties and network topologies // Springer, 2006.

6. R. Ramanathan, On the Performance of Ad Hoc Networks with Beamforming Antennas // Proceedings of ACM MobiHoc, Long Beach, CA, October 2001.

7. R. R. Choudhury, X. Yang, R. Ramanathan, and N. Vaidya, Using Directional Antennas for Medium Access Control in Ad Hoc Networks // in Proceedings of ACM MOBICOM, Atlanta, Georgia, September 2002.

8. R. Ramanathan, Antenna Beamforming and Power Control for Ad Hoc Networks // Mobile Ad Hoc Networks, IEEE Press, 2004.

9. Y. Wang and J. J. Garcia-Luna-Aceves, Collision Avoidance in Single-Channel Ad Hoc Networks Using Directional Antennas // in Proc. of IEEE Intl. Conf. on Distributed Computing Systems (ICDCS '03), May 2003.



РОССИЙСКАЯ АКАДЕМИЯ ЕСТЕСТВЕННЫХ НАУК ИНФОРМАЦИОННЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ РЕГИОНАЛЬНОЕ ОТДЕЛЕНИЕ

XXIV-я международная конференция "Развитие инфокоммуникационного и информационного права в России, странах СНГ и ЕС"

Российская Академия естественных наук (РАЕН) и его отделение "Информационные и телекоммуникационные технологии" (ИТТ) проводит более 10 лет международные конференции по актуальным вопросам развития инфокоммуникаций с приглашением ведущих ученых и специалистов России, стран СНГ и Европы (www.raenitt.ru).

В период с 8 по 11 апреля 2009 г. в г. Вена (Австрия) в конгресс-центре отеля Parkhotel Schoenbrunn 4*

состоится XXIV-я международная конференция "Развитие инфокоммуникационного и информационного права в России, странах СНГ и ЕС", организуемая ИТТ РАЕН совместно с Ассоциацией региональных операторов связи (АРОС), Ассоциацией CDMA, Казахской академией инфокоммуникаций (КАИ) и ЗАО "Современные Телекоммуникации".

На конференцию приглашены представители МСЭ, Европейского института стандартизации телекоммуникаций (ETSI), ведущих операторов фиксированной, сотовой и беспроводной связи, производители и поставщики программного обеспечения, контента и оборудования NGN/UMTS/WiMAX/DVB-H-T, научных и консалтинговых организаций, инвесторы. В ходе работы секций конференции планируется рассмотреть актуальные аспекты совершенствования телекоммуникационного и информационного права, лицензирования и использования радиочастотного спектра, изменения правового поля в ходе конвергенции сетей и услуг NGN/UMTS/WiMAX и внедрения MVNO в условиях конкуренции между технологиями, вопросы регулирования требований к качеству услуг связи.

Приглашаем Вас принять участие в работе круглого стола и выступить с докладом. Тезисы для публикации в трудах конференции и журнале "Т-Сотт" направляйте в адрес ИТТ РАЕН до 30 марта 2009 г. для Программного комитета конференции vtiir@mail.ru.

Расчет взаимных помех между проектируемыми и действующими радиосредствами на локальном объекте

РАССМОТРЕНА ПРОБЛЕМА ВЗАИМНЫХ ПОМЕХ МЕЖДУ ПРОЕКТИРУЕМЫМИ И ДЕЙСТВУЮЩИМИ РАДИОСРЕДСТВАМИ НА ЛОКАЛЬНОМ ОБЪЕКТЕ (БАШНЕ, ВЫСОТНОМ ЗДАНИИ). ОПИСАНА МЕТОДИКА РАСЧЕТА И ПРОГРАММНЫЙ КОМПЛЕКС, ПОЗВОЛЯЮЩИЕ ВЫЯВИТЬ ИСТОЧНИКИ И ОЦЕНИТЬ УРОВНИ ПОТЕНЦИАЛЬНЫХ ПОМЕХ. РЕЗУЛЬТАТЫ РАСЧЕТОВ ЯВЛЯЮТСЯ ОСНОВОЙ ДЛЯ УСТРАНЕНИЯ ПОМЕХ.

Л.Ш. Альтер,
СПБГУТ,
И.И. Подманков,
М.В. Свириденко,
НПК СвязьСервис

Проблема взаимных помех. Одновременная работа на локальном объекте нескольких десятков радиосредств различных служб (радиовещания и ТВ, систем сотовых, транкинговых, радиорелейных, абонентского радиодоступа) создает условия, при которых излучения передатчиков возбуждают в близкорасположенных приемных антеннах интенсивные мешающие сигналы и, как следствие, ухудшают качество связи.

Несовершенство параметров РЭС и их группирование на локальных объектах (рис. 1), ограниченность частотного ресурса являются причиной возникновения проблемы взаимных межсистемных помех или электромагнитной совместимости (ЭМС) РЭС [1, 2].

При проектировании новой сети связи необходимо оценить возможность появления помех при вводе нового средства и, если необходимо, предусмотреть мероприятия по их



Рис. 1. Размещение антенн на локальном объекте

устранению. Перед специалистами, занимающимися вопросами проектирования, частотно-территориального планирования радиосетей и обеспечения их ЭМС возникают следующие задачи [3]:

- расчет ЭМС проектируемых РЭС с действующими РЭС на объекте;
- выбор частот, свободных от помех (из числа доступных), для проектируемых РЭС;
- определение необходимых частотно-территориальных разнесов антенн РЭС на объекте;
- подбор характеристик антенн;
- выявление групп конфликтующих РЭС на объекте.

Разработанному программному комплексу и методике решения указанных задач посвящена статья.

Параметры РЭС, влияющие на ЭМС, и виды помех. Из-за технического несовершенства передатчиков их спектр излучения, помимо основного, содержит нежелательные (внеполосные, побочные, шумовые и др.) излучения (рис. 2). Приемники, помимо основного канала, имеют большое число неосновных каналов — соседних, побочных (рис. 3). Таким образом, основные и неосновные излучения передатчиков могут создавать помехи по основным и неосновным каналам приемника. Кроме этого, возможно образование нелинейных эффектов блокирования и интермодуляции (рис. 4) при действии мешающих сигналов на вход приемника.

Наиболее распространены помехи:

- а) по основному и соседним каналам приема (СК), которые обусловлены недостаточной прямоугольностью характеристик избирательности приемников (рис. 5, кривая 1), и внеполосными, шумовыми излучениями передатчиков (кривая 2);

- б) по побочным каналам приема (ПК), находящимся за пределами основного канала, в которых помеха проходит на выход приемника (зеркальный канал и др.);

- в) гармонические (ГР), образованные побочными излучениями передатчика на частотах, в целое число раз больших частоты основного излучения;

- г) блокирования (БЛ), которые проявляются в уменьшении полезного сигнала (отношения сигнал/шум S/N) на выходе приемника в результате действия на его входе интенсивного мешающего сигнала, частота которого не совпадает с частотой основного канала приема;

- д) интермодуляции (ИМ) — нелинейный эффект, возникающий при взаимодействии на входе приемника двух или более мешающих сигналов, частоты которых F_1, F_2, \dots не совпадают с частотами основного канала приема, и образующий комбинационные помехи на частотах $F_{им} = |\pm k_1 F_1 \pm k_2 F_2 \pm \dots|$, где k_1, k_2, \dots — целые числа (0, 1, 2, ...). На рис. 4 представлена помеха вида $F_n = F_1 - F_2 + F_3$, где УВЧ, УПЧ — характеристики избирательности усилителя высокой и промежуточной частот.

Критерий образования помехи i -го вида ($i = СК, ПК, ГР, БЛ, ИМ$)

$$P_{пом} > P_{доп.i}$$

где $P_{пом}$ — мощность мешающего сигнала на входе приемника; $P_{доп.i}$ — допустимый уровень мешающего сигнала на входе, создающего помеху i -го вида.

Методика расчетов помех основана на рекомендациях Международного союза электросвязи и отечественных Руководящих документах:

- Рек. МСЭ-R SM.337 "Частотный и территориальный разнос радиосредств";

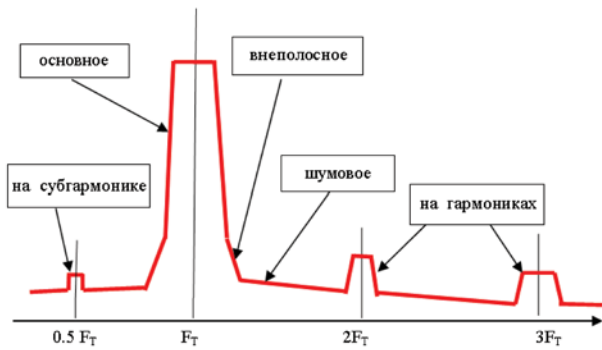


Рис. 2. Излучения передатчика

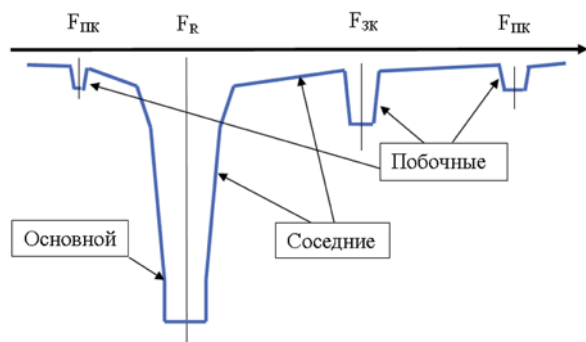


Рис.3. Каналы приемника

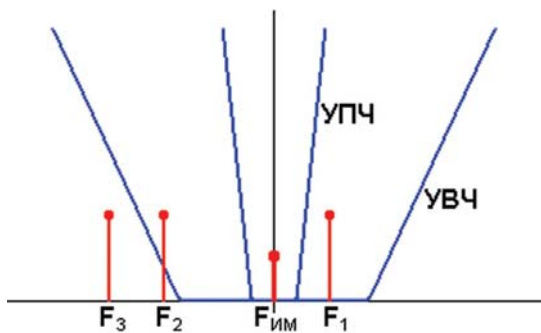


Рис. 4. Помеха интермодуляции от трех передатчиков

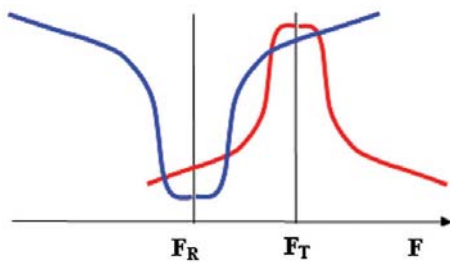


Рис.5. Помеха по соседнему каналу

- Рек. МСЭ-R F.699 "Эталонные диаграммы излучения антенн радиорелейных станций для использования при изучении вопросов оценки помех";
- Рек. МСЭ-R SM.1134 "Расчет помех интермодуляции в сухопутной подвижной службе";
- РД 45.030-99 ОТП на радиорелейное оборудование цифровых магистральных радиорелейных линий ВСС России;
- РД 45.118-99 ОТП на радиорелейное оборудование цифровых внутризоновых радиорелейных линий ВСС России и др.

Процедура расчета помех состоит из формирования всех возможных пар "приемник — мешающий передатчик" и расчета заданных видов помех в каждой паре. Анализ помех каждого вида помех содержит расчет допустимого уровня мешающего сигнала на входе и мощности мешающего сигнала на входе приемника. По результатам сравнения указанных величин делается вывод о наличии (отсутствии) помех для рассматриваемой пары радиосредств. Для помех интермодуляции рассчитываются все возможные пары и тройки мешающих передатчиков: "приемник — два мешающих передатчика", "приемник — три мешающих передатчика".

Мощности помех на входе приемника являются функцией

$$P_{\text{пом}} = \Phi_1(P_T, L_T, G_T(\alpha_T), \Pi_T, \Pi_R, G_R(\alpha_R), L_R, L_0, \text{КОП}),$$

где P_T — мощность мешающего передатчика, L_T — потери в ан-

тенном тракте передатчика, $G_T(\alpha_T)$ — коэффициент усиления антенны передатчика в направлении на "пораженный" приемник, Π_T, Π_R — поляризация полезного и мешающих сигналов, $G_R(\alpha_R)$ — коэффициента усиления антенны "пораженного" приемника в направлении на мешающий передатчик, L_R — потери в антенном тракте приемника, L_0 — потери распространения мешающего сигнала, КОП — коэффициент ослабления помехи (определяемый спектральной маской излучения передатчика и избирательностью тракта приемника).

Допустимые уровни помех являются функцией

$$P_{\text{доп}i} = \Phi_2(P_{\text{РО}}, A_0, S_{\text{ИМ}}, S_{\text{БЛ}}, S_{\text{ПК}}),$$

где $P_{\text{РО}}$ — чувствительностью приемника, A_0 — защитное отношение, $S_{\text{ИМ}}, S_{\text{БЛ}}, S_{\text{ПК}}$ — избирательность приемника по интермодуляции, блокированию, побочному каналу.

Программный комплекс. Для автоматизации расчетов помех разработан программный комплекс, содержащий Справочник типов передатчиков, приемников, а также Справочник РЭС группировки (рис. 6).

Справочник типов РЭС содержит следующие характеристики

- передатчиков — класс излучения, ширина полосы излучения на уровнях -3, -30 и -60 дБ относительно нулевого уровня, ослабление побочных излучений;
- приемников — реальная чувствительность; защитное отношение по входу; полосы пропускания МШУ, УВЧ, УПЧ, модема на уровнях -3, 30 и -60 дБ; избирательности по соседнему, побочным каналам приема, блокированию и интермодуляции; промежуточная частота и вид настройки гетеродина.

Характеристики оборудования, использованные в справочнике типов РЭС, приводятся в: 1) в форме № 1 ГКРЧ; 2) Руководящих документах; 3) нормативных документах, регламентирующих параметры ЭМС (в т.ч.



Рис. 6. Состав программного комплекса

Нормы 19-02); 4) отраслевых стандартах на оборудование; 5) ТУ на оборудование.

Справочник РЭС группировки включает следующие характеристики

- приемника — наименование и тип РЭС, частота приема, потери в фидере, тип антенны и ее высота установки, азимут, угол места;
- передатчика — наименование и тип РЭС, частота передачи, потери в фидере, тип антенны и ее высота установки, азимут, угол места.

Главное окно и вкладки результатов расчетов помех СК приведены на рис. 7.

Комплекс предназначен для работы в среде WINDOWS NT4.0 / 2000 / XP. Для комфортной работы необходимо одно из приложений: Excel из пакета MS Office или Calc из пакета OpenOffice. Приложение необходимо для подготовки файлов Справочников, используемых программой, а также для просмотра и обработки результатов расчетов, сохраненных в формате *.csv-файлов.

С помощью специального редактора можно производить расчет для всех РЭС группировки или только выделенных РЭС. Для подготовки исходных данных можно использовать электронные таблицы Microsoft Excel с файлами разделенного текстового формата (CSV) а так же экспорт результатов расчета из программы анализа в Microsoft Excel через файлы CSV-формата.

Управление работой программы осуществляется в интерактивном режиме через диалоговые окна. Программа позволяет управлять условиями расчета помех и порядком сортировки результатов расчетов.

Выходные данные представляют собой таблицы для каждого вида помех. В таблицах указываются параметры пораженного приемника, параметры мешающего передатчика (двух, трех передатчиков для помех интермодуляции), а также величину превышения уровня мешающего сигнала относительно допустимого уровня на входе приемника.

Устранение потенциальных помех решается путем применения комплекса организационных и технических мероприятий [1-3]. Организационные мероприятия, связанные с правильным учетом технических параметров средств, влияющих на обеспечение ЭМС, включают выбор рабочих частот (при которых исключаются взаимные помехи) радиосредствам из набора возможных, установление необходимых частотных и/или территориальных разносов РЭС, поляризационных развязок между антеннами радиосредств и др. Технические мероприятия направлены на ослабление помех в источниках (например,

дополнительные фильтры на выходах), на защиту приемников (например, применение дополнительных фильтров на входе). Расчеты, выполненные с помощью комплекса, являются основой для разработки мероприятий по устранению помех.

Пример расчета. На объекте расположены РЭС различных служб (ТВ, подвижной, фиксированной), в т.ч. базовая станция подвижной службы диапазона 450 МГц (СПС-450), передатчик которой имеет следующие параметры: $F_T = 455$ МГц, $L_T = 3$ дБ, вибраторная антенна установлена на высоте $h_{aT} = 41$ м, $G_T = 6$ дБи.

Планируется установить БС стандарта CDMA-450, приемник которой имеет следующие параметры: $F_R = 453,975$ МГц, $L_R = 3$ дБ, секторная антенна установлена на $h_{aR} = 50$ м, $G_R = 13$ дБи.

Расчет ЭМС проектируемой БС и действующих РЭС выявил помеху по соседнему каналу (рис. 7), образованную воздействием излучения передатчика СПС-450 на приемник БС CDMA-450. Уровень помехи превышает допустимый уровень ($P_{изб}$) на 5,4 дБ. Увеличение разноса антенн по высоте ($h_{aT}^* = 60$ м) устранило помеху $P_{изб} = -1,0$ дБ.

Заключение

При большой концентрации радиосредств на локальном объекте могут образовываться недопустимые взаимные помехи. В

связи с этим при проектировании радиосетей необходимо производить расчет взаимных помех между проектируемыми и действующими радиосредствами. При этом необходимо учитывать помехи по основному и соседним каналам приема от основных, внеполосных, побочных излучений мешающих передатчиков по основному, соседним и побочным каналам приема приемника, а также помехи блокирования и интермодуляции.

Такой расчет позволит заранее выявить возможные помехи и, при необходимости, используя результаты расчетов, предусмотреть меры по их устранению.

Разработанный программный комплекс обеспечивает автоматизацию расчетов. По заданиям проектных организаций и операторов он использовался для 45 объектов, на которых проектировались РЭС, системы сотовые и абонентского доступа в различных городах России, и показал свою эффективность.

Литература

1. А. Л. Бадалов, А. С. Михайлов. Нормы на параметры электромагнитной совместимости РЭС//Справочник. — М.: Радио и связь, 1990.
2. А. Д. Князев. Элементы теории и практики электромагнитной совместимости радиоэлектронных средств. — М.: Радио и связь, 1984.
3. А.Х. Коновалов, Г.З. Рубин. Вопросы объектовой электромагнитной совместимости при проектировании сетей подвижной радиосвязи. ГСПИ РТВ. <http://www.gspirtv.ru/content/view/40/33/>

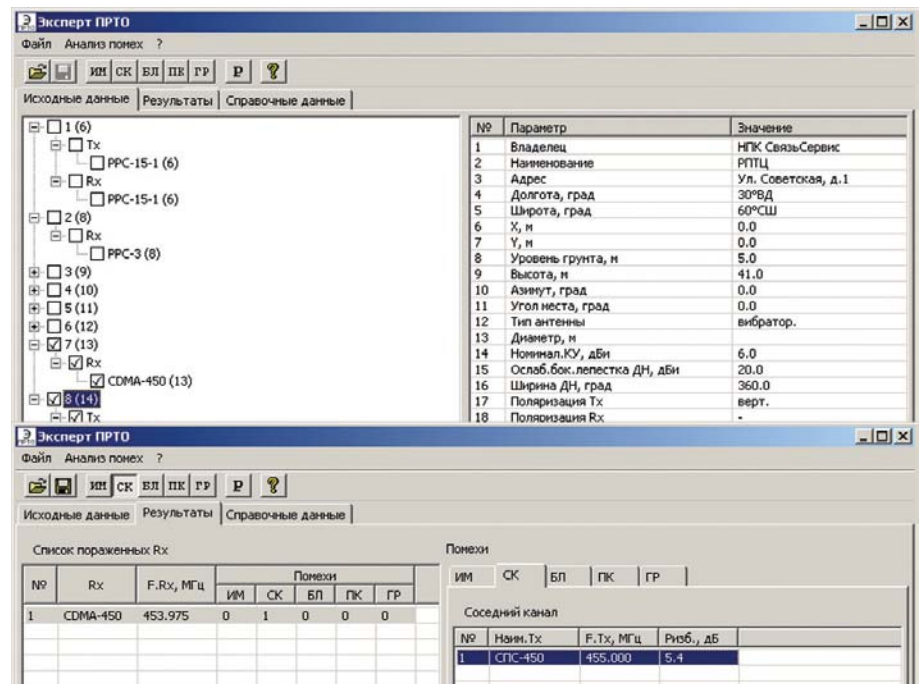


Рис. 7. Главное окно и вкладка Результаты СК

Технологии современных систем контроля и управления доступом



Зелевич Е.П.,
профессор МТУСИ

Адекватное решение о санкционированном доступе на объект или в отказе в нём принимается системой контроля и управления доступом (СКУД) на основании анализа свойств сущности, которую предъявляет пользователь системы. В зависимости от вида предъявленной сущности процессы аутентификации могут быть реализованы различным образом.

Пользовательские сущности могут быть представлены в виде неотъемлемых характеристик, присущих субъекту доступа, в частности, квазистатических, т.е. практически постоянных биометрических данных личности, таких как радужная оболочка и сетчатка глаза, отпечатки пальцев, геометрия ладони и др. Кроме того, пользовательские сущности могут быть представлены в виде динамических идентификационных признаков человека, таких как динамика воспроизведения подписи, параметры речи, клавиатурный почерк, походка и др., относительно медленно меняющихся во времени. В этом случае решение о доступе на объект или отказе в нём принимается на основании анализа идентификационного образа субъекта доступа путём его сравнения с эталонным, в том или ином виде хранящимся в устройстве ввода идентификационных признаков (УВИП).

Пользовательские права на санкционированный доступ также могут быть реализованы на основе знания чего-либо, например, пароля, персонального идентификационного кода PIN, а также секретных и открытых ключей,

обладание которыми демонстрируется в ходе взаимодействия пользователя системой по сценарию "запрос-ответ".

Идентификаторы для систем контроля и управления доступом. Для подтверждения своей подлинности пользователь может предъявлять системе тот или иной идентификатор, которым он обладает и в качестве которого могут выступать карты с магнитной полосой, электронные карты, радиочастотные идентификаторы и др. [1]. Цель - снижение рисков принятия неверного решения (табл. 1).

Системы контроля и управления доступом, которые принимают решения по конкретному признаку сущности пользователя, являются простейшими и не обеспечивают в полной мере высоких требований к современным системам по степени защиты. В целях повышения уровня защиты системы от НСД применяется организация доступа по совокупности сущностей, предъявляемых системе. Например, доступ может быть организован на основании предъявления идентификатора в виде карты совместно с вводом PIN-кода. Более высокий уровень защищённости системы реализуется путём анализа неотъемлемых характеристик пользователя в сочетании с предъявлением идентификатора.

В современных системах контроля и управления доступом наибольшее применение находят радиочастотные идентификаторы (РЧИД). В состав систем, использующих радиочастотную идентификацию, как и в прочие системы идентификации, использующих носитель идентификационного признака, входят считыватель и непосредственно идентификатор. Идентификатор включает в себя микросхему энергонезависимой памяти с фиксированным или перепрограммируемым кодом, антенну и конденсатор,

которые в совокупности представляют входной резонансный колебательный контур. Антенна в зависимости от используемого системой диапазона частот выполняется в виде многовиткового контура или печатных проводников.

При попадании идентификатора в активную зону считывателя контуры идентификатора и считывателя оказываются индуктивно связанными. Контур считывателя можно рассматривать как первичный, а контур идентификатора - как вторичный. При появлении в активной зоне первичного контура антенны идентификатора - вторичного контура - происходит увеличение их взаимной индуктивности и соответственно появляется возможность обеспечения электропитания пассивного идентификатора. Кроме того, изменения параметров вторичного контура, например, его перестройка или шунтирование, могут обеспечить информационный обмен между считывателем и идентификатором.

Микросхема идентификатора содержит энергонезависимую память для хранения кода идентификатора, модулятор, изменяющий параметры контура и обеспечивающий информационный обмен с терминалом, выпрямитель и стабилизатор напряжения электропитания с буферным конденсатором, цепь синхронизации, узел детектирования информации для обеспечения двухстороннего обмена информацией карты с терминалом.

Терминал (считыватель) представляет собой микропроцессорное устройство, содержащее первичный колебательный контур и электронную схему, обеспечивающую детектирование сигнала, получаемого с карты. На характеристики системы существенное влияние оказывает частотный диапазон (табл. 2).

В низкочастотном диапазоне (125,0...400,0 кГц) функционирует большинст-

Таблица 1

Возможные варианты решения системы контроля и управления доступом при предъявлении действующего и фальсифицированного идентификатора

Гипотеза	Решение системы контроля и управления доступом	
	Доступ разрешён	Доступ запрещён
Предъявлен действующий идентификатор	Обоснованное разрешение доступа	Ложный запрет доступа
Предъявлен фальсифицированный идентификатор	Несанкционированный доступ	Обоснованный запрет доступа

Таблица 2

Параметры радиочастотных идентификаторов в различных диапазонах частот

Используемый диапазон частот	Компоненты антенны	Дальность считывания, м	Проникающая способность	Критичность к ориентации относительно считывателя	Функционирование считывателя на металлической поверхности
НЧ 30,0...300,0 кГц	Индуктивность (>100 витков) и конденсатор	0,2	Высокая	Низкая	Возможно
ВЧ 3,0...30,0 МГц	Индуктивность (<100 витков) и конденсатор	<1,0	Средняя	Средняя	Возможно с уменьшением дальности считывания
СВЧ >900,0 МГц	Диполь (отрезки проводника)	> 1,0	Низкая	Высокая	Существенно уменьшает дальность считывания

Таблица 3

Характеристики систем радиочастотной идентификации в разных диапазонах частот

Диапазон частот	Характеристики системы РЧИД	Примеры применения
НЧ, 30 - 300 кГц	Малая дальность считывания. Низкая стоимость меток.	Контроль доступа. Идентификация животных. Складской учёт (логистика).
ВЧ, 3 - 30 МГц	Средняя дальность считывания. Высокая стоимость меток.	Контроль доступа. Смарт-карты.
СВЧ, 300 МГц - 5,8 ГГц	Большая дальность и высокая скорость считывания информации. Требуется точная ориентация.	Наблюдение за перевозкой грузов железной дорогой. Системы взимания платы за пользование дорогой с водителей автомобилей.

во систем со считывателями и идентификаторами, как правило, хранящими фиксированный номер (код) без возможности его модификации (перезаписи). Существенным недостатком систем этого диапазона является необходимость использования многовитковой катушки идентификатора, что исключает возможность её изготовления печатным способом. Широко распространены системы с рабочей частотой 125,0 кГц. Сравнение характеристик систем, функционирующих в разных диапазонах частот, дано в табл. 3.

В настоящее время наиболее перспективные системы реализуются в высокочастотном диапазоне 4,0...24,0 МГц. Это связано с двумя факторами: во-первых, увеличение рабочей частоты позволяет повысить скорость двустороннего информационного обмена между картой и терминалом. Вторым обстоятельством, дающим таким системам существенные преимущества перед упомянутыми выше, является возможность выполнения антенны в виде печатных проводников. В этом диапазоне работают системы с бесконтактными смарт-картами типов MIFARE (фирма Philips) и iCLASS (фирма HID).

Классификация систем РЧИД по диапазону рабочих частот и дальности считывания

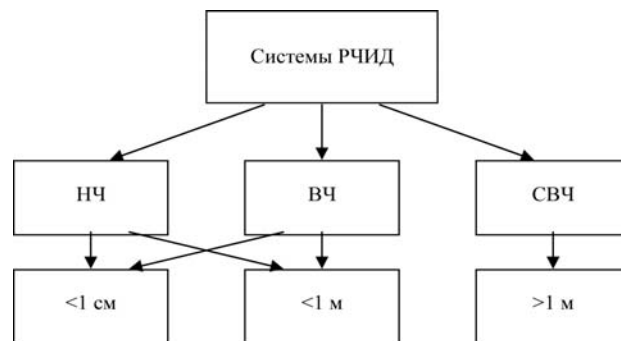
идентификаторов представлена на рисунке.

Системы с большой дальностью считывания могут быть реализованы в диапазоне частот 900,0 МГц и выше. Следует отметить, что в этом случае активная зона считывателя существенно зависит от взаимного расположения антенны идентификатора относительно антенны считывателя. Кроме того, на параметрах системы сказываются окружающие условия, в том числе поверхность, на которой установлен считыватель, наличие окружающих предметов, их форма, влажность среды и т.п.

Примеры зависимости дальности считывания от размеров и формы антенны сведены в

табл. 4.

Широко распространённые радиочастотные идентификаторы типа Proximity реализуют двусторонний обмен информацией между считывателем и идентификатором через индуктивную (трансформаторного типа) связь, и не требуют организации радиоканала между считывателем и идентификатором. В частности, в ходе сессии информационного обмена между идентификатором и терминалом идентификатор не выступает в качестве передатчика, а осуществляет модуляцию амплитуды несущей частоты считывателя в соответствии с кодовой последовательностью, введённой в его память.



Классификация систем РЧИД по диапазону рабочих частот и дальности считывания идентификаторов

Таблица 4

Зависимость дальности считывания идентификационной информации от размеров и формы антенны

Размеры идентификатора, мм	Дальность считывания идентификатора, см			
	Рабочая частота 125 кГц		Рабочая частота 13,5 МГц	
	Тип системы		Тип системы	
	ближняя (размер антенны 76x102 мм)	дальняя (размер антенны 406x812 мм)	ближняя (размер антенны 76x152 мм)	дальняя (размер антенны 51x140 мм)
12*	2,5	10,0-12,5	4,0	18,0-23,0
25*	5,0	20,0-30,0	10,0	36,0-53,0
50*	7,5-10,0	45,0-56,0	12,5-15,0	63,0-76,0
57x86**	10,0-12,0	68,0-81,0	15,0-18,0	90,0-102,0

* — форма идентификатора - круглая,

** — форма идентификатора - в виде карты.

В диапазоне СВЧ реализуется другой принцип двустороннего взаимодействия идентификатора и считывателя: передача информации осуществляется по радиоканалам.

Для обеспечения функционирования идентификатора в его антенне (индуктивности) должна быть наведена ЭДС, достаточная для обеспечения его электропитания, так как он не имеет встроенного аккумулятора. Величина напряжения, наведённого в антенне идентификатора, зависит от того, находится ли он в ближней или дальней рабочих зонах, и может находиться в пределах 5,0...200,0 В.

Синхронизирующий сигнал, необходимый для обеспечения функционирования идентификатора, может формироваться из несущего сигнала или вырабатывается встроенным генератором. Формирование кодового сигнала, полученного от идентификатора, осуществляется пиковым детектором считывателя.

Процедура информационного обмена между идентификатором и считывателем реализуется следующим образом:

- считыватель, непрерывно формирующий колебания сигнала несущей частоты, анализирует наличие модуляции в сигнале, появление которой означает обнаружение идентификатора в зоне действия считывателя;

- идентификатор, находящийся в поле считывателя, накапливает электроэнергию, достаточную для обеспечения его функционирования, а затем в соответствии с протоколом взаимодействия с терминалом инициирует передачу хранящейся в нём кодовой последовательности;

- передача кодовой информации от идентификатора к считывателю осуществляется путём адекватного управления элементом, шунтирующим его контур, что приводит к соответствующему изменению напряжения несущего сигнала в связанном с ним контуре считывателя;

- восстановление в считывателе кодовой информации идентификатора осуществляется путём пикового детектирования огибающей несущего сигнала амплитудно-манипулированного в соответствии с используемым алгоритмом.

Кодирование. Выбранный способ кодирования определяет возможность обнаружения и исправления ошибок, возникших при информационном обмене между идентификатором и терминалом. Кроме того, он определяет способ выделения синхросигнала, полосу частот, занимаемую системой, и другие параметры.

Среди известных способов кодирования наибольшее распространение получили следующие:

- простейший двухуровневый код типа NRZ, характерный отсутствием возврата уровня сигнала к "нулю" в пределах тактового интервала, основным недостатком которого является отсутствие возможности прямого выделения синхросигнала;

- двухчастотный код, характерный наличием дополнительного перехода 0-1 или 1-0 при передаче информационных "единиц" и сменой полярности на границе каждого тактового интервала при передаче информационных "нулей", важным достоинством которого является свойство самосинхронизации и возможность выявления возникающих ошибок;

- манчестерский код, представляющий собой разновидность приведенного выше способа кодирования, который характеризуется наличием переходов от высокого уровня к низкому при передаче информационных "единиц" и обратных переходов при передаче информационных "нулей", также обладающий свойством самосинхронизации и отсутствием постоянной составляющей в монотонных информационных последовательностях.

Защита информации. Снижение рисков возможных несанкционированных воздействий на СКУД при использовании идентификаторов в виде смарт-карт реализуется в ходе аутентификационных процедур. Цель аутентификации заключается в проверке идентичности и аутентичности каждой из частей коммуникационной пары. Применительно к смарт-картам такая процедура предполагает, что карта или терминал принимают решение о том, является ли другой участник информационного обмена подлинным.

Участники сессии обмена информацией должны обладать некоторой общей секретной информацией, которая анализируется в процессе аутентификации. В ходе аутентификационной процедуры должны быть созданы условия, при которых перехват секретной информации становится невозможным.

В настоящее время при реализации СКУД используются подходы, предполагающие реализацию процедур динамической аутентификации. При динамической аутентификации информационные блоки, которыми обмениваются идентификатор и считыватель, формируются таким образом, что структура данных, передаваемых во время предыдущей информационной сессии, отличается от структуры данных, передаваемых в ходе текущего обмена информацией, и по этой причине не могут быть использованы для несанкционированного доступа к ресурсам системы [2-4].

Следует также учитывать принципиальное отличие между однонаправленной и двусторонней процедурами аутентификации. В первом случае определяется аутентичность в одном из направлений информационного обмена, а во втором — устанавливается взаимная аутентичность.

Аутентификация, базирующаяся на криптографических алгоритмах, подразделяется на симметричную и асимметричную версии. В настоящее время для систем со смарт-картами применяются в основном симметричные процедуры. Асимметричные процедуры, базирующиеся на алгоритмах RSA (или аналогичных), менее распространены. Однако предполагается, что в будущем эта ситуация может измениться.

Процесс аутентификации смарт-карт всегда содержит процедуру выработки производного отклика на случайное воздействие. Участник сессии информационного обмена использует определённый алгоритм вычисления такого отклика и посылает его в ответ на полученное воздействие.

В связи с наличием радиоканала в системах с радиочастотной идентификацией для их защиты должны быть приняты дополнительные

Оценка уровня защищенности различных методов идентификации при НСД различных видов

Основа метода идентификации	Уровень защищённости от различных видов НСД						Возможность аутентификации
	Кража	Съём информации	Манипулирование	Копирование	Принуждение	Повреждение	
Документ пользователя	Н	В	В	Н...В	Н	Н...В	Н
Персональная конфиденциальная информация	В	Н	С...В	В	Н	Н...В	Н
Физические параметры пользователя	В	В	В	П...В	Н	Н...В	В

Сокращенные обозначения уровня защищенности, использованные в таблице:
 н — низкий, с — средний, п — повышенный, в — высокий.

меры, так как сессии информационного обмена могут быть достаточно просто перехвачены злоумышленником. На практике наиболее предпочтительным алгоритмом является тот, в котором используется конфиденциальный ключ, представляющий собой инструмент засекречивания, используемый при взаимной аутентификации.

Биометрические методы идентификации пользователя в системах СКУД. Достижения высокого уровня защиты ресурсов систем с использованием идентификаторов в виде карт пользователя, использующих технологию радиочастотной идентификации, может быть достигнута только в совокупности с применением такого высокоэффективного метода, как биометрическая идентификация субъекта, что позволяет осуществить жёсткую "привязку" идентификатора к конкретному пользователю - персонификацию. Данный метод для идентификации субъекта использует его характерные уникальные физиологические или поведенческие особенности [5].

В системах контроля и управления доступом наиболее употребимы системы идентификации субъектов по отпечаткам пальцев, по геометрии руки и по радужной оболочке глаза.

Наибольшее распространение получили системы идентификации, основанные на дактилоскопическом (папиллярном) методе, так как современные средства микроэлектроники позволяют создавать необходимые миниатюрные считывающие элементы. Следует отметить, что изображение 2,0 x 3,0 см содержит около 240 тыс. элементов, что требует объёма памяти 240 кбайт и приводит к удорожанию системы. По этой причине исходное папиллярное изображение сжимается с коэффициентом сжатия порядка 10.

Современные методы устранения избыточности позволяют создать образцы отпечатков с объёмом данных от 40 байт до 1 кбайта с невозможностью восстановления исходного отпечатка, что защищает персональные данные субъекта.

В ходе функционирования системы идентификации пользователей осуществляется путём сравнения данных, полученных от предъявленного отпечатка субъекта с эталонным образом, хранящимся в памяти системы.

Реализация алгоритмов сравнения может осуществляться двумя способами. В первом случае производится поиск отпечатка, адекватного предъявленному, по всей имеющейся базе данных. Во втором случае произво-

дится сравнение образа считанного отпечатка с конкретным образцом, извлечённым из памяти системы, что предполагает введение в неё сведений о конкретном пользователе. Вызов из памяти необходимого образа может производиться кодонаборным способом или считывателем, например, с радиочастотного идентификатора.

Оценка уровня защищенности комбинированных систем контроля и управления доступом, использующих защиту ресурсов идентификаторов в сочетании с биометрической идентификацией. При использовании исключительно методов криптозащиты ресурсов идентификаторов СКУД, выполненных на основе технологии пластиковых карт и в частности такого их вида, как радиочастотные идентификаторы, широко используемые в настоящее время, не удаётся обеспечить привязку субъекта к используемому им документу доступа. Необходимый эффект персонификации субъекта доступа может быть достигнут только при дополнительном использовании методов биометрической идентификации. Представление о результативности использования методов биометрической идентификации при несанкционированных воздействиях (НСД) различных видов дает табл. 5.

Рассмотрение представленных в таблице данных позволяет сделать вывод, что при всех возможных несанкционированных воздействиях, включая кражу, съём информации, манипулирование, кодирование, принуждение и повреждение, только определение физических параметров пользователя позволяет достичь высокого уровня аутентификации субъекта СКУД [6].

Инновационным решением в сфере обработки папиллярных образов в системах

контроля и управления доступом является использование радиочастотных идентификаторов с большим ресурсом памяти, что позволяет хранить в них полный объём необходимой информации для последующего сравнения с предъявленным пользователем папиллярным образом. Такой метод исключает необходимость занесения всей совокупности папиллярных образов пользователей системы в оперативную память, что в свою очередь обеспечивает возможность практически неограниченного расширения системы и позволяет обходиться без объединения всех терминалов в единую сеть с центральным процессором.

Литература

1. Зелевич Е.П. Пластиковые карты в связи. М.: Радио и связь, 2004. — 288 с.
2. Зелевич Е.П. Защита информации в системах связи с интеллектуальными картами//Мобильные системы, 2004. — №2. — С.34-37.
3. Зелевич Е.П. Основные вопросы защиты процедур информационного обмена в системах с пластиковыми картами//Мобильные системы, 2005. — №3. — С.35-39.
4. Обеспечение информационной безопасности в экономической и телекоммуникационной сферах. Коллективная монография. Кн.2. Сер. "Защита информации" под ред. Е.М.Сухарева. М.: Радиотехника, 2003. — 216 с.
5. Петраков А.В., Дорошенко П.С., Савлуков Н.В. Охрана и защита современного предприятия. М.: Энергоатомиздат, 1999. — 568 с.
6. Волковицкий В.Д., Волхонский В.В. Системы контроля и управления доступом. — СПб.: Экополис и культура, 2003. — 165 с.: ил.

Позиционирование оператора связи на телекоммуникационном рынке на основе метода Уолша

Артемяева Г.С.,
доцент МТУСИ

Резникова Н.П.,

профессор, зав. кафедрой МТУСИ

Тихвинский В.О.,

председатель ИТТ РАЕН,

профессор МТУСИ

Введение

Любому оператору связи важно осознавать, а следовательно, и анализировать природу явлений и состояний внешней среды, в которой он работает, для того, чтобы понять, выявить и, по возможности, оценить те ключевые факторы, которые воздействуют на работу и ее результаты, прежде всего, в стратегическом плане. К таким факторам можно отнести и изменения в регуляционном механизме отрасли. Формулирование стратегии заключается в установлении соответствия (припасовке) собственных перспективных возможностей и условий внешней среды. Подходы к стратегическому планированию (см., например, [1,2,3,4,5, 6,7]) основаны на том, что до выработки стратегий необходимо провести стратегический анализ для получения представления о существующей стратегической позиции организации во внешней среде, для чего следует пройти определенную последовательность этапов:

1 этап. Стратегический анализ, включающий анализ внешней среды, в которой работает оператор; оценку ресурсов организации для того, чтобы понять и оценить свои стратегические возможности.

2 этап. Проведение SWOT-анализа, в ходе которого выявляются собственные силы и слабости, а также — возможности и угрозы со стороны рынка и позиционируется собственное положение, как возможность противостоять этому влиянию, если оно негативное, и наоборот. Оценивается, почему эти факторы важны, с какой степенью неопределенности приходится сталкиваться. В частности, оценивается текущее конкурентное положение организации относительно основных существующих и потенциальных конкурентов (осуществляется позиционирование).

Такой анализ дает определенную уверенность менеджерам оператора в том, что они

подготовлены, чтобы ответить на вызов со стороны новых обстоятельств, обусловленных развитием внешней среды. Например, в соответствии с действующим законодательством, операторы сотовой связи столкнутся с регулированием со стороны государства, если будет принята соответствующая поправка в закон "О связи" [10].*

Государственное регулирование операторов, признанных существенными, означает, что цены на ряд услуг компании будут подвергаться воздействию со стороны регулирующих органов на основе утвержденных методов расчета экономически обоснованных цен (тарифов) на такие услуги.

В экономическом плане государственное регулирование операторов, признанных существенными, означает, что цены на ряд услуг компании будут подвергаться воздействию со стороны регулирующих органов на основе утвержденных методов расчета экономически обоснованных цен (тарифов) на такие услуги. В случае принятия поправки возможны, среди прочих, следующие сценарии развития событий:

- от компании-оператора потребуется введение системы раздельного учета доходов и расходов для обоснования себестоимости услуг, подвергаемых регулированию;
- можно ожидать определенного снижения доходности (и рентабельности) в части регулируемых услуг и ухудшения конкурентного положения оператора на рынке.

Поэтому может представлять определенный интерес позиционирование такого оператора по отношению к уже регулируемым компаниям связи, следовательно, правомерно поставить вопрос о том, с помощью какого инструментария можно быстро и достаточно надежно оценить то, насколько устойчиво конкурентное положение компании на рынке услуг связи в момент анализа.

Позиционирование компании можно про-

* 10 апреля 2008 г. депутат М.Л. Коробов внес в Государственную Думу законопроект № 44016-5 "О внесении изменений в Федеральный закон "О связи" [4]. В поправке предлагается, чтобы существенными считались, в том числе, компании, владеющие не менее 25% номеров на территории субъекта РФ или всей России.

вести с использованием подхода, изложенного в [7] и названного авторами статьи "методикой К. Уолша". Подход, с одной стороны, реализован на примере оператора ОАО "ВымпелКом", одного из ведущих операторов сотовой связи в России, который предоставляет свои услуги под торговой маркой "Билайн", являющейся одной из наиболее известных торговых марок России, и который может подпасть под регулирование. Вместе с тем, подход представляет общий интерес для позиционирования любой компании на конкурентном рынке.

Рассмотрение вопроса позиционирования оператора является основной целью настоящей статьи.

Исходные предпосылки

Как известно, к основным характеристикам любого рынка относится не только предложение, складывающееся под влиянием поставщиков, но, прежде всего, платежеспособный спрос (потребители), а также — пространство, время и конкуренция. В соответствии с Законом РФ от 26.07.2006 № 135-ФЗ "О защите конкуренции", конкуренция — соперничество хозяйствующих субъектов, при котором "исключается или ограничивается возможность каждого из них в одностороннем порядке воздействовать на общие условия обращения товаров на соответствующем товарном рынке".

С экономической точки зрения, деловая конкуренция рассматривается в 3 основных ракурсах: 1) как степень состоятельности на рынке в достижении одних и тех же целей; 2) как набор условий, по которым определяется тип отраслевого рынка; 3) как регулирующий элемент рыночного механизма.

С точки зрения первого ракурса, основными целями любой компании могут быть прибыль и рентабельность, доля на рынке, цена компании и др. Отсюда для оценки устойчивости положения компании должны быть проведены расчеты по совокупности показателей, характеризующих эффективность операционной и финансовой деятельности, и осуществлено сравнение этих показателей с рассчитанными аналогичным образом одноименными показателями других компаний. Для примера в настоящей статье осуществлено позиционирование ОАО "Вымпелком" среди других операторов. При этом разумным представлялось выбрать для сравнения операторов, уже признанных существенны-

ми, т.е. регулируемых. Выбраны МРК (межрегиональные компании) еще и потому, что они предоставляют услуги сотовой связи, а многие абоненты сотовых операторов используют для исходящего вызова на сотовый телефон местную сеть.

С точки зрения второго ракурса современный рынок услуг сотовой связи характеризуется набором условий, объединяемых понятием несовершенная конкуренция. Несовершенная конкуренция — состояние рынка, на котором много покупателей и мало продавцов, которые осуществляют действия по подавлению конкуренции со стороны других фирм. Используемые при этом средства известны и достаточно типичны, например: демпинговые цены; создание входных барьеров на рынок различных товаров (работ, услуг); ценовая дискриминация (продажа одного и того же продукта по разным ценам); использование или разглашение конфиденциальной научно-технической, производственной и иной информации; распространение ложных сведений (информации) относительно характеристик услуг в рекламе или иными способами; замалчивание важной для потребителя информации и др. Этот ракурс в статье не рассматривался.

С точки зрения третьего ракурса рассмотрение конкуренции, государство рано или поздно прибегает к регулированию естественной монополии, имитируя тем самым воздействие конкуренции на рассматриваемом рынке. Поэтому важная задача компании — дать прогноз последствий от такого вмешательства по основным показателям деятельности. В настоящей статье такой прогноз не осуществлялся по причине использования исключительно открытых данных из публичной отчетности: баланса и отчета о прибылях и убытках компаний, которые позволяют провести стороннему наблюдателю только экспресс-анализ. Предполагаемое изменение цен на услуги, которые могут быть подвергнуты регулированию, повлияет на спрос, а следовательно, доходы и объем предложения, что, в свою очередь, должно вызвать изменение расходов, налоговых выплат и т.п. Проследить все возможные цепочки положительных и отрицательных последствий введения регулирования без доступа к системе бюджетирования компаний нельзя. Точные расчеты могут выполнить менеджеры компании в соответствии с данными управленческого и финансового учета.

Позиционирование на основе метода Уолша

Для позиционирования положения оператора на основе финансово-экономического анализа сформирована таблица 1, содержащая наиболее значимые показатели из нескольких блоков, характеризующих эффективность операционной и финансовой деятельности любой компании: ликвидность, финансовая устойчивость, положение на рынке и др. [7, 8, 9]. Для позиционирования конкретной компании (в нашем случае — ОАО "ВымпелКом") среди операторов, занимающих существенное положение в сети связи общего пользования, из табл. 1 из-за ограниченности рамок статьи выбраны основные показатели, представленные в табл. 2 для иллюстрации метода и наиболее разносторонне характеризующие рассматриваемую компанию. Вместе с тем, авторами были рассчитаны значения всех показателей из табл. 1 по всем рассмотренным компаниям за период 2005-2007 гг., что и должны делать менеджеры для позиционирования своей компании.

Позиционирование ОАО "ВымпелКом" осуществлено на основе графического метода, собственно и названного нами "методикой К. Уолша". Этот метод позволяет представить каждый анализируемый параметр в виде треугольников таким образом, что: в вершине треугольника отражается значение коэффициента для анализируемой компании; у основания треугольника слева и справа располагаются, соответственно, минимальное и максимальное значение коэффициента, полученного в результате анализа одноименных показателей сравниваемых компаний; внутри треугольника расположен диапазон наиболее часто встречающихся значений рассматриваемого коэффициента для исследуемых компаний, т.е. в эти границы попадает около 50% исследуемых компаний.

Полученные "треугольники" (см. рис. 1-8) наглядно отражают положение компании.

Высокое значение коэффициента ДСК (в сравнении с другими операторами см. рис. 1.), говорит об успехе компании, что ведет к высокому рыночному курсу ее акций и относительной легкости привлечения новых капиталов для ее развития. В этом случае компании легче увеличивать масштабы своей деятельности, если, конечно, общие условия для этого на рынке благоприятны, а это, в

* В рамках статьи числовые значения для ряда показателей не приводятся, т.к. авторы использовали только данные форм 1 и 2 отчетности, однако, расчеты могут быть проведены аналитиками для более глубокого анализа.

Значения показателей ОАО "Вымпелком" для позиционирования

Показатели	Ед.изм.	Формулы	Строки	2005г.	2006г.	2007г.
Доходность совокупных активов (ДСА) (ROTA)	%	$\frac{\text{Прибыль до выплаты процентов и налогов (ПВПН)}}{\text{Совокупные активы (СА)}} \times 100$	$\frac{\text{форма 2 стр.050}}{\text{форма 1 стр.300(700)}}$	20,82%	25,67%	29,15%
Доходность собственного капитала (ДСК) (ROE)	%	$\frac{\text{Прибыль после налогов (ППН)}}{\text{Собственный капитал (СК)}} \times 100$	$\frac{\text{форма2 стр160}}{\text{форма1 стр490}}$	25,20%	30,51%	32,35%
Рентабельность реализации	%	$\frac{\text{ПВПН}}{\text{Выручка от реализации}} \times 100$	$\frac{\text{форма 2 стр 050}}{\text{форма 2 стр 010}}$	40,63%	39,57%	41,52%
Рентабельность материальных затрат ¹	%	$\frac{\text{материальные затраты}}{\text{Выручка}} \times 100$	$\frac{\text{форма5 стр601}}{\text{форма2 стр010}}$			
Рентабельность затрат на оплату труда	%	$\frac{\text{затраты на оплату труда}}{\text{Выручка}} \times 100$	$\frac{\text{форма5 стр602}}{\text{форма2 стр010}}$			
Рентабельность отчислений на социальные нужды	%	$\frac{\text{отчисления на соц. нужды}}{\text{Выручка}} \times 100$	$\frac{\text{форма5 стр603}}{\text{форма2 стр010}}$			
Рентабельность амортизации	%	$\frac{\text{Амортизация}}{\text{Выручка}} \times 100$	$\frac{\text{форма5 стр604}}{\text{форма2 стр010}}$			
Рентабельность прочих затрат	%	$\frac{\text{Прочие затраты}}{\text{Выручка}} \times 100$	$\frac{\text{форма5 стр605}}{\text{форма2 стр010}}$			
Оборачиваемость совокупных активов	раз	$\frac{\text{Выручка от реализации}}{\text{СА}}$	$\frac{\text{форма2 стр.010}}{\text{форма1 стр.300(700)}}$	0,5124	0,6486	0,7021
Оборачиваемость основных средств	раз	$\frac{\text{Выручка}}{\text{Основные средства}}$	$\frac{\text{форма2 стр.010}}{\text{форма1 стр.(120 + 130)}}$	1,0298	1,2612	1,5957
Оборачиваемость товарно-материальных запасов	раз	$\frac{\text{Выручка}}{\text{Запасы}}$	$\frac{\text{форма 2 стр .010}}{\text{форма 1 стр .(210 + 220)}}$	3,5859	5,5844	7,6031
Оборачиваемость дебиторской задолженности	раз	$\frac{\text{Выручка}}{\text{Дебиторская задолженность}}$	$\frac{\text{форма2 стр.010}}{\text{форма1 стр.(230 + 240)}}$	4,770861864	6,6082	7,8338
Число дней хранения запасов	дни	$\frac{\text{Запасы}}{\text{Выручка}} \times 365$	$\frac{\text{форма 1 стр .(210 + 220)}}{\text{форма 2 стр .010}} \times 365$	101,78	65,35	48,01
Средний срок оплаты счетов дебиторов (период оборота дебиторской задолженности)	дни	$\frac{\text{Дебиторская задолженность}}{\text{Выручка}} \times 365$	$\frac{\text{форма 1 стр .(230 + 240)}}{\text{форма 2 стр .010}} \times 365$	76,50	55,23	46,59
Коэффициент текущей ликвидности	раз	$\frac{\text{Оборотные активы}}{\text{Краткосрочные обязательства}}$	$\frac{\text{форма1 стр.290}}{\text{форма1 стр.690}}$	2,24	2,41	2,73
Коэффициент срочной ликвидности	раз	$\frac{\text{Оборотные активы} - \text{Запасы}}{\text{Краткосрочные обязательства}}$	$\frac{\text{форма 1 стр .(290 - (210 + 220))}}{\text{форма 1 стр. 690}}$	1,19	1,31	1,87
Коэффициент обеспеченности реализации оборотным капиталом	%	$\frac{\text{ОА} - \text{КО}}{\text{Выручка}} \times 100$	$\frac{\text{форма1 стр.(290 - 690)}}{\text{форма2 стр.010}}$	33,08%	22,97%	26,66%
Коэффициент покрытия процентов	раз	$\frac{\text{ПВПН}}{\text{Проценты}}$	$\frac{\text{форма2 стр050}}{\text{форма2 стр070}}$	7,33	10,02	14,16
1 Коэффициент квоты собственника	раз	$\frac{\text{Совокупные обязательства}}{\text{Собственный капитал}}$	$\frac{\text{форма1 стр.(590 + 690)}}{\text{форма1 стр.490}}$	1,142	0,82	0,65
2 Коэффициент квоты собственника	%	$\frac{\text{Собственный капитал}}{\text{Совокупные активы}} \times 100$	$\frac{\text{форма1 стр.490}}{\text{форма1 стр.300(700)}}$	46,68%	55,07%	60,28%
3 Коэффициент квоты собственника	%	$\frac{\text{Совокупные обязательства}}{\text{Совокупные активы}} \times 100$	$\frac{\text{форма1 стр.(590 + 690)}}{\text{форма1 стр.300(700)}}$	53,32%	44,93%	39,72%
Балансовая стоимость акции, или обеспечение активами	руб.	$\frac{\text{Совокупные активы}}{\text{Число обыкновенных акций}}$	$\frac{\text{форма1 стр.300(700)}}{\text{Число акций}}$	2,77	3,50	4,32
Рыночная капитализация	тыс.	Число обыкновенных акций × Рыночный курс акций	-			
Прибыль на одну акцию (ПА)	руб.	$\frac{\text{ППН}}{\text{Число акций}}$	$\frac{\text{форма2 стр.160}}{\text{Число акций}}$	0,33	0,59	0,84
Дивиденды на одну акцию (ДА)	руб.	$\frac{\text{Сумма дивидендов на обыкновенные акции}}{\text{Число акций}}$	$\frac{\text{форма3 стр.203(403)}}{\text{Число акций}}$	-	-	0,17
Покрытие дивидендов	раз	$\frac{\text{ПА}}{\text{ДА}} = \frac{\text{ППН}}{\text{Сумма дивидендов на обыкновенные акции}}$	$\frac{\text{форма2 стр.160}}{\text{форма3 стр.203(403)}}$	-	-	5,050
Коэффициент выплаты дивидендов	%	$\frac{\text{ДА}}{\text{ПА}} = \frac{\text{Сумма дивидендов на обыкновенные акции}}{\text{ППН}}$	$\frac{\text{форма3 стр.203(403)}}{\text{форма2 стр.160}}$	-	-	0,198
Полная доходность акций	%	$\frac{\text{ПА}}{\text{Курс акций}}$	-			
Текущая доходность акций	%	$\frac{\text{ДА}}{\text{Курс акций}}$	-			
Кратное прибыли (КП)	руб.	$\frac{\text{Курс акции}}{\text{ПА}}$	-			
Кратное балансовой стоимости акции	раз	$\frac{\text{Рыночная капитализация}}{\text{Собственный капитал}}$	$\frac{\text{Рыночная капитализация}}{\text{форма 1 стр 490}}$			
Оборотные активы на 1 руб. выручки	%	$\frac{\text{Оборотные активы}}{\text{Выручка}}$	$\frac{\text{форма 1 стр.290}}{\text{форма 2 стр.010}}$	0,59	0,39	0,42
Нераспределенная прибыль на 1 руб. выручки	%	$\frac{\text{Нераспределенная прибыль}}{\text{Выручка}}$	$\frac{\text{форма 2 стр .190}}{\text{форма 2 стр .010}}$	0,23	0,26	0,28

¹ В рамках статьи числовые значения для ряда показателей не приводятся, т.к. авторы использовали только данные форм 1 и 2 отчетности, однако, расчеты могут быть проведены аналитиками для более глубокого анализа.

Таблица 2

Основные финансовые показатели, характеризующие компанию

Компания	Год	ДСК, %	ДСА, %	Рентабельность реализации, %	Период оборачиваемости дебиторской задолженности, дни	Коэффициент текущей ликвидности	Коэффициент срочной ликвидности	Коэффициент покрытия процентов	Коэффициент квоты собственного капитала, раз
1	2	3	4	5	6	7	8	9	10
ОАО "Северо-Западный телеком"	2005	8,24	10,55	18,40	38	1,03	0,67	9,97	0,83
	2006	13,38	15,48	25,18	35	0,63	0,41	7,09	0,77
	2007	39,11	12,50	24,21	35	0,80	0,74	6,90	0,65
ОАО "Уралсвязьинформ"	2005	12,77	15,67	24,47	33	0,51	0,26	3,56	1,75
	2006	11,24	15,31	22,55	37	0,51	0,38	3,77	1,69
	2007	17,15	16,66	22,10	36	0,37	0,31	4,67	1,42
ОАО "Сибирьтелеком"	2005	6,37	11,37	16,00	39	0,61	0,33	2,82	1,63
	2006	10,37	10,39	17,50	47	0,48	0,35	2,94	1,71
	2007	19,17	14,50	20,23	45	1,00	0,39	4,40	1,54
ОАО "Ростелеком"	2005	23,10	22,61	29,70	57	3,09	2,93	95,20	0,33
	2006	16,30	12,88	12,97	64	2,14	2,03	29,13	0,37
	2007	18,24	11,86	12,91	60	2,12	2,03	33,98	0,32
ОАО "ВолгаТелеком"	2005	13,85	16,63	28,20	30	0,69	0,46	6,38	0,95
	2006	13,52	13,07	33,00	46	0,61	0,43	6,43	0,99
	2007	15,95	14,93	24,25	41	0,61	0,39	7,34	0,96
ОАО "Дальсвязь"	2005	17,08	14,20	16,30	36	0,51	0,26	6,54	1,31
	2006	13,10	17,36	25,10	42	0,45	0,29	7,00	1,56
	2007	10,23	18,45	25,92	43	0,66	0,54	5,70	1,08
ОАО "ЮТК"	2005	2,44	9,62	23,10	26	0,27	0,11	1,73	2,47
	2006	8,68	11,57	27,20	25	0,27	0,12	2,30	2,03
	2007	12,02	12,89	27,80	31	0,30	0,18	2,98	1,81
ОАО "Центртелеком"	2005	4,26	13,11	21,50	30	0,30	0,16	2,52	1,94
	2006	11,87	15,18	25,30	40	0,82	0,51	3,29	1,75
	2007	17,85	17,70	26,04	40	0,59	0,44	4,58	1,34
ОАО "ВымпелКом"	2005	25,20	20,82	40,63	76,50	2,25	1,19	7,331	1,142
	2006	30,51	25,67	39,57	55,23	2,41	1,31	10,03	0,82
	2007	32,35%	29,15	41,52	46,59	2,73	1,87	14,17	0,66

свою очередь, приводит к росту прибыли и цикл повторяется снова. Цифры свидетельствуют, что за рассматриваемый период показатель ДСК в ОАО "Вымпелком" демонстрирует положительную тенденцию, намного выше, чем у остальных компаний в 2006 г. и только на семь пунктов меньше, чем у ОАО "Северо-Западный Телеком" в 2007 г.

Коэффициент ДСА показывает, насколько эффективно компания использует свои активы, чтобы они приносили операци-

онную прибыль. Показатель ДСА у ОАО "Вымпелком" в анализируемом периоде также намного превышает показатели сравниваемых с ним компаний. Разложение ДСА на составляющие по известной формуле Дюпона [2] позволило определить два важных коэффициента (см. табл.1), а именно: "рентабельность реализации" (рис. 3) и "оборачиваемость совокупных активов".

Коэффициент "рентабельность реализации" показывает прибыль, как долю выручки

от реализации продукции и часто называется коэффициентом рентабельности реализации. Как видно из рисунка, этот показатель также намного превышает показатели других компаний. Второй коэффициент фиксирует совокупные доходы компании по отношению ко всем ее активам. Рассмотренные коэффициенты: рентабельность реализации и оборачиваемость совокупных активов являются показателями, влияя на которые можно пытаться повысить доходность совокупных активов. Так например, для оценки влияния на рентабельность реализации можно воспользоваться показателями "рентабельность материальных затрат", "рентабельность затрат на оплату труда", "рентабельность отчислений на социальные нужды", "рентабельность амортизации", "рентабельность прочих затрат" (см. табл.1).

Показатель ПОДЗ, см. рис. 4, выражается числом дней, необходимых для инкассирования счетов клиентов, и, чаще всего, называется "средним сроком оплаты счетов дебиторов" или периодом оборота дебиторской задолженности". Он показывает среднюю продолжительность (в днях) кредита, которым фактически пользуются покупатели товаров и услуг компании, т.е. средний период времени до оплаты клиентами их счетов. Показатель несколько хуже среднего (и за 2006 г., и за 2007 г.), но он на 11-13% лучше, чем у худшей компании.

Цифры свидетельствуют о том, что за рассматриваемый период показатель "коэффициент текущей ликвидности" в ОАО "ВымпелКом" демонстрирует положительную тенденцию, намного выше, чем у остальных компаний. Необходимым значением для показателя "коэффициент текущей ликвидности" является 1,5; оптимальным считается значение $\approx 2 \div 3,5$.

Коэффициент "срочной ликвидности" ОАО "ВымпелКом" выше рекомендованного (рекомендованное значение коэффициента равно 0,7-0,8).

Коэффициент покрытия процентов учитывает возможности компании обслуживать долги. На его величину влияют три фактора:

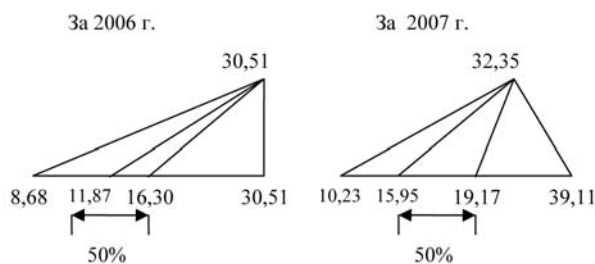


Рис. 1. Доходность собственного капитала (ДСК)

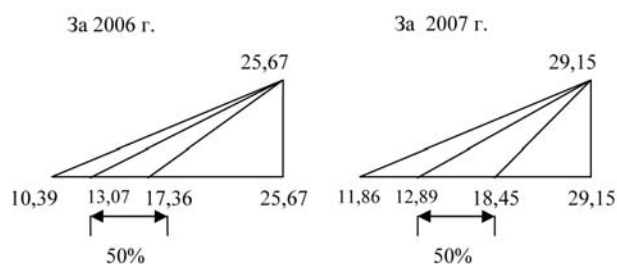


Рис. 2. Доходность совокупных активов (ДСА)

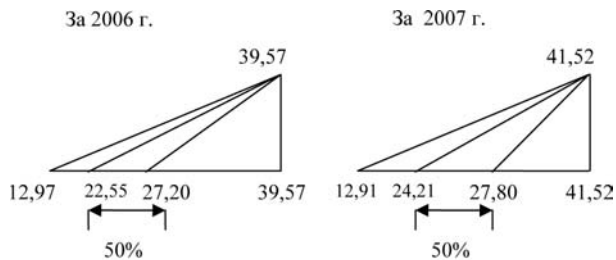


Рис. 3. Рентабельность реализации

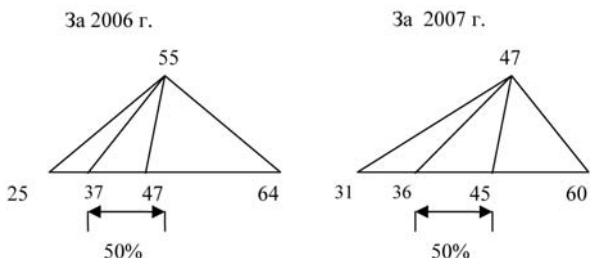


Рис. 4. Период оборачиваемости дебиторской задолженности (ПОДЗ)

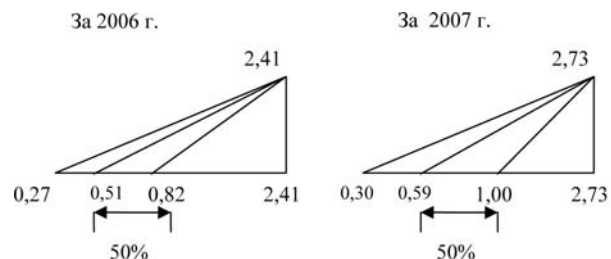


Рис. 5. Коэффициент текущей ликвидности

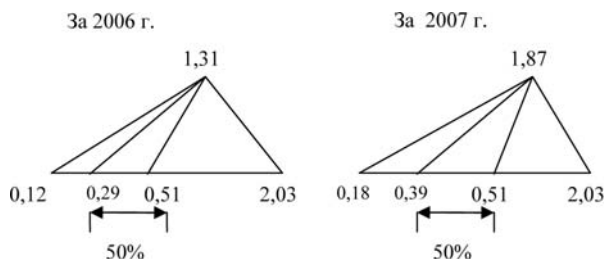


Рис. 6. Коэффициент срочной ликвидности

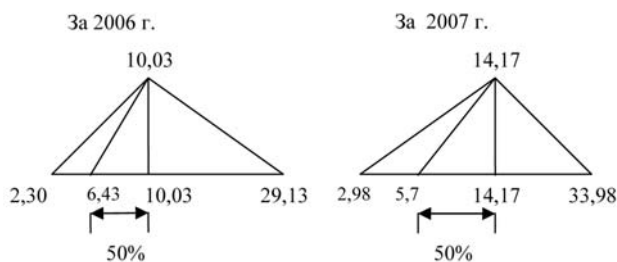


Рис. 7. Коэффициент покрытия процентов

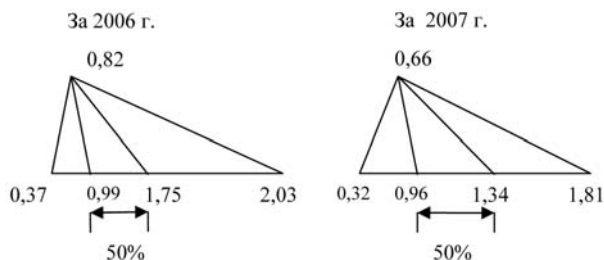


Рис. 8. Коэффициент квоты собственника

операционная прибыль; общая сумма заемных средств; эффективная ставка процента. Данные расчетов, оставшихся за пределами статьи, показали, что на протяжении исследуемого периода наблюдается рост прибыли компании от продаж, а в 2006 и 2007 гг. — сокращение процентов к уплате, следствием чего является ежегодный рост коэффициента покрытия процентов.

Цифры свидетельствуют о том, что за рассматриваемый период показатель "коэффициент покрытия процентов" в ОАО "ВымпелКом" демонстрирует положительную тенденцию, намного выше среднего. Значение этого коэффициента выше только у ОАО "Ростелеком".

Коэффициент квоты собственника (соотношение заемного и собственного капитала) — один из самых важных показателей корпоративных финансов, свидетельствующий о финансовой устойчивости компании. Основное предназначение этого показателя — установить соотношение различных способов финансирования, отраженных в балансе, а также сравнить величину акционерного капитала и капитала кредиторов. Если значение коэффициента квоты собственника не укладывается в нормальное ограничение (не выше 1,5), это говорит о том, что у компании есть серьезные проблемы, связанные с погашением долгосрочных долгов.

Заключение

Практически по всем рассмотренным коэффициентам ОАО "ВымпелКом" демонстрирует существенное превышение значений показателей над аналогичными показателями других (регулируемых) операторов.

Выбранная совокупность показателей при оценке позиции компании на рынке позволила показать, что компания имеет достаточно высокую конкурентоспособность и отражает истинную позицию компании. Вместе с тем, в случае рассмотрения других показателей или другой совокупности компаний для позиционирования своей, или за другие периоды может оказаться, что показатели разнонаправленные (одни лучше, а другие хуже по сравнению с другими операторами). В таком случае следует воспользоваться одним из известных методов для ранжирования операторов по совокупности параметров, в том числе, методами кластерного анализа или таксонометрическим методом.

Литература

1. Ансофф И. Новая корпоративная стратегия. — СПб: Изд. "Питер", 1999. — 416 с.
2. Резникова Н.П. Маркетинг в телекоммуникациях. — М.: Эко-Трендз, 2002. — 336 с.
3. Менеджмент в телекоммуникациях / Под ред. Н.П. Резниковой, Е.В. Деминой. — М.: Эко-Трендз, — 392 с.
4. Day George S. Market Driven Strategy/ Processes for Creating Value/ The Free Press. Collier Macmillan Publishers. 1990 — 405 pp.
5. Минцберг Г., Куинн Дж.Б., Гоцал С. Стратегический процесс / Пер. с англ. Под ред. Ю.Н. Каптуревского. — СПб: Питер, 2001. — 688 с.
6. Porter Michael E. Competitive Strategy. Techniques for Analyzing Industries and Competitors. The Free Press. Collier Macmillan Publishers. 1980 — 396 pp.
7. Уолш К. Ключевые показатели менеджмента: Как анализировать, сравнивать и контролировать данные, определяющие стоимость компании: Пер с англ. — 2-е изд. — М.: Дело, 2001. — 360 с.
8. Донцова Л.В. Анализ финансовой отчетности: учебник / Л.В. Донцова, Н.А. Никифорова. — 4-е изд., перераб. и доп. — М.: Издательство "Дело и Сервис", 2006. — 368 с.
9. Ковалев В.В. Введение в финансовый менеджмент. — М.: Финансы и статистика, 2004. — 768 с.
10. Федеральный закон "О связи" от 07.07.2003 № 126-ФЗ (в последней редакции от 29.04.2008 № 58-ФЗ).

ОФИЦИАЛЬНАЯ ПОДДЕРЖКА:
УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ ПО РБ
ТОРГОВО-ПРОМЫШЛЕННАЯ ПАЛАТА РБ

17-20
марта



БАШЭКСПО
ВЫСТАВОЧНЫЙ ЦЕНТР

УФА
2009



СВЯЗЬ. ИНФОКОМ

XIII специализированная выставка

450080, Уфа, а/я 144, тел./факс: (347) 256-51-80, 290-87-07
E-mail: infocom@bashexpo.ru, <http://www.bashexpo.ru>



2009

ЮГТРАНС

У МЕЖДУНАРОДНЫЙ ТРАНСПОРТНЫЙ ФОРУМ

У МЕЖДУНАРОДНЫЙ ТРАНСПОРТНЫЙ ФОРУМ “ЮГТРАНС-2009”

19-20 марта 2009 г.

Новороссийск, п. Кабардинка, отель “Надежда”

www.yugtrans.info

В рамках Форума состоятся конференции:

- Порты и терминалы юга России
- Контейнерный бизнес
- Транспорт и логистика

Официальная поддержка Форума:

Федеральное агентство морского и речного транспорта
Министерства транспорта РФ

Генеральный интернет-партнер



Генеральный
информационный спонсор
ДЕЛОВОЙ ЖУРНАЛ
РЖД-партнер

Партнер Форума



Эксклюзивный
информационный спонсор

www.transportweekly.com

Информационная поддержка



деловой журнал
КОНТЕЙНЕРНЫЙ БИЗНЕС

SPECSERVER.COM

ОРГАНИЗАТОР ФОРУМА



ООО “Международные конференции”

в Москве: +7 (495) 646-01-51
в Санкт-Петербурге: +7 (812) 448-08-48
в Новороссийске: +7 (8617) 601-341
e-mail: info@konfer.ru
www.konfer.ru

www.yugtrans.info



III Международная выставка современной продукции, новых технологий и услуг железнодорожного транспорта

exporail 2009

18 – 20 марта

ЦВК "ЭКСПОЦЕНТР", Москва

При поддержке:

РЖД Российские
железные дороги

ВСЕ ДЛЯ ЖЕЛЕЗНЫХ ДОРОГ:

- Подвижной состав и комплектующие
- Технологии проектирования и строительства
- Железнодорожные пути и объекты инфраструктуры, станции и вокзалы
- Электрификация и электроснабжение дорог
- Обеспечение перевозок, оплата проезда и информационные системы
- Диспетчерская централизация и управление движением поездов
- Системы безопасности и сигнальное оборудование
- Лизинг, страхование, консалтинг

В деловой программе выставки международная
железнодорожная конференция

www.exporail.ru

Организатор:

РЕСТЭКБРУКС

Россия, 197110, Санкт-Петербург,
Петрозаводская ул., 12
Тел.: (812) 320-80-94, 303-88-62
Факс: (812) 320-80-90
E-mail: exporail@restec.ru

Генеральный
информационный партнер:

ДЕЛОВОЙ ЖУРНАЛ
РЖД-партнер

Структурообразование средств механизации технологического процесса ремонта тележек грузовых вагонов

КОМПЛЕКСНАЯ МЕХАНИЗАЦИЯ И АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА РЕМОНТА ТЕЛЕЖЕК ГРУЗОВЫХ ВАГОНОВ НА ВАГОНОРЕМОНТНЫХ ПРЕДПРИЯТИЯХ РФ. НОВУЮ ТЕХНОЛОГИЮ ПРЕДЛАГАЕТ НПФ "ПРОМТЕХНИКА"



Суслин Ю.И.,
Директор НПФ "Промтехника"

Современное развитие производственных отношений предусматривает необходимость снижения себестоимости вагоноремонтного предприятия, что невозможно без дальнейшего развития поточных технологий с позиции создания технологических комплексов на основе комплексной механизации и автоматизации производственных процессов, в том числе для поточной технологии ремонта тележек грузовых вагонов. Это определяет новую более сложную и актуальную научно-техническую проблему создания перспективных средств комплексной механизации и автоматизации поточной технологии ремонта тележек грузовых вагонов, способных решить задачу снижения численности обслуживающего персонала и повышение комфортности его работы, исключение влияния человеческого фактора на качество процесса ремонта, повышение производительности и снижения себестоимости ремонта и, в конечном счете, обеспечение высокой степени безопасности движения поездов.

Разнообразие производственных помещений тележечного и колеснороликового цехов, многообразие их конфигураций и координат расположения относительно вагоносборочного цеха, обусловили большое разнообразие схем и средств механизации ремонтного производства. Неполное соответствие качества современного технологического оборудования всем требованиям, вытекающим из условий

эксплуатации, восполняется, как правило, их конструктивным многообразием.

В этой связи особую актуальность приобретает объективная систематизация, необходимая как для анализа и оценки схем механизации технологического процесса ремонта тележек грузовых вагонов, так и для определения степени технического совершенства, эффективности и комфортности работы, а также путей дальнейшего совершенствования существующей и создания новой техники для комплексной механизации и автоматизации процесса.

В результате анализа многочисленных существующих и возможных классификационных признаков показало, что наиболее общим, обладающим достаточной собирательной способностью и обеспечивающим объективность систематизации различных схем и конструктивно разнообразных средств механизации и автоматизации технологического процесса ремонта вагонных тележек, является функциональный признак элементов, определяющих структуру схем механизации. Такими функциональными элементами обусловленными технологическим процессом, являются:

— "П" — подготовка к реализации технологического процесса ремонта тележек грузовых вагонов, которая в общем случае должна включать: средства доставки узлов и деталей вагонной тележки в тележечный и колеснороликовый цех; поэтапную разборку тележки включая снятие с колесных пар, демонтаж триангелей, тормозной системы и системы пружин; обмывка и очистка тележки. В связи с чем для общего случая запишем формулу функционального элемента "подготовка":

$$\Pi = F(T; M; P), \quad (1)$$

где Т — средства транспортировки; Р — средства осуществляющие разборку; М — моечная машина.

— "Д" — диагностика деталей и узлов вагонной тележки, включающая в общем случае средства неразрушающего контроля и средства измерения геометрических параметров, а также контроль срока эксплуатации. Формула функционального элемента "диагностика" имеет вид:

$$D = F(D_{ц.к.}; D_{г.р.}; D_{с.с.}), \quad (2)$$

где D_{ц.к.} — диагностика неразрушающего контроля; D_{г.р.} — измерение геометрических параметров; D_{с.с.} — контроль усталостных изменений в металлоконструкции или контроль ее срока службы.

— "В" — восстановление заданных конструктивных, технологических и режимных параметров их контроль, а также осуществление операций по сборке, испытаниям и возвращению в вагоносборочный цех. Формула функционального элемента "восстановление":

$$V = F(H; K; C), \quad (3)$$

где H — ремонт и восстановление конструктивных параметров; K — контроль и испытание функциональных узлов; C — доставка и сборка в вагоносборочном цехе.

Функциональные элементы технологического процесса ремонта тележек грузовых вагонов в общей схеме механизации и автоматизации данного технологического процесса могут быть объединены для совместной работы путем наложения на них технологической (-), кинематической (+) и конструктивно (базисной) (*) связей.

Пользуясь приведенными ранее буквенными обозначениями символов функциональных структурных элементов и условными обозначениями связей между ними, можно классическую схему механизации, у которой имеют место все функциональные элементы, описать следующими общими структурными формулами:

при наличии технологической связи элементов П — Д — В; (4)

при наличии кинематической связи П + Д + В; (5)

при наличии конструктивной (базисной) связи П * Д * В. (6)

Полученные формулы определяют по существу структуру схем механизации и автоматизации процесса ремонта тележки грузовых вагонов, где функциональные элементы являются структурными элементами базовой формулы (4), названной так потому, что она описывает классическую схему технологического процесса ремонта тележки грузового вагона в самом общем виде и в ней четко выражены все функциональные элементы механизации этого процесса.

Различное сочетание структурных элементов и их связей приводит к образованию новых формул, определяющих структуру схем механизации процесса ремонта тележки грузового вагона в различных условиях эксплуатации.

Путем наложения соответствующих связей и вырождения структурных элементов можно получить целый ряд формул, производных от базовой.

В таблице 1 дано общее структурообразование схем и средств механизации технологического процесса ремонта тележек грузовых вагонов, из которой видно, что все полученные формулы разделились на шесть отличных друг от друга групп (I — VI).

Анализ полученных структурных формул и

сравнение их с современными схемами и средствами механизации процесса ремонта тележек грузовых вагонов показал, что структурными формулами I группы охватывается семейство обособленных машин и механизмов, каждая из которых имеют свою индивидуальную особенность. Поэтому они названы индивидуальными машинами и механизмами (ИМ).

II группа формул объединяет семейство наборов, кинематически не связанных между собой, индивидуальных машин и механизмов, необходимых и достаточных для механизации технологических операций процесса ремонта тележек грузовых вагонов.

Эти наборы машин и механизмов названы ремонтными комплектами (Рк).

III группа формул объединяет семейство наборов, в которых в неполной степени прослеживается наличие кинематических связей, но не потерявшие своих индивидуальных особенностей, и тем не менее имеющие набор необходимых и достаточных для механизации технологических операций процесса ремонта тележек грузовых вагонов. Эти наборы машин и механизмов занимают промежуточное положение между комплектами и комплексами, поэтому они названы ремонтными полуконструкциями (РПК).

IV группой формул охватывается семейство, кинематически связанных, но сохранивших свои индивидуальные особенности, машин и механизмов, комплексно механизующих все основные операции технологического процес-

са ремонта тележек грузовых вагонов. Они названы ремонтными комплексами (РК).

V группой формул охватывает семейство технологически согласованных, кинематически увязанных и частично соединенные конструктивными (базисными) элементами машин и механизмов, выполняющих все операции технологического процесса ремонта тележек грузовых вагонов. Машины и механизмы этой группы занимают промежуточное положение между ремонтными комплексами и ремонтными агрегатами, и поэтому они названы ремонтными полуагрегатами (РПА).

VI группа формул охватывает семейство технологически согласованных, кинематически увязанных и соединенных конструктивной (базисными) элементами машин и механизмов, выполняющих все операции технологического процесса ремонта тележек грузовых вагонов. Они названы ремонтными агрегатами (РА).

Каждая группа структурных формул отражает одновременно и качественную степень развития схем и средств механизации технологического процесса ремонта тележек грузовых вагонов. Причем каждая последующая группа формул описывает семейство машин и механизмов, находящихся на более высокой степени развития техники по ремонту тележек грузовых вагонов.

Для придания структурным формулам определенности, символы структурных элементов снабжаются соответствующими индексами, а при необходимости указываются их количест-

Таблица 1

Структурообразование схем и средств механизации технологического процесса ремонта тележек грузового вагона

Принципы построения структурных формул	Согласование элементов						Базовая формула	Сочленение элементов				Совмещение элементов									
	С вырождением							Частичное	Полное	С вырождением		Частичное	Полное	С вырождением							
Структурные Формулы	В	Д	П	В - Д	Д - П	В - П	В - Д - П	В + Д - П	В + П - Д	В + П - Д	В + Д + П	В + Д	В + П	Д + П	В * Д + П	В * П + Д	В + П * Д	В * Д * П	В * Д	В * П	П * Д
Группа формул	I			II			III			IV			V				VI				
Средства механизации ремонтного процесса	Индивидуальные машины и механизмы (ИМ)			Ремонтные комплекты (Рк)			Ремонтные полуконструкции (РПК)			Ремонтные комплексы (РК)			Ремонтные полуагрегаты (РПА)				Ремонтные агрегаты (РА)				

Примеры структурных формул реализованных технологических комплексов ремонта тележек грузовых вагонов

№ пп.	Наименование вагоноремонтных предприятий	Структурная формула	Уровень средств механизации	Год внедрения
1.	ВРД (Новокузнецк)	УРВТ-ММВТ-КПТ5п*{СРБ+ДПС+СУПМ}	III-ремонтные полукомплексы (РПК)	2006
2.	ВРД (Кандалакша)	УРВТ+НВТ4п*{УРС+ММВТ+УЗВТ}+ +КПТ11п*{ДПф+ДПС+СРТ+УРБ}-СИОТ	IY-ремонтные комплексы (РК)	2007
3.	ВРД (Магнитогорск)	УРВТ+НВТ4п*{УРС+ММВТ+УЗВТ}+ КПТ10п*{ДПф+ДПС+СРТ+УРБ+УСБ+УЗВТ}+ +НКП*{ССТ+СИОТ}+УРВТ	Y-ремонтные полуагрегаты (РПА)	2007
4.	Типовой проект (см. рисунок)	УРВТ+НВТ4п*{УРС+ММВТ+УЗВТ+СОКП}+ +КПТ11п*{ДПф+ДПС+СРТ+УСБ+СУПМ+СОВТ+ +УЗВТ}+НКП4п*{ССТ+СИОТ}+УРВТ	Y-ремонтные полуагрегаты (РПА)	2009

Индексы функциональных машин технологических комплексов:

УРВТ — установка разворота вагонной тележки; ММВТ — моечная машина вагонной тележки; КПТ5п — конвейер подачи тележки 5-ти позиционный; КПТ11п — конвейер подачи тележки 11-ти позиционный; СРБ — стэнд разборки боковин; ДПС — диагностическая платформа для установки СПРУТ-М (установка измерения диагностических параметров тележки); СУПМ — стэнд установки и клепки пластин модернизации; УРС — установка снятия каркаса тележки с колесных пар; УЗВТ — установка загрузки вагонной тележки; ДПФ — диагностическая платформа для МСН10 (установка феррозондового контроля); СРТ — стэнд раскантовки тележки; УРБ — установка разборки боковин; СИОТ — стэнд испытания и обмера тележки; НКП — накопитель есных пар; ССТ — стэнд сборки тележки; СОКП — сухая очистка колесных пар; СОВТ — система ориентации вагонной тележки

венные показатели. В таблице 2 представлены примеры структурных формул технологического оборудования для конкретных вагоноремонтных предприятий ОАО "РЖД" и частных вагоноремонтных заводов.

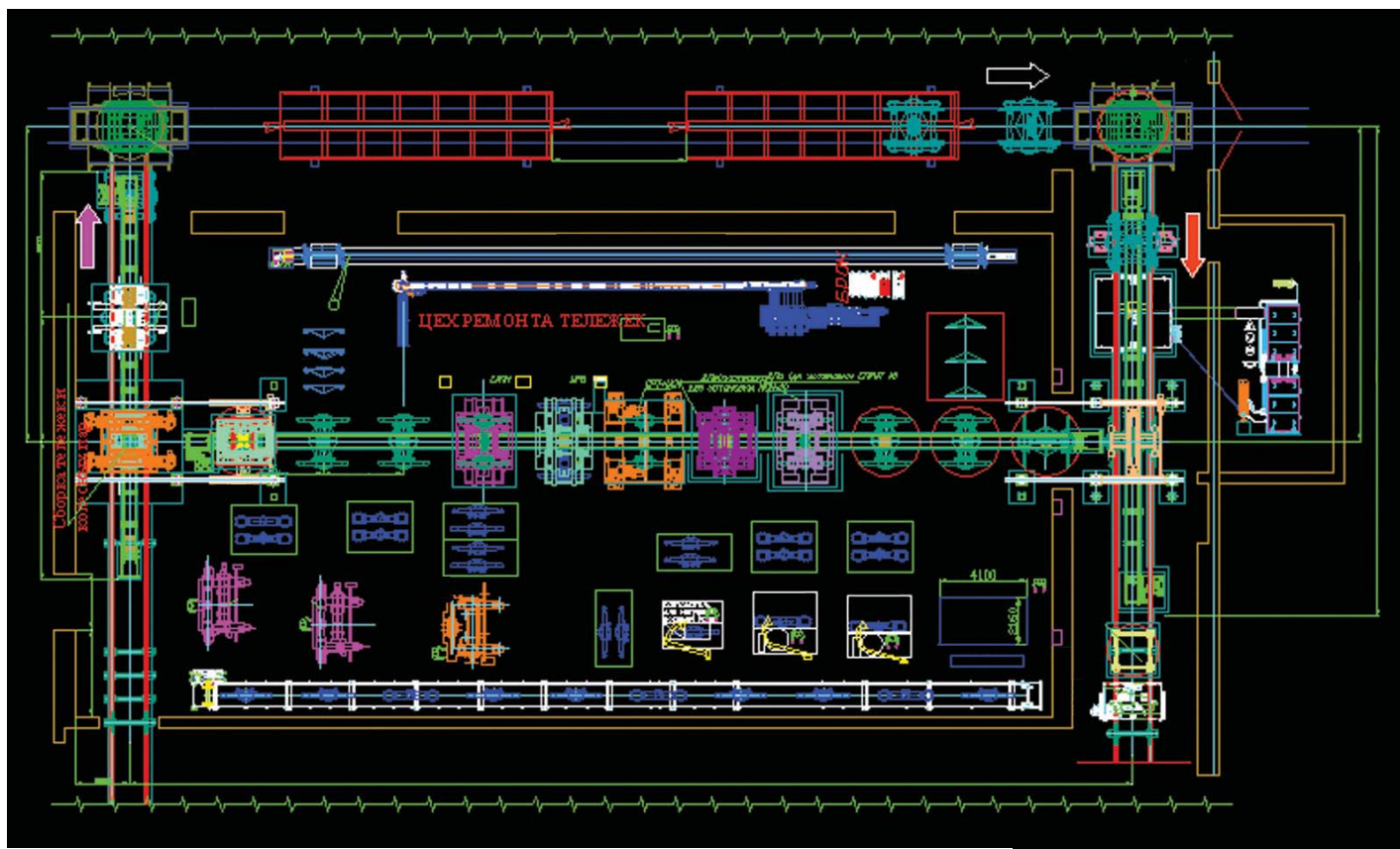
На рисунке представлен типовой проект технологического комплекса ремонта тележек грузовых вагонов определяющий IY группу формул, соответствующий наибольшей степени механизации современного техноло-

гического процесса ремонта тележек грузовых вагонов.

Аналогичным образом, используя представленную теоретическую методологию, могут быть составлены конкретные структурные формулы для любого тележечного и колесноролликового цехов вагоноремонтного предприятия и по ним можно определить к какой группе формул его следует отнести, а значит определить степень его совершенст-

ва, то есть это комплекты машин и механизмов, ремонтные комплексы или ремонтные агрегаты.

Разработанная технология создает теоретическую базу для повышения уровня механизации и автоматизации технологического процесса ремонта тележек грузовых вагонов на вагоноремонтном предприятии, что в свою очередь определяет уровень безопасности движения поездов.



Типовой проект технологического комплекса

МЕЖДУНАРОДНЫЙ КОНГРЕССНО-ВЫСТАВОЧНЫЙ ПРОЕКТ

НАВИГАЦИОННЫЕ СИСТЕМЫ, ТЕХНОЛОГИИ И УСЛУГИ

3-Й МЕЖДУНАРОДНЫЙ ФОРУМ

➤ ● **ПО СПУТНИКОВОЙ НАВИГАЦИИ**

12-13 МАЯ / www.glonass-forum.ru

МЕЖДУНАРОДНАЯ ВЫСТАВКА

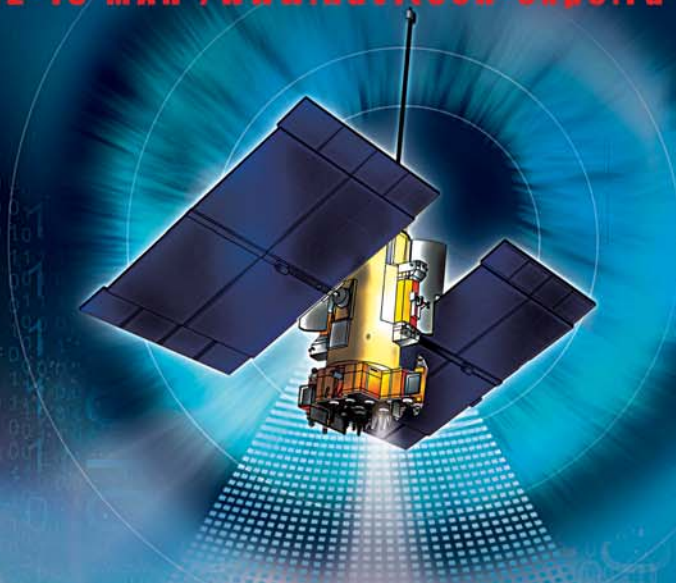
➤ ● **НАВИТЕХ-ЭКСПО**

12-15 МАЯ / www.navitech-expo.ru

12-15 мая

2009

**ЦВК «ЭКСПОЦЕНТР»
Москва, Россия**



**Генеральный
Информационный
Партнер**



**Генеральный
Интернет-Партнер**



При поддержке
Ассоциации разработчиков,
производителей и потребителей
оборудования и приложений
на основе глобальных навигационных
спутниковых систем
«ГЛОНАСС / ГНСС – Форум»
www.aggf.ru



Экспертные партнеры

- компания «М2М Телематика»
- GPS-CLUB (www.gps-club.ru) - сообщество любителей и профессионалов



ОРГАНИЗАТОРЫ ПРОЕКТА

 **ЭКСПОЦЕНТР**
МЕЖДУНАРОДНЫЕ ВЫСТАВКИ И КОНГРЕССЫ
МОСКВА

ЦВК «Экспоцентр»
Тел.: (499) 795 37 58, 795 37 39 / Факс: (495) 609 41 68
E-mail: navitech@expocentr.ru
www.navitech-expo.ru, www.expocentr.ru



**ПРОФЕССИОНАЛЬНЫЕ
КОНФЕРЕНЦИИ**

ООО «Профессиональные конференции»
Тел.: (495) 797 62 22 / Факс: (495) 797 62 23
E-mail: info@ptcentre.ru
www.glonass-forum.ru

Последствия воздействия некоторых несанкционированных сообщений ОКС-7 на сети связи общего пользования

ПОКАЗАНЫ ОСОБЕННОСТИ УГРОЗ "ОТКАЗ В ОБСЛУЖИВАНИИ" НА СЕТЕВОМ УРОВНЕ ОКС-7 И ПОСЛЕДСТВИЯ ПРИ ИХ РЕАЛИЗАЦИИ НА ФУНКЦИОНИРОВАНИЕ СЕТЕЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ.

М.Н. Даннави,
Аспирант кафедры
"Мультимедийные сети и услуги связи", МТУСИ

В рекомендации ITU-T Q.705 [1] указывается на необходимость защиты сетей от несанкционированных сообщений ОКС-7. Фальсификация злоумышленником сообщений обновления маршрутизации в сетях связи общего пользования может быть причиной серьезных последствий вплоть до нарушения функционирования части сети. Такие угрозы информационной безопасности относятся к типу "отказ в обслуживании" DoS (denial of services). В протоколах маршрутизации на межсетевом уровне IP-сетей предусмотрены стандартизированные механизмы защиты от атак, соответствующих этим угрозам информационной безопасности (стандарты RFC 2453, RFC 2082 и др.).

В некоторых зарубежных и отечественных публикациях последних лет отмечаются аналогичные угрозы информационной безопасности в ОКС-7, реализация которых может приводить к значительному ущербу функционирования сетей общего пользования ТфОП/ISDN, GSM и IN [2,3].

Угрозы "отказ в обслуживании" DoS воздействуют на качество обслуживания пользователей сетей общего пользования — ТфОП, сотовой сети стандарта GSM и интеллектуальной сети IN. Объясняется это тем, что ОКС-7 является составной частью этих сетей. Наибольший ущерб от таких угроз проявляется в отказе предоставления соединений одновременно большому количеству абонентов сети связи [2].

Угрозы DoS в ОКС-7 могут исходить от передаваемых злоумышленником ложных сообщений в результате "маскирования" под действительный пункт сигнализации. Наиболее серьезные последствия исходят от сообщений выполняющих следующие функции:

- управление сетью сигнализации МТРЗ (Message Transport Protocol level 3, подсистема

передачи сообщений на третьем уровне) [4,5];

- управление подсистемой SCCP (Signaling Connection Control Part, подсистема управления сигнальным соединением) [6, 7].

К таким сообщениям относятся:

- "недоступность подсистемы пользователя" UPU (Use Part Unavailable);

- "запрещение переноса сигнального графика" TFP (Transfer Prohibited);

- "переключение" COO (Changeover Order) и "аварийное переключение" ECO (Emergency Changeover).

- "доступ к подсистеме запрещен" SSP (Subsystem Prohibited);

- "подсистема SCCP перегружена" SSC (SCCP Subsystem Congested).

Фальсификация каждого такого сообщения образует группу угроз DoS ОКС-7 на различных участках сетей связи общего пользования.

Результаты анализа таких угроз показывают следующее:

1. Угрозам DoS ОКС-7 потенциально подвержены как абоненты фиксированной сети ТфОП/ISDN, так и пользователи мобильных станций сети GSM.

2. Угрозы DoS ОКС-7 проявляются при фальсификации сообщений обновления маршрутизации подсистемы МТРЗ сетевого уровня.

3. Реализация угроз DoS ОКС-7 может иметь место в результате фальсификации сообщений обновления маршрутизации между всеми смежными пунктами сигнализации сетей связи общего пользования.

4. Нарушению маршрутизации от воздействия угроз DoS ОКС-7 подвержены пункты сигнализации ОКС-7 смежные с пунктом сигнализации источником этих фальсифицированных сообщений обновления маршрутизации.

Местом локализации при тестировании, а также местом защиты от воздействия угрозы являются эти пункты сигнализации.

5. Нарушению маршрутизации от воздействия фальсифицированных сообщений подвергаются также пункты сигнализации, которые не являются смежными с указанными выше в п. 4 пунктами сигнализации. Однако эти пункты сигнализации не позволяют обеспечить защиту от угроз DoS ОКС-7 пункта сигнализации — источника угроз.

Отметим основные особенности последствий при реализации угроз DoS ОКС-7:

1. Риск при реализации угроз DoS ОКС-7 в результате фальсификации указанных сообщений подсистем МТРЗ отражается на пользователях сетями ОП (ТфОП/ISDN, GSM, IN) в части:

- отказа в установлении соединения;
- отказа в предоставлении всех или определенных услуг интеллектуальной сети;
- ухудшения качества обслуживания.

Под термином риск понимается последствие реализуемых угроз ИБ [8].

2. Риск при реализации угроз DoS ОКС-7 может относиться к следующим соединениям:

- а) В ТфОП/ISDN — международным, междугородным или местным.
- б) В GSM — внутри одного региона страны, между разными регионами страны, между мобильными абонентами разных стран.
- в) Между абонентами ТфОП/ISDN и абонентами GSM.
- г) В сети GSM мобильных абонентов домашней и абонентов-роумеров.

3. Важной особенностью этих угроз DoS проявляется в том, что последствия их реализации отражаются одновременно на большом числе пользователей сетями ОП.

4. Заинтересованными в защите от угроз DoS ОКС-7 являются [9]:

- пользователи в отношении доверия к сети и услугам, предоставляемым конкретным оператором/поставщиком услуг;
- операторы сетей и поставщики услуг в обеспечении защиты своих эксплуатационных и коммерческих интересов, в выполнении своих обязательств перед населением;
- органы государственной власти в выполнении директив и законов с тем, чтобы обеспечить готовность предоставления услуг и добросовестную конкуренцию.

Оценка последствий угроз DoS подсистем МТРЗ СССР ОКС-7 в сетях связи ОП. Предлагаемые в документах ITU-T и ETSI методы количественной оценки угроз ИБ не отражают особенности последствий воздействия угроз DoS подсистем сетевого уровня ОКС-7 в сетях свя-

зи ОП. Все эти методы основаны на экспертной оценке некоторых характеристик. Для сетей UMTS и услуги "универсальная персональная связь" UPT интеллектуальной сети количественная оценка производится для каждой угрозы. В случае UMTS эта величина рассчитывается на основании двух значений — следствие воздействия угрозы и вероятность ее реализации [10]. В случае услуги UPT каждая угроза дополнительно учитывает сложность реализации механизма защиты от нее [11]. В случае глобальной сети IN приводится оценка угрозы ИБ, которая относится к уязвимости конкретного сообщения прикладного уровня INAP, либо потока сообщений между функциональными объектами [12].

Оценка ИБ в этом случае производится по трем уровням:

- высокий, если информация содержит приватные или конфиденциальные данные;
- средний, если информация содержит адреса и данные по оплате;
- низкий, если информация относится к разведению соединений.

Анализ вышеприведенных особенностей угроз DoS ОКС-7 при фальсификации сообщений маршрутизации показывает, что для них упомянутый выше метод количественной оценки, используемый в интеллектуальной сети и сетевой сети UMTS [10-12] не подходит. Во-первых, для DoS ОКС-7 требуется качественная оценка риска, которая отражала бы все основные виды последствий реализации угроз.

Во-вторых, вероятность реализации угрозы DoS ОКС-7 практически оценить экспертным методом невозможно. Для того, чтобы оценить угрозы DoS ОКС-7 в сетях ОП используем так называемый показатель качества, определяемый окончательным пользователем во время эксплуатации QoE (Quality of end-user experience) [13-15]. Отметим разницу между QoE и показателем качества обслуживания согласно рекомендации E.800. Отличие между ними состоит в том, что QoS определяется требованиями оператора, а QoE — требованиями окончательного пользователя. QoS определяется оператором как готовность сети обеспечить обслуживание с гарантийным качеством. QoE показывает удовлетворен ли пользователь различными характеристиками обслуживания сети ОП при ее эксплуатации. К числу таких характеристик относится интегральная характеристика качества обслуживания (integrity of the service). Эта характеристика является обобщенным восприятием пользователем качества обслуживания сетью и состоит из многих показателей (задержка, джиттер и др.) К этим характеристикам относится и обеспечение информационной безопас-

ности. В данном случае к ним относится защита от угроз DoS ОКС-7 в сетях ОП из-за фальсификации сообщений обновления маршрутизации.

Термин QoE выражается в таких характеристиках человеческого восприятия, как "великолепно", "очень хорошо", "хорошо", "глухо", "очень плохо". Показатели QoS, выполнение которых оператором сети при ее проектировании не могут охватить полностью все аспекты, которые влияют на обобщенный показатель удовлетворенности пользователем качеством обслуживания QoE. Можно сказать, что цели оператора по обеспечению QoS являются важными для хорошего восприятия пользователем качества обслуживания QoE. При проектировании сети оператору связи важно знать все аспекты, которые влияют на QoE. Обеспечение защиты от угроз DoS ОКС-7 в сетях связи ОП из-за фальсификации сообщений обновления маршрутизации являются одними из важных задач, так как их реализация в значительной степени влияет на QoE.

Операторы сетей связи ОП, которые обеспечивают высокое QoE имеют большое преимущество в условиях конкуренции с операторами сетей с худшим QoE в отношении доходов, числа клиентов. Наблюдается цепная реакция, когда один разочарованный обслуживанием абонент сообщает о плохом QoE порядка тринадцати другим абонентам [14]. Оператор связи не имеет возможности получить от пользователей жалобы на качество обслуживания для того, чтобы оценить уровень качества обслуживания. Анализ показывает, что около 90% клиентов не жалуются, а просто покидают сеть оператора с плохим QoE [14]. Это дает основание полагать, что о последствиях реализации угроз DoS ОКС-7 в сетях ОП становится известно не только клиентам, непосредственно столкнувшимся с атаками.

Из вышеизложенного следует, что реализация угроз DoS ОКС-7 в сетях связи ОП частично отражается в показателе обобщенного восприятия качеством обслуживания пользователями сети оператора — QoE. Длительность нахождения сети в состоянии реализации угроз DoS ОКС-7, участок поражения сети (международный, междугородный, местный), отказ в предоставлении определенных услуг, а также число одновременно подверженных угрозам пользователей определяет уровень этих угроз ИБ в обобщенном показателе QoE.

Количественная оценка каждого из этих видов угроз DoS ОКС-7 может быть получена координатным путем в результате анализа журнальных записей аудита и системы извещений. Средства аудита позволяют записывать по-

дробную информацию о сообщениях обновления маршрутизации. Система извещений позволяет в реальном масштабе времени указывать на признаки атак, вызванных фальсификацией сообщений обновления маршрутизации с тем, чтобы выйти из состояния неработоспособности участка сети связи ОП. Обобщенный показатель пользователя сетью QoE по опыту эксплуатации может быть косвенной оценкой угроз DoS ОКС-7 в сетях ОП при фальсификации сообщений обновления маршрутизации.

Выводы

Результаты настоящей работы могут быть использованы при решении задач информационной безопасности сетей связи общего пользования ТфОП/ISDN, GSM и IN.

Литература

1. ITU-T recommendation Q.705 Specifications of signaling system № 7 signaling network structure, 1996

2. Ли Драйберг, Джефф Хьюитт. Система сигнализации № 7 (SS7/ОКС7). Протоколы, структура и применение. — М.: Вильямс, 2006.

3. Бельфер Р.А., Горшков Ю.Г. Анализ угроз информационной безопасности ОКС-7 типа отказ в обслуживании. Тезисы докладов Московской отраслевой научно-технической конференции "Технологии информационного общества". — М., 2007.

4. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Стек протоколов ОКС-7. Подсистема МТР. Справочник — М.: Радио и связь, 2003.

5. ITU-T Recommendation Q.704. Specification of signalling system № 7. Message transfer part. Signalling network functions and messages, 1996.

6. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Стек протоколов ОКС-7. Подсистема SСCP. Справочник. — СПб.: БХВ — Санкт-Петербург, 2006.

7. ITU-T Recommendation Q.716. Signalling System No. 7 — Signalling connection control part (SСCP) performance, 1993.

8. Брэгг Р., Родс-Оусли М., Страссберг К. Безопасность сетей. Полное руководство. — М.: "ЭКОМ", 2006.

9. ITU-T Recommendation E.408. Telecom-communication networks security requirements, 2004.

10. TS 121 133 — V3.2.0 — Universal Mobile Telecommunications System(UMTS); 3G Security: security threats and requirements (3G TS 21.133 version v320 release 2001).

11. ETSI ETR 083 / Universal Personal Telecommunication (UPT); General UPT Security architecture, 1993.

12. Contribution 19/2 SG 17 ITU-T. Towards the model for network security network, 2002.

13. Quality of Experience (QoE) of mobile services: Can it be measured and improved? NOKIA CORPORATION, 2004. www.nokia.com/NOKIA_COM_1/Operators/Downloads/Nokia_Services/whitepaper_qoe_net.pdf.

14. Soldoni D., Li M., Cuny R. QoS and QoE management in UMTS cellular Systems. "John Wiley & Sons" Ltd, 2006.

15. Бельфер Р.А., Даннави М.Н. Показатели качества обслуживания пользователей. Тезисы докладов Московской отраслевой научно-технической конференции "Технологии информационного общества". — М., 2007.

ТВ РОССИИ НА ПОРОГЕ ЦИФРОВОЙ ЭРЫ

Digital TV Russia 2009

Конкуренция • Конвергенция • Кооперация

2-3 апреля 2009 года • Holiday Inn MOSCOW – Suschevsky • Москва

2-ая Международная конференция

по технологическим, правовым и коммерческим аспектам развития цифрового ТВ в России

ЛИДЕРЫ ИНДУСТРИИ ЦИФРОВОГО ВЕЩАНИЯ НА КОНФЕРЕНЦИИ 2009 ГОДА!

Ключевыми темами для обсуждения станут наиболее актуальные вопросы:

- Взаимодействие государства, вещателей, операторов связи, финансовых институтов по поддержке финансовой устойчивости и стабильности медиаотрасли в условиях кризиса
- Законодательное обеспечение введения цифрового ТВ
- Влияние кризиса на бизнес-модели цифрового ТВ
- Контент как основа вещания во всех средах
- Развитие коммерческих сервисов цифрового ТВ: кабельное, мобильное, спутниковое ТВ, IPTV
- Стратегия развития каналов цифрового вещания в крупных центрах и в регионах

Организатор:



При поддержке:



Информационные партнеры:



Зарегистрируйтесь по телефону: +7 (495) 666-2244,
по e-mail: mail@infor-media.ru, или на сайте www.top-dtv.ru

При регистрации до 9 февраля сэкономьте 200 Евро!

На конференции выступят:

Представители НАТ, «Цифрового альянса России», Россвязькомнадзора

Себастьян Морис, Президент MPEGIP

Илья Пономарев, Председатель подкомитета по технологическому развитию комитета по информационной политике, технологиям и связи, Государственная Дума РФ

Александр Калинин, Первый заместитель генерального директора, ФГУП РТРС

Рустэм Султанов, Совладелец / Директор по развитию бизнеса, Немецкий музыкальный интерактивный телеканал IM1.TV

Евгений Соломатин, Директор по развитию, «Коминфо Консалтинг»

Константин Быструшкин, Заместитель Генерального директора, «МНИТИ»

Герасим Гадиян, Генеральный директор, НПК «ЭРА», Генеральный директор, HD Media

Екатерина Петухова, Эксперт, HDCC Ltd

***Александр Теппер**, Генеральный директор, «КОСМОС ТВ»

Артем Кудрявцев, Первый заместитель генерального директора по финансам и инвестициям, «Система Масс-медиа»

***Олег Колесников**, Технический директор, «НТВ Плюс»

* ожидается подтверждение

Годовой отчет Symantec по безопасности Messagelabs Intelligence 2008

Этот ежегодный отчет указывает на то, что 2008 год стал переломным с точки зрения кибербезопасности, так как революционные усовершенствования вредоносного ПО и методов спама наложили свой отпечаток на теневую экономику.

В феврале 2008 г. общий уровень спама достиг 82,7%, а средний уровень за год составил 81,2 против 84,6% в 2007 г. 90% всего спама распространялось бот-сетями, включая знаменитую сеть Storm (Peasomm), которая появилась на горизонте угроз в начале 2007 г. и почти исчезла к концу 2008 г., уступив место конкурирующим бот-сетям, таким как Srizbi и Cutwail (Pandex), пока меры, предпринятые сообществом в сентябре и ноябре, не привели к закрытию двух ISP в США, обвинявшихся в размещении командно-управляющих каналов некоторых крупнейших бот-сетей, включая Mega-D (Ozdok) и Srizbi, ответственных за 50% всего спама. Все пострадавшие сети, за исключением Srizbi, передислоцировались, так что уровень спама восстановился почти до тех же значений, что и до закрытия, а отсутствие Srizbi восполнили конкурирующие бот-сети, такие как Cutwail и Rustock.

В 2008 г. спамеры начали распространять спам через крупные, уважаемые службы веб-почты и приложений, обманывая механизм CAPTCHA (полностью автоматизированный открытый тест Тьюринга по распознаванию людей и машин) с целью создания большого числа персональных учетных записей в этих службах.

В 2008 г. получили распространение сложные вредоносные веб-программы, нацеленные на сайты социальных сетей и уязвимости легитимных веб-сайтов, что привело к установке вредоносного ПО на компьютеры без вмешательства пользователей. Число новых зараженных веб-сайтов, появляющихся каждый день, выросло с 1068 в январе до максимального значения в ноябре, составившего 5424. Среднее число ежедневно блокируемых новых веб-сайтов выросло в 2008 г. до 2290 с 1253 в 2007 г. — главным образом из-за усилившихся атак с применением методов SQL-инъекции.

Веб-атаки стали более популярными, а атаки через e-mail участились по сравнению с 2007 г. на 0,15%. При этом появились две новые тенденции в способах атак.

Рост популярности угроз подобного рода за прошедший год можно проиллюстрировать следующим примером: в конце июля была осуществлена целенаправленная троянская атака, нацеленная против фирмы, участвующей в организации Олимпийских игр, в результате чего в компьютер жертвы был внедрен вредоносный код, спрятанный во вложенном в электронное сообщение файле и использующий JavaScript для установки на компьютер исполняемой программы. Эта программа была передана нескольким спортивным организациям и представителям

спортсменов стран-участниц. В результате другой атаки, предпринятой с целью корпоративного шпионажа, известной фирме под видом жалобы на получателя было подброшено сообщение, в котором содержалось почти 900 целевых "троянских коней", предназначенных для высших руководителей этой организации во всем мире.

К концу 2008 г. кризис кредитной системы привел к множеству новых атак, нацеленных на финансовые организации: спамеры и мошенники пытались использовать панику и неопределенность, вызванные событиями на Уолл-стрит и во всем мире.

Основные тенденции 2008 г.

- **Веб-безопасность:** В 2008 г. среднее число новых вредоносных веб-сайтов, блокируемых за день, выросло до 2290 против 1253 в 2007 г.; рост на 82,8% произошел за счет увеличения числа атак с использованием метода SQL-инъекций.

- **Спам:** В 2008 г. средний уровень спама составил 81,2%, уменьшившись на 3,4% по отношению к уровню 2007 г. в 84,6%. В текущем году большая часть спама состояла из текстовых или HTML-сообщений, исходивших от известных поставщиков услуг веб-почты и приложений.

- **Вирусы:** Средний уровень вирусов в 2008 г. составил одно из 143,8 сообщений (0,70%), что на 0,15% меньше, чем в 2007 г., когда средний уровень составлял одно из 117,7 сообщений (0,85%). Снижение уровня можно объяснить переходом к распространению вредоносных программ с использованием в качестве основного способа заражения контента, размещаемого на веб-сайтах, и попутных загрузок вместо завлекающих сообщений e-mail.

- **Фишинг:** В 2008 г. число фишинговых атак составило одну на 244,9 сообщений e-mail (0,41%) против одной атаки на 156 сообщений e-mail в 2007 г. Пик активности фишеров пришелся на февраль, когда одно на каждые 99,1 электронных сообщений было фишинговым. Этот всплеск был вызван увеличением числа предлагаемых комплектов фишинговых инструментов plug-and-play и ростом использования для фишинга специализированных бот-сетей.

Годовой отчет Messagelabs Intelligence содержит более подробные сведения обо всех перечисленных выше тенденциях и дополнительные цифры, а также более детальное описание тенденций 2008 г.

Полный текст отчета находится на странице http://www.message-labs.com/Threat_Watch/Intelligence_Reports.

Отчет о состоянии подпольной экономики

Корпорация Symantec совместно с компанией Sofline выпустила "Отчет о состоянии подпольной экономики" (Report on the Underground Economy). Он содержит сведения об онлайн-черном рынке, который превратился в эффективный мировой рынок. На нем регулярно покупаются и продаются краденые товары и предлагаются основанные на мошенничестве услуги, причем стоимость товаров, предлагаемых отдельными продавцами, измеряется миллионами долларов. Отчет составлен на основе данных, собранных организацией Symantec Security Technology and Response (STAR) на серверах черного рынка в период с 1 июля 2007 г. по 30 июня 2008 г.

Потенциальная общая стоимость всех рекламируемых товаров черного рынка, обнаруженных Symantec за отчетный период, превысила 276 млн. долл. Эта сумма подсчитана, исходя из рекламируемых цен на товары и услуги, и соответствует выручке, которую получили бы рекламодатели, если бы им удалось реализовать весь свой товар.

Наиболее широко рекламируемой категорией товаров и услуг на черном рынке являются сведения о кредитных картах, на долю которых приходится 31% всех предложений. Хотя краденые номера кредитных карт продаются всего по 10-25 центов, средняя стоимость рекламируемой партии номеров кредитных карт превысила 4000 долл. Общая стоимость всех рекламируемых номеров кредитных карт за отчетный период, по расчетам Symantec, составила 5,3 млрд. долл.

Второй по популярности категорией рекламируемых товаров и услуг были банковские реквизиты, на долю которых пришлось 20% от общего объема черного рынка. Эти сведения продаются по цене от 10 до 1000 долл., но средняя стоимость рекламируемых краденых банковских реквизитов приближается к 40 тыс. долл. Таким образом, общая стоимость рекламируемых краденых банковских реквизитов за отчетный период составила 1,7 млрд. долл. Популярность этой информации на черном рынке можно объяснить высоким и быстрым потенциальным доходом. В одном из случаев средства с банковских счетов были переведены в неизвестном направлении менее чем за 15 минут.

В течение отчетного периода Symantec зафиксировала 69130 активных рекламодателей и 44321095 сообщений, опубликованных на подпольных форумах. Потенциальная стоимость всех рекламируемых товаров десяти наиболее активными рекламодателями составила 16,3 млн. долл. для номеров кредитных карт и 2 млн. долл. для банковских реквизитов. Более того, потенциальная стоимость товаров, рекламируемых самым активным рекламодателем, составила 6,4 млн. долл.

С географической точки зрения подпольная экономика очень разнообразна. Она приносит доход киберпреступникам самых разных мастей от слабо сплоченных групп до организованных коллективов со сложной иерархией. В течение отчетного периода наибольшее число серверов черного рынка наблюдалось в Северной Америке (45%). На долю региона EMEA пришлось 38% таких серверов, на долю Азиатско-Тихоокеанского региона — 12%, а на долю Латинской Америки — всего 5%. Во избежание обнаружения подпольные серверы постоянно меняют свое географическое положение.

Более подробные сведения и цифры по черному рынку можно получить на следующих ресурсах:
http://eval.symantec.com/mktginfo/enterprise/whitepapers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf
http://eval.symantec.com/mktginfo/enterprise/whitepapers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf.

Результаты разработки метода расчета пропускной способности сетей подвижной связи

ОСОБЕННОСТЬЮ СЕТЕЙ ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ (СПРС-ОП) ЯВЛЯЕТСЯ МОБИЛЬНОСТЬ ПОЛЬЗОВАТЕЛЕЙ И ИХ НЕРАВНОМЕРНОЕ РАСПРЕДЕЛЕНИЕ НА ТЕРРИТОРИИ СЕТИ, А ТАКЖЕ НЕОБХОДИМОСТЬ ОЦЕНКИ ВЛИЯНИЯ МУЛЬТИМЕДИЙНЫХ ПРИЛОЖЕНИЙ, ДЛЯ РЕАЛИЗАЦИИ КОТОРЫХ ТРЕБУЕТСЯ ПОВЫШЕННАЯ СКОРОСТЬ ПЕРЕДАЧИ ИНФОРМАЦИИ. ПРЕДСТАВЛЕНЫ РЕЗУЛЬТАТЫ РАЗРАБОТКИ МЕТОДА РАСЧЕТА ПРОПУСКНОЙ СПОСОБНОСТИ СПРС-ОП.

Степанова И.В.,
Кондратов А.Г.,
МТУСИ

Преобладающим видом трафика в СПРС-ОП является телефонный трафик, объем которого в России неуклонно растет, так же как и число мобильных абонентов. В тоже время быстро растет объем мультимедийного трафика, для которого перспективно выделение на время сеанса связи группы каналов в радиointерфейсе базовой станции и формирование высокоскоростного информационного потока на различных участках мобильной сети и на стыке с другими телекоммуникационными структурами. С одной стороны решается задача быстрой передачи ограниченных объемов данных между мобильными абонентами и создается возможность интерактивного режима обмена информацией. С другой стороны групповой режим обслуживания заявок, предусматривающий объединение нескольких каналов, повышает вероятность отказов в обслуживании групповой заявки.

В таблице 1 представлены результаты расчета вероятности потерь по вызовам, выполнен-

ного для вариантов совместного и дифференцированного использования ресурса каналов в радиointерфейсе базовой станции. Величина λ характеризует интенсивность поступления вызовов. Величины $P_{отк1}$ и $P_{отк4}$ характеризуют, соответственно, вероятность отказа в обслуживании из-за занятости всех каналов трафика в радиointерфейсе для вызова телефонии (занимается один канал) и для мультимедийного вызова (занимаются четыре канала). Величины F_1 и F_4 характеризуют, соответственно, долю вызовов телефонии и долю вызовов мультимедиа, $F_1 + F_4 = 1$.

Проведенные исследования показали, что раздельное или дифференцированное использование ресурса каналов радиointерфейса может становиться перспективным даже при сравнительно небольшой доле заявок на групповое обслуживание. Для рассмотренного примера выделение пучка группового обслуживания емкостью $V_4 = 16$ каналов позволяет обеспечивать допустимую вероятность потерь по вызовам вплоть до случая возрастания параметра совокупного потока $\lambda_{доп}$ до величины 7496 вызовов в час при условии, что доля групповых заявок F_4 может возрасть до $F_4 = 1470 / 7496 = 0,196$. Допустимое число вызовов телефонии составляет $\lambda_{1доп} = 6026$ вызовов в час. Если сравнить для этого значения результаты аналитических расчетов дифференциального и совместного использования ресурса каналов, то можно сделать вывод о перспективности выделения отдельного пучка группового обслуживания уже при доле заявок на групповое обслуживание $F_4 = 0,05$. Так, при $\lambda_1 = 6000$ вызовов в час совместное использование ресурса каналов дает плохие показатели: $P_{отк1} = 3,21 \cdot 10^{-2}$ и $P_{отк4} = 1,31 \cdot 10^{-1}$.

Показатели, аналогичные дифференциаль-

Таблица 1

Результаты аналитической оценки совместного и дифференцированного использования ресурса каналов при поступлении смешанного потока вызовов

Совместное использование ресурса каналов $V = 192$ канала трафика при поступлении смешанного потока вызовов				
λ , вызовы в час	F_1	F_4	$P_{отк1}$	$P_{отк4}$
5100	0,95	0,05	$1,26 \cdot 10^{-3}$	$5,92 \cdot 10^{-3}$
5400	0,95	0,05	$5,23 \cdot 10^{-3}$	$2,34 \cdot 10^{-2}$
5700	0,95	0,05	$1,48 \cdot 10^{-2}$	$6,36 \cdot 10^{-2}$
6000	0,95	0,05	$3,21 \cdot 10^{-2}$	$1,31 \cdot 10^{-1}$
6000	0,80	0,20	$1,11 \cdot 10^{-1}$	$4,04 \cdot 10^{-1}$
Дифференцированное использование ресурса каналов при поступлении смешанного потока вызовов с выделением $V_{гр} = V_4 = 16$ каналов				
$P_{отк1}$	$\lambda_{доп}$, вызовы в час	$P_{отк4}$	$\lambda_{доп}$, вызовы в час	$\lambda_{доп}$, вызовы в час
$5 \cdot 10^{-2}$	1470	$1,136 \cdot 10^{-2}$	6026	7496

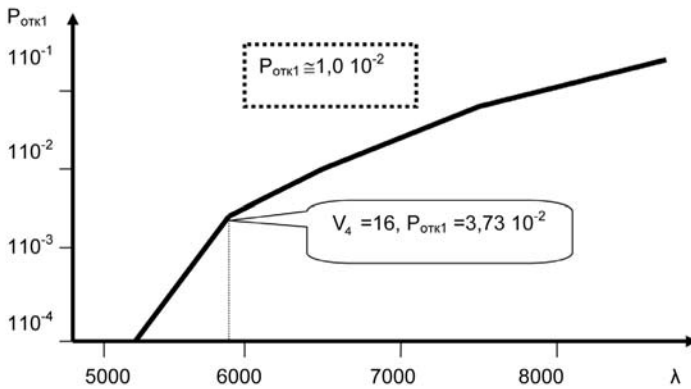


Рис. 1. Зависимость вероятности $P_{отк1}$ от интенсивности вызовов простейшего потока вызовов при $F_4 = 0,20$ и $P_{отк4} \approx 1,0 \cdot 10^{-2}$

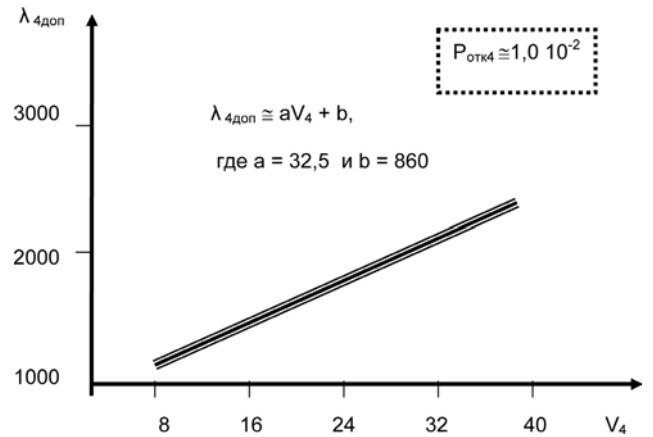


Рис. 2. Зависимость допустимой интенсивности потока групповых заявок от числа каналов трафика V_4 в выделенном пучке обслуживания групп заявок при $F_4 = 0,20$ и $P_{отк4} \approx 1,0 \cdot 10^{-2}$

ному использованию ресурса каналов могут быть достигнуты при $\lambda_1 = 5100$ вызовов в час, то есть реализация выделенного канала группового обслуживания позволяет повысить допустимую величину параметра потока на 15%, при этом предусматривается возможность изменения показателя F_4 в диапазоне $F_4 \leq 0,196$.

В таблице 2 сделана выборка результатов для фиксированных значений $P_{отк4} \approx 1 \cdot 10^{-2}$, результаты которой также отражены на рис. 1, 2. Установлено, что при фиксированном допустимом значении вероятности $P_{отк4}$ (например, при $P_{отк4} \approx 1,0 \cdot 10^{-2}$ допустимая интенсивность потока вызовов $\lambda_{4доп}$ линейно зависит от числа каналов в выделенном пучке группового обслуживания $\lambda_{4доп} \approx aV_4 + b$, где $a = \text{const}$ и $b = \text{const}$ (для данного случая $a = 32,5$ и $b = 860$). Может быть определена допустимая величина $\lambda_{1доп} = \lambda_{4доп} (F_1/F_4)$.

Метод раздельного использования ресурса каналов при введении группового обслуживания мультимедийных заявок основывается на общем выводе о целесообразности выделения отдельного пучка каналов, предназначенного только для обслуживания групповых заявок мультимедийных услуг, и включает в себя следующие этапы.

1. Сначала должна выполняться оценка или прогнозирование реальной или ожидаемой в

ближайшее время доли вызовов с привлечением дополнительных услуг, требующих повышенной скорости передачи. Может также прогнозироваться перспективность выделения отдельных каналов для работы в режиме потокового трафика stream.

2. Уточнение диапазона изменения параметра потока вызовов в течение суток и в ЧНН по результатам данных статистики и интенсивности обслуживания вызовов, характерной для данной сети мобильной связи.

3. Уточнение особенностей построения конкретной сети мобильной связи и имеющегося ресурса каналов на различных участках сети мобильной связи.

4. Изучение необходимости перехода к дифференциальному обслуживанию исходя из имеющегося ресурса каналов в радиоинтерфейсе базовой станции и предполагаемой доли вызовов с привлечением дополнительных услуг. Расчет вероятности потерь по вызовам, требующим занятия одного канала или группы каналов, путем решения системы уравнений равновесия.

5. Выбор варианта выделения отдельного пучка каналов для обслуживания групповых заявок (с использованием ресурса каналов трафика или с использованием возможностей каналов синхронизации или управления).

6. Проведение аналитических расчетов для варианта дифференциального использования каналов с целью получения зависимости $\lambda_{доп} = F(V_{гр})$ и уточнения коэффициентов линейной зависимости.

7. Выбор емкости пучка группового обслуживания с учетом данных статистики по интенсивности поступления вызовов.

Выводы

1. Развитие средств связи предполагает широкое внедрение мультимедийных услуг. Объединение нескольких каналов в радиоинтерфейсе базовой станции в единый цифровой поток, выполняемое с целью снижения общего времени передачи информации, существенно повышает вероятность отказов в обслуживании групповой заявки и ведет к возникновению значительных дополнительных потерь по вызовам.

2. Проведенные исследования показали, что выделение специальных пучков каналов для обслуживания мультимедийных заявок становится перспективным даже при сравнительно небольшой доле заявок на групповое обслуживание.

Литература

1. Степанова И.В. Проектирование сетей мобильной связи // Труды МТУСИ: Сборник статей. — М., 2004. — С. 139-146.
2. Генеральная схема создания и развития федеральной сети подвижной радиотелефонной связи общего пользования России стандарта GSM (Одобрено решением ГКЭС от 25.12.2002 № 50). — М., 2003.
3. Степанова И.В., Кондратов А.Г. Результаты аналитической оценки вероятности потерь по вызовам в радиоинтерфейсе базовой станции // Международный форум информатизации (МФИ-2007): Труды конференции "Телекоммуникационные и вычислительные системы". — М.: МТУСИ, 2007. — С.112-113.

Таблица 2

Результаты расчета вероятности отказов в обслуживании заявок при раздельном использовании каналов трафика

V = 192 канала; длительность телефонного разговора $t_1 = 100$ с; длительность передачи мультимедийного сообщения $t_4 = 8$ с					
V ₄ =8			V ₄ =16		
λ, вызовы в час	P _{отк1}	P _{отк4}	λ, вызовы в час	P _{отк1}	P _{отк4}
5500	0.0	0.0	5500	0.0	0.0
6000	$3,4 \cdot 10^{-5}$	$1,954 \cdot 10^{-1}$	6000	$3,0 \cdot 10^{-4}$	0.0
7000	$6,6 \cdot 10^{-3}$	$6,242 \cdot 10^{-1}$	7000	$1,8 \cdot 10^{-2}$	0.0
7500	$2,5 \cdot 10^{-2}$	$8,19410^{-1}$	7500	$4,8 \cdot 10^{-2}$	$7,1 \cdot 10^{-2}$

1-3 апреля 2009 года в г. Астане пройдет III Международная выставка-форум информационно-коммуникационных технологий «e-KAZAKHSTAN», организаторами которых выступают Агентство Республики Казахстан по информатизации и связи и выставочная компания «Астана-Экспо КС». Выставка пройдет в новом выставочном комплексе «Корме» Центра международной торговли Астана, который построен и оснащен в соответствии с самыми высокими международными стандартами.

В выставке участвуют крупнейшие мировые поставщики информационных технологий, отечественные и зарубежные производители телекоммуникационного оборудования, компьютеров и программного обеспечения, средств и систем безопасности.

Это уже третья по счету выставка, на которой ее участники продемонстрируют последние достижения и полный спектр своих технологических решений и услуг, а также продолжат обсуждение актуальных проблем, связанных с реализацией Государственной программы формирования «электронного правительства» и «информационного общества» в Республике Казахстан.



e-KAZAKHSTAN

III Международная выставка-форум
информационно-коммуникационных технологий

1-3
сәуір апреля
2009

Выставочный центр «КОРМЕ»

Основные разделы выставки:

- ! Возможности портала электронного правительства, удостоверяющих центров, республиканских и региональных ведомственных информационных систем, баз данных, единой транспортной среды госорганов, применяемые стандарты
- ! Преодоление «цифрового неравенства»
- ! Возможности институтов развития, ПИТ в реализации Программы; прикладных программ для государственных органов и существующих прогрессивных технологий в других странах
- ! Аппаратные средства
- ! Программное обеспечение
- ! Системная интеграция
- ! Информационная безопасность
- ! Услуги по разработке программного обеспечения
- ! IT-консалтинг
- ! Сетевые решения
- ! Беспроводные решения
- ! Цифровое теле-, радиовещание
- ! Электронная культура (электронные СМИ, электронные библиотеки и музеи)

справки по телефонам:

+ 7 (7172) 52-43-23

+ 7 (7172) 52-43-24

+ 7 (7172) 52-43-25

natali@astana-expo.com
info@ekaz.kz

<http://www.ekaz.kz>



digital communication



Центрально-Азиатская Международная Выставка
ТЕЛЕКОММУНИКАЦИИ И КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ



Kitel

26-29 мая 2009
Казахстан, Алматы



ИТЕСА Алматы: Тел.: +7 727 2583434;
Факс: +7 727 2583444; E-mail: telecoms@iteca.kz



ИТЕ Москва (Россия)
Тел.: +7 (495) 935 7350 #4123
Факс: +7 (495) 935 7351; e-mail: Kochergina@ite-expo.ru

Развитие казахоязычного Интернет-пространства

ОДНИМ ИЗ САМЫХ ЗАМЕТНЫХ ЯВЛЕНИЙ В МИРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ЯВЛЯЕТСЯ ИНТЕРНЕТ. ПОЯВИВШИЙСЯ ИЗ ВОЕННЫХ РАЗРАБОТОК, ОН НАЧАЛ СВОЕ РАЗВИТИЕ В СРЕДЕ УНИВЕРСИТЕТОВ И ВСЕГО ЗА НЕСКОЛЬКО ЛЕТ ИЗМЕНИЛ ЖИЗНЬ ПОЧТИ ВСЕГО ЗЕМНОГО ШАРА. В ДАННОЙ СТАТЬЕ ПРИВОДЯТСЯ ДАННЫЕ ПО ТЕКУЩЕМУ СОСТОЯНИЮ КАЗАХОЯЗЫЧНОГО ИНТЕРНЕТ-ПРОСТРАНСТВА, ПОТРЕБНОСТИ ГРАЖДАН РЕСПУБЛИКИ В КАЗАХОЯЗЫЧНЫХ САЙТАХ, АНАЛИЗУ КАЧЕСТВА И СОДЕРЖАНИЯ ИНФОРМАЦИИ НА НИХ, РЕЙТИНГУ САЙТОВ.

Сеилов Ш.Ж.

Президент, д.э.н.,

Казахская Академия инфокоммуникаций

Жуманов Ж.М.

Исполнительный директор, MCS,

Казахская Академия Инфокоммуникаций

Введение

Интернет в результате своего стремительного развития из явления технического превратился в часть социальной жизни планеты, стал "междисциплинарным" явлением. Вместе с проблемами доступа и скоростей передачи данных в настоящее время большая часть внимания специалистов уделяется проблемам информационного содержания (контента), правового регулирования Интернет, влиянию Сети на различные аспекты жизни общества.

Не последнее место в данном списке занимает представление в Интернет адекватной и актуальной информации о различных странах и культурах. В настоящее время имидж любого государства напрямую зависит от того образа, который формируется у миллионов активных пользователей Интернет. В последние годы частым стало употребление терминов "Информационное взаимодействие" и "Информационное противостояние" применительно к общению пользователей различных ресурсов Интернет.

Все это говорит о том, что Интернет стал одним из важнейших факторов всестороннего развития государства. И очень важно уделять пристальное внимание к его развитию в стране.

Учитывая то, что казахоязычный Интернет является неотъемлемой частью Казнет, почти все черты Казнета присущи и казахоязычным сайтам. Статья основана на матери-

алах исследования казахоязычного Интернет-пространства, которое Казахская Академия Инфокоммуникаций проводило в текущем году по заказу Министерства культуры и информации Республики Казахстан.

Анализ текущего состояния казахоязычного Интернет-пространства

1. Казахский язык и количество его носителей в мире

Казахский язык является государственным языком Республики Казахстан. Казахский язык входит в кыпчакскую подгруппу тюркских языков (в нее также входят: татарский, башкирский, карачаево-балкарский, кумыкский, караимский, крымскотатарский, каракалпакский, карагачский, ногайский). Вместе с ногайским, каракалпакским и карагачским языками казахский язык относится к кыпчакско-ногайской ветви.

Население Республики Казахстан по данным Агентства Республики Казахстан по статистике, на 1 сентября 2008 г. составляло 15 713 157 человек. Национальный состав Казахстана, в процентах от всего населения представлен в таблице 1.

Таблица 1

Национальный состав населения РК	
Народы	%
Казахи	59,2
Русские	25,6
Украинцы	2,9
Узбеки	2,9
Уйгуры	1,5
Татары	1,5
Немцы	1,4
Другие	5,0

По данным переписи населения 1999 г. в Казахстане родным языком свободно владело 98% казахов. Если провести аналогию с последними данными по населению, то на сегодняшний день в Республике Казахстан более 9 млн человек владеют казахским языком. По статистическим оценкам, всего на казахском языке говорят в мире около 12 млн человек, из них в Казахстане — более 9 млн человек, в остальных странах СНГ — 2 миллиона, в Китае — 1,5 млн. Кроме того, казахский язык распространен в Монголии, Афганистане, Пакистане, Иране, Турции, Германии.

Таким образом, можно констатировать, что в мире существует значительная потенциальная аудитория потребителей информации на казахском языке, из которой 25% проживает за пределами территории Республики Казахстан.

2. Данные по операторам доступа к сети Интернет в Республике Казахстан

По данным Агентства Республики Казахстан по информатизации и связи, на осуществление деятельности по предоставлению услуг доступа к сети Интернет АИС РК всего было выдано 776 лицензий 403 компаниям, из них 14 лицензий были приостановлены и 177 аннулированы.

Всего на рынке доступа к сети Интернет в Казахстане предоставляет услуги более 39 субъектов, наибольшую рыночную долю из которых занимают АО "Казакхтелеком", АО "Нурсат", АО "Арна" и АО "Astel".

По данным Агентства Республики Казахстан по статистике предприятиями связи за январь-декабрь 2007 г. оказано услуг на сумму 314 млрд тенге, что в сопоставимых ценах на 14,5% больше объема аналогичного периода прошлого года.

При этом структура доходов от услуг телекоммуникаций такова: мобильная связь занимает — 51,4%, фиксированная связь — 24,9%, передача данных и Интернет — 8,7%, IP-телефония — 1,7%, услуги платного TV — 3,9 и другие виды связи — 9,4% (рис. 1).

Наиболее высокие темпы по сравнению с 2006 г. демонстрируют предприятия, предоставляющие услуги Интернета службы передачи данных, мобильной связи, службы передачи данных. Таким образом, услуги по передаче данных и Интернет занимают важное место в телекоммуникационной отрасли и, соответственно, в экономике Республики Казахстан. Учитывая то, что данный сектор является одним из быстроразвивающихся, можно с уверенностью утверждать, что с технической стороны развитие Казнета в ближайшие годы должно быть обеспечено на должном уровне.

3. Оценка общего состояния сети Интернет в Казахстане

Пользователи услуг сети Интернет

Для оценки развития сети Интернет в стране в мировой практике используется понятие "Проникновение Интернет". Этот показатель представляет собой количество пользователей сети Интернет на 100 человек населения страны.

Важным является то, каким образом пользователи подключаются к сети Интернет. Традиционным и самым распространенным является подключение с использованием телефонной линии. Можно подключаться, используя коммутируемое подключение — через аналоговый модем, или, более современное решение, — с использованием технологии ADSL. Другими вариантами подключения к Интернет могут быть: беспроводные сети, спутниковое подключение, подключение через мобильные устройства.

Рисунок 2 иллюстрирует проникновение Интернет в Казахстане и показывает, какую долю составляют пользователи ADSL (услуга АО "Казхателеком" "Мегалайн").

На рисунке 3 представлен график роста проникновения Интернет в Казахстане за 2000-2007 гг.

Таблица 2

Возрастной состав пользователей Интернет	
Возрастная группа	Доля
моложе 18	21,3
18-24	34,1
25-30	15,0
31-35	9,5
36-40	7,2
41-50	9,5
51-60	3,4

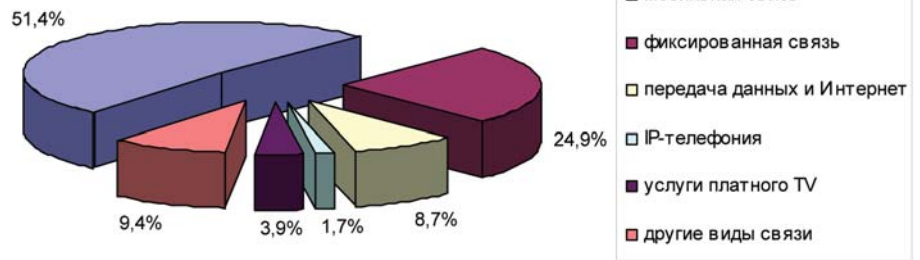


Рис. 1. Структура доходов от услуг телекоммуникаций

Также следует отметить, что в 2008 г. были неоднократно снижены тарифы доступа к сети Интернет. Для пользователей широкополосного доступа с 1 марта 2008 г. были сняты ограничения по трафику на все ресурсы, входящие в IP-адресное пространство АО "Казхателеком" и повышена скорость доступа на внутренние ресурсы до 256 кбит/с. С 1 июня 2008 г. была повышена скорость доступа на внутренние ресурсы до 512 кбит/с.

По приведенным данным можно судить о том, что Интернет в Казахстане становится все доступнее широким слоям населения, о чем свидетельствует увеличивающиеся темпы

роста количества пользователей.

Динамика увеличения количества доменных имен

По оценкам специализированных сервисов, с начала 2008 г. количество сайтов в Казнете увеличилось ориентировочно с 5 000 до 6 000. Это говорит о том, что в месяц в Казнете появляется около 100 сайтов.

В таблице 3 представлены данные по количеству доменных имен, регистрируемых в доменной зоне .kz. За последние 3 года наблюдается устойчивый рост количества доменных имен.



Рис. 2. Уровень проникновения Интернет в Казахстане

*Источник: <http://www.internetworldstats.com>

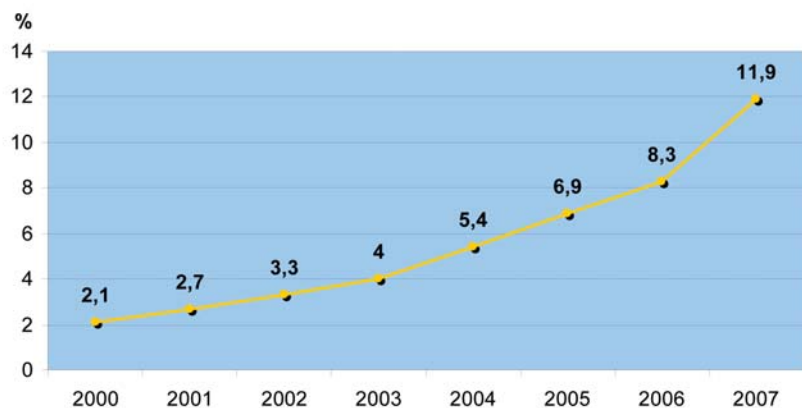


Рис. 3. Динамика уровня проникновения Интернет в Казахстане

Таблица 3

Динамика роста доменных имен

Страна	Зона	2004г.	2005г.	2006г.	2007г.
Россия	.RU	305 632	446 729	718 101	1 157 567
Россия (СССР)	.SU	3 420	4 906	8 152	30 492
Украина	.UA	133 907	169 644	241 666	335 073
Казахстан	.KZ	н/д	9 574	16 431	26 293
Узбекистан	.UZ	н/д	3 155	3 621	5 767
Германия	.DE	8 266 466	9 378 395	10 422 702	11 673 389
Весь мир	-	70 500 k	91 000 k	120 000 k	156 000 k

Кодировки казахского языка

Долгое время в Казахстане активно обсуждалась проблема представления символов казахского алфавита в компьютерных программах и в Интернет. Суть проблемы заключалась в том, что в прошлом при разработке многих программных продуктов не учитывалось использование символов, отличных от тех, что присутствуют в алфавите английского языка. При наличии дополнительных символов, как во многих европейских языках, или при использовании, к примеру, кириллицы или иероглифов, приходилось создавать новые наборы шрифтов. До некоторого времени создание этих наборов шрифтов происходило нецентрализованно. В результате этого для одного и того же языка оказывалось по нескольку несовместимых между собой наборов. К примеру, для русского языка широкое распространение получили:

- кодовая страница 866;
- кодовая страница 1251;
- KOI-8R;
- ISO-8859-5.

Для казахского языка также было создано несколько вариантов:

- KazWin;
- Kaz;
- KaZ;
- KZ;
- KZ-bis;
- KZ-1048.

После широкого распространения стандартов Unicode, данная проблема перестала быть актуальной для пользователей современных программных продуктов. Старые версии программного обеспечения все еще могут иметь проблемы с правильным отображением, но, как правило, для них предусмотрены специальные механизмы обновления, помогающие решить подобные проблемы.

На данный момент для web-страниц на казахском языке рекомендуемой является кодировка UTF-8. Поскольку этот формат основывается на Unicode, то эта кодировка применима для оформления web-страниц на любом языке. Проблема может быть только в том, что в конкретных шрифтах, которые использует программа-браузер на вашем компьютере, может не оказаться полного набора символов, необходимых для демонстрации текста на избранном языке. Кодировка UTF-8 в настоящее время поддерживается всеми современными браузерами.

С использованием UTF-8 не требуется устанавливать разные специальные "казахские" шрифты, типа Kaz, KaZ, KZ. Большинство из них нестандартны, они и породили нынешнюю путаницу в кодировках. Достаточно просто обновить базовые шрифты, их свежие версии поддерживают казахский язык наряду с другими языками. При работе над веб-сайтами все инструменты для создания web-страниц позволяют сохранять созданные документы в кодировке UTF-8 без необходимости знания технических деталей.

Перевод казахского алфавита на латиницу

Одним из вариантов решения проблемы с кодировками было предложение перехода на алфавит с использованием латинских символов. Основным аргументом приверженцев этой идеи было то, что клавиатура современного компьютера создана для латинской графики, поэтому перевод казахского языка на нее позволит решить все проблемы. Оппоненты перехода утверждают, что клавиатура и вообще современный облик компьютера — дело временное. С появлением более совершенной техники, учитывающей особенности языка, переход на нее будет намного проще,

столь радикальной реформы языка. Переход же на латиницу обязательно вызовет большой ряд проблем, в культуре, языкознании, библиотечном деле, сохранении интеллектуального наследия. На сегодняшний день есть некоторое количество сайтов, которые используют для казахского языка, как кириллицу, так и латиницу. Однако, как было описано в предыдущем разделе, в настоящее время проблема отображения символов казахского языка уже решена более экономичным способом.

Следует отметить и то, что казахская письменность не самая уникальная. К примеру, еврейский (12-14 миллионов носителей), арабский (420 миллионов носителей) или китайский языки, не смотря на свои общеизвестные особенности, без больших проблем используются в Интернет.

Государственная политика и правовое регулирование Интернет

О значительной востребованности развития Казнета и казахоязычного Интернета свидетельствует то, внимание к этой области, которое уделяется государством. Государственный подход к управлению Интернетом имеет междисциплинарную природу и базируется на пяти основных аспектах:

Первый аспект — это управление телекоммуникационной средой доступа в Интернет, широкополосный доступ в Интернет, управление доменными именами, сервисами и вопросы стандартизации.

Второй аспект связан с сокращением цифрового разрыва. Цифровой разрыв — это понятие, введенное для социологической оценки по всей местности применения Интернета в обществе. В данном случае мы рассматриваем его как разрыв между использованием Интернета в городе и в сельской местности.

Третий аспект — экономический. Имеются в виду инвестиции в область Интернет-торговли, электронная цифровая подпись, Интернет-банкинг и т.д.

Четвертый аспект — социокультурный. Подразумевается многоязычие в Интернете. Для казахстанского Интернета безусловный приоритет — это развитие государственного языка.

Пятый аспект — правовой. Это одно из самых важных направлений, которое связано с развитием нормативно-законодательной базы, это — пользование цифровой подписью, закон об авторском праве, торговой марке и т.д.

О том, что государство принимает активное участие в процессе информационного наполнения Казнета, свидетельствуют планы по поддержке создания 30 информационных

ресурсов в Интернет: 10 государственных и 20 частных. 26 сентября 2008 г. в Астане состоялась презентация девяти новых познавательных порталов в зоне .kz. Среди них: информационно-познавательный портал Министерства образования и науки РК (<http://www.it-bilim.kz>), портал АИС РК, предназначенный для повышения квалификации и тестирования отечественных специалистов в области информационных технологий (<http://www.it4u.kz>), электронный государственный библиотечный фонд "Библиотека Казахстана" (<http://www.kazneb.kz>), портал, популяризирующий историко-культурное наследие Казахстана (<http://www.madenimura.kz>), портал Министерства индустрии и торговли РК (<http://www.mit-portal.kz>), портал Министерства здравоохранения РК (<http://www.info-health.kz>), портал "Национальное наследие" (<http://www.ata-mura.kz>).

К ключевым проблемам правового регулирования общественных отношений, возникающих в связи с использованием сети Интернет, можно отнести три:

- проблему юрисдикции отношений в сети Интернет;
- проблему ответственности информационных провайдеров (посредников);
- проблему разработки и реализации инициатив в сфере саморегуляции отношений в сети Интернет.

Они являются теми критериями, которые определяют состояние решения любой проблемы в сфере правового регулирования информационного пространства и сервисов сети Интернет.

Любое государство и любой человек хочет быть хозяином в своем доме. Для государств это естественное желание обеспечивается принципами международного права, принципом государственного суверенитета, заключающимся в верховенстве, самостоятельности и независимости государственной власти, и принципом невмешательства во внутренние дела других государств. Для личности — международным и национальным законодательством, гарантирующим всем известные права человека и гражданина.

Последнее десятилетие глобальное информационное пространство, существующее, в первую очередь, в виде сети Интернет и возникшее в результате интернационализации общественных отношений и научно-технического прогресса, заставляет пересматривать границы дома и объем прав и обязанностей хозяина. Кроме того, часть пользователей, проповедуя "экстерриториальность" Сети, декларирует свою независимость от го-

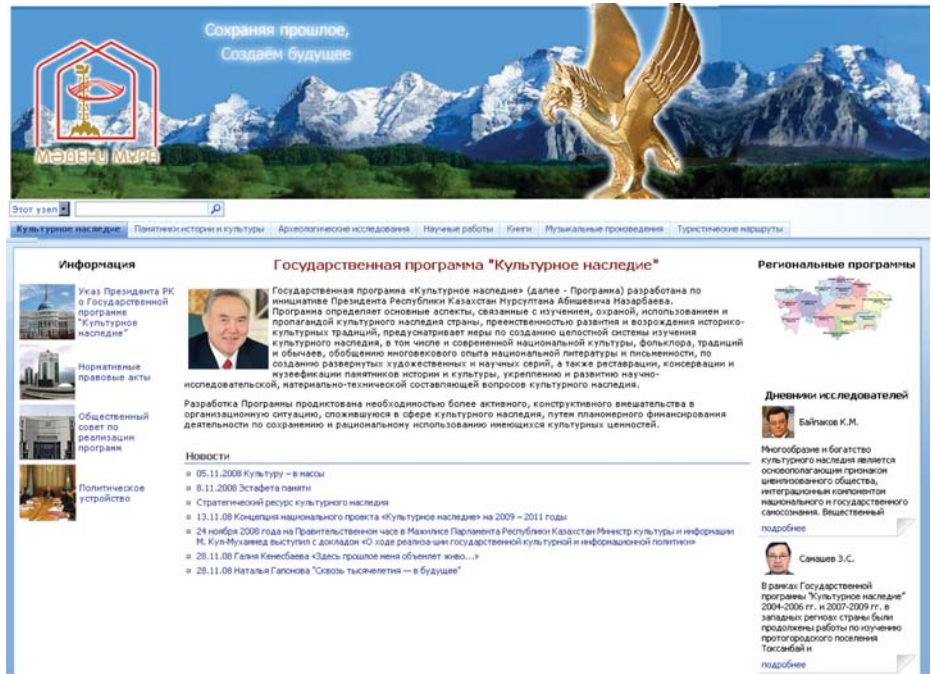


Рис. 4. Главная страница портала "Культурное наследие"

сударств и закона и борется за свою "суверенную Сеть".

Упрощенно цепочку информационных общественных отношений в терминах можно представить следующим образом: пользователь (потребитель) — информационный ресурс — собственник (владелец ресурса). При этом в существующей общественно-правовой ситуации каждый из элементов находится в сфере юрисдикции определенной страны мира. Понимая, что для каждого элемента цепочки отношения существует свой собственный правовой режим, имеем в общем случае три варианта правового регулирования: регулирование отношений по законодательству страны проживания пользователя, страны местонахождения ресурса и по законодательству страны собственника.

На самом деле приведенная схема весьма условна и не учитывает тот факт, что цепочка информационных общественных отношений, выстраивающаяся в процессе использования Сети, имеет не три, а минимум пять элементов (рис. 5), в число которых входят лица, оказывающие услуги по доступу, размещению и распространению информации в сети Интернет и называемые информационными провайдерами (посредниками).

Рассмотренная многомерность информационных общественных отношений вполне закономерно представляет собой источник растущего клубка общественно-правовых противоречий. Регулировать эти противоречия и конфликты в связи с эксплуатацией Сети пользователями, собственниками и хозяе-

вами серверов хостинга из разных стран мира пытаются уже сейчас.

Основными источниками права, регулирующего общественные отношения, являются международные договоры, национальное законодательство, судебная практика и обычаи, формирующиеся в процессе реализации тех или иных общественных отношений.

В настоящее же время несколько десятков стран имеют зачатки национального законодательства, касающегося использования глобального информационного пространства. Международные соглашения по этому вопросу отсутствуют, обычаи использования Сети весьма противоречивы — а значит, спорных ситуаций становится все больше, и постепенно формируется судебная практика по данным общественным отношениям. Нельзя сбрасывать со счетов и геополитические интересы различных стран. Одни из этих стран еще не осознали значения всемирного информационного пространства, другие стремятся распространить на него свое влияние, в частности, пытаются использовать свою



Рис. 5. Схема общественных отношений, возникающих в связи с использованием сети Интернет

систему права и свое законодательство для разрешения конфликтов в Сети.

В спорных ситуациях сталкиваются различные интересы и правовые системы, и возникает коллизия: какое право применять, в чем ведении находится тот или иной информационный процесс, юрисдикция какого государства распространяется на те или иные информационные общественные отношения?

В международном праве для ответа на эти вопросы существуют так называемые коллизионные нормы. Они не разрешают вопрос сами по себе, а лишь указывают на те нормы, которые должны быть использованы в данной конкретной ситуации (например, *lex loci contractus* — закон места совершения сделки, *lex loci actus* — закон места совершения акта, *lex patrie* — закон гражданства, *lex domini-cilii* — закон местожительства, *lex rei sitae* — закон местонахождения вещи и т. д.).

В настоящее время таковые нормы для Интернета отсутствуют, и международное информационное пространство пытаются "осваивать", используя подручные средства и национальные правовые концепции. Можно заметить, что аналогичные процессы имели место в первые десятилетия нашего века в сфере освоения воздушного пространства, но, несомненно, темпы освоения, масштабы и потенциальные возможности Сети на фоне общего потенциала развития планеты выглядят значительнее.

Судебная практика, трактующая и разрешающая проблему юрисдикции Сети, сейчас относится главным образом к наиболее доходным отраслям бизнеса в Сети — игорному и торговле информацией "для взрослых" — и формируется в тех странах, которые уже встали на путь правового регулирования Интернета.

Существует несколько возможных путей решения проблемы юрисдикции использования сети Интернет.

В первую очередь, это международные договоры, определяющие статус международного информационного пространства и фиксирующие соответствующие коллизионные нормы использования законодательства различных государств. Не панацеей, но временным выходом могут служить региональные многосторонние соглашения, а также двусторонние договоры о правовой помощи. Именно в них нужно вкраплять коллизионные нормы, помогающие стабилизировать международные информационные отношения. В идеале, необходима унификация норм национальных законодательств относительно использования Сети. Требуется соответствующее национальное информационное законодательство, чтобы не быть ни "открытыми

на фоне всеобщей закрытости", ни отгораживаться от всех железным занавесом. Конечно, предварительно необходимо на государственном уровне решить, какова в принципе идеология использования информационного пространства и в рамках данного решения принять соответствующие нормы.

Регулирование отношений, помимо проблемы юрисдикции, определяется специальным институтом ответственности информационных провайдеров: ISP, ASP, владельцы служб информационных объявлений (от досок объявлений до Интернет-аукционов), в европейском законодательстве в ходу термин "intermediary service providers", в американской практике — on-line service provider, provider of access, provider of the informational content.

В российских законопроектах употребляются термин "информационный посредник". Например, определяя его как "лицо, которое от имени другого лица отправляет, получает или хранит электронные документы или предоставляет другие услуги в отношении данных документов".

Действия информационных провайдеров по оказанию услуг обладают следующими свойствами. Провайдер не инициирует информационные отношения, не выбирает содержание передаваемой информации и ее получателя, не влияет на содержание информации и хранит таковую только в пределах времени, определяемого техническими стандартами и протоколами для нужд передачи информации.

Ответственность провайдеров базируется на том, что они имеют организационно-техническую возможность в любой момент времени воздействовать на информационные общественные отношения своих пользователей. Форма воздействия может быть довольно разнообразной: от блокирования информационного обмена до информирования третьих лиц о содержании передаваемой информации.

В каком случае провайдер — владелец информационного ресурса и/или информационной системы — несет ответственность за действия лиц, которые воспользовались указанными ресурсами и/или системами?

На этот счет существуют три основных подхода:

- провайдер несет ответственность за все действия пользователей, вне зависимости от наличия у него, как у субъекта права, знания о совершаемых действиях;
- провайдер не несет ответственности за действия пользователей в том случае, если выполняет определенные условия, связанные с характером предоставления услуг и взаимодействием с субъектами информационно-

го обмена и лицами, чьи права нарушаются действиями пользователей;

- провайдер не отвечает за действия пользователей.

Законодательства разных стран предлагают решение проблемы ответственности провайдеров сообразно трем приведенным схемам. Если, например, в Китае и странах Ближнего Востока принят первый подход, в США — третий (в подавляющем большинстве случаев провайдеры обладают иммунитетом и не несут ответственности за действия своих пользователей), то в Европе придерживаются второго подхода: наиболее детально решение проблемы ответственности проработано в европейской директиве по электронной коммерции.

Директива устанавливает, что провайдер не несет ответственности за передаваемую информацию в случае, если он не инициирует ее передачу, не выбирает получателя информации и не влияет на целостность передаваемой информации. При этом допускается временное хранение передаваемой информации для осуществления необходимых технических действий по ее передаче. Также детализируются условия кэширования, и утверждается, в частности, что провайдер не несет ответственности за действия пользователей при предоставлении услуг хостинга, если он не был осведомлен об их противозаконной деятельности и после получения информации прекратил размещение или доступ к информации пользователей.

Резюмируя вышесказанное, можно утверждать, что проблема ответственности провайдеров — это актуальный вопрос государственной политики по использованию сети Интернет. В зависимости от того, как будет определена и регламентирована роль провайдеров в информационных общественных отношениях в сети Интернет, возможны разные пути развития сети Интернет.

Действующие нормативные акты по вопросам регулирования Интернет возможно классифицировать на группы по предмету правового регулирования:

1. Определяющие правовой статус информационных ресурсов сети Интернет и порядок доступа к ним;
2. Регулирующие деятельность операторов сетей передачи данных и доступа в Интернет, а также поставщиков услуг IP-провайдеров и других лиц, использующих информационные ресурсы или сети передачи данных для предоставления услуг доступа;
3. Регулирующие тарифы на услуги доступа к сети Интернет.

К первой группе возможно отнести:

1) Закон Республики Казахстан "Об информатизации". Закон предусматривает понятия информатизации и информационных услуг, веб-сайта, доменного имени, электронных информационных ресурсов и их владельцев.

Предметом Закона является регулирование правового статуса владельцев информационных ресурсов и информационных систем, которые в зависимости от права собственности и категории доступа подразделяются на:

- государственные и негосударственные;
- общедоступные и ограниченного доступа.

При этом, Закон об информатизации определяет информационные ресурсы как элемент состава имущества, которые находятся в частной и государственной собственности. Приведенная законодателем правовая конструкция вызывает вопросы, поскольку информационные ресурсы, содержащиеся в сети, могут быть без особых проблем отделены от своих материальных носителей, в связи с чем, правовой статус такого вида объектов целесообразно определить через правовой механизм исключительных прав (право интеллектуальной собственности), предусмотренный Разделом 5 ГКРК.

Для системного внедрения информатизации в деятельности государственных органов Законом введено понятие национального оператора в сфере информатизации — юридического лица, созданного по решению Правительства Республики Казахстан, на которое собственником в лице государства возложены задачи по интеграции и обеспечению безопасности государственных информационных систем и государственных электронных информационных ресурсов, по участию в реализации единой технической политики в сфере информатизации, функции проектного интегратора инфраструктуры "электронного правительства". В соответствии с постановлением Правительства Республики Казахстан от 16 января 2004 г. № 44, Национальным оператором в сфере информатизации определено акционерное общество "Национальные информационные технологии".

Другой важной составляющей Закона являются требования по регистрации электронных информационных ресурсов, информационных систем и их аудиту. Порядок регистрации информационных ресурсов и систем определен постановлением Правительства Республики Казахстан от 19 октября 2004 г. № 1075, в соответствии с которым обеспечение ведения Государственного регистра, а также организация технических условий для доступа физических и юридических лиц к общедоступным государственным информационным ресурсам с целью удовлетворения их информационных потребностей, осуществляется Национальным оператором в сфере информатизации.

Аудит информационных систем заключается в

системном процессе оценки текущего состояния информационных систем, действий и событий, происходящих в ней устанавливающий уровень их соответствия определенным критериям, техническим регламентам, стандартам и нормативно-технической документации. Аудит информационных систем производится за счет владельцев информационных ресурсов. Проведение аудита осуществляется лицами, обладающими специальными знаниями и опытом работы в сфере информационных технологий в порядке, определяемом уполномоченным органом (Агентство Республики Казахстан по информатизации и связи).

2) "Закон Республики Казахстан "Об электронном документе и электронной цифровой подписи".

Законом даны понятия электронного документа и документооборота, ключей цифровой подписи и также установлена равнозначность, при соблюдении установленных условий, электронных документов/подписей документам/подписям на бумажном носителе.

3) Закон Республики Казахстан "О национальной безопасности", в части обеспечения информационной безопасности Республики Казахстан.

4) Закон Республики Казахстан "О средствах массовой информации", в части регулирования деятельности электронных средств массовой информации.

5) Закон Республики Казахстан "О государственных секретах", в части доступа к государственным информационным ресурсам.

6) Указ Президента Республики Казахстан от 10 ноября 2004 г. № 1471 "О государственной программе формирования "электронного правительства" в Республике Казахстан на 2005-2007 гг.

7) Постановление Правительства Республики Казахстан от 13 октября 2006 г. "Об утверждении Программы снижения информационного неравенства в Республике Казахстан на 2007-2009 гг."

8) Постановление Правительства Республики Казахстан от 5 июня 2007 г. № 460 "Об утверждении перечня персональных данных физических лиц, включаемых в состав государственных электронных информационных ресурсов".

9) Постановление Правительства Республики Казахстан от 30 июня 2007 г. № 553 "Об утверждении положения и состава Межведомственной комиссии Республики Казахстан по координации работ в сфере информатизации".

10) Постановление Правительства Республики Казахстан от 13 июля 2007 года № 598 "Об утверждении Правил размещения электронных информационных ресурсов на веб-сайтах государственных органов".

Ко второй группе нормативных правовых актов можно отнести:

1) Закон Республики Казахстан "О связи", в части регулирования деятельности операторов связи.

2) Постановление Правительства Республики Казахстан от 29 сентября 2004 г. "О некоторых вопросах лицензирования деятельности в области связи", в части определения лицензирования операторских услуг по передаче данных и доступу к сети Интернет.

3) Постановление Правительства Республики Казахстан от 22 июля 2003 г. № 724 "Вопросы Агентства Республики Казахстан по информатизации и связи", в части определения компетенции уполномоченного органа в области связи по контролю за деятельностью операторов связи, предоставляющих доступ к услугам передачи данных и Интернет.

4) Приказ Председателя Агентства Республики Казахстан по информатизации и связи от 12 июля 2004 г. № 145-п "Об утверждении Правил присоединения сетей телекоммуникаций к сети телекоммуникаций общего пользования и регулирования пропуска телефонного трафика по сети телекоммуникаций общего пользования Республики Казахстан", в части регулирования вопросов технического взаимодействия сетей операторов связи.

Нормативные правовые акты, регулирующие тарифы на услуги доступа к сети Интернет.

1) Закон Республики Казахстан "О конкуренции и ограничении монополистической деятельности", в части регулирования деятельности операторов связи, занимающих доминирующее положение на рынке доступа в Интернет.

2) Закон Республики Казахстан "О связи", в части определения универсальных услуг телекоммуникаций.

Из анализа приведенных выше нормативных правовых актов усматривается отсутствие норм, регулирующих предоставление услуги по доступу в Интернет конечному потребителю (пользователю). В тоже время условия предоставления иных услуг связи — местной, междугородной и международной, телеграфной, сотовой — урегулированы соответствующими Правилами, принятыми уполномоченным государственным органом в области связи.

Полагаем, что отсутствие такого акта в сфере доступа к сети Интернет создает вакуум и не позволяет определить параметры качества услуги ее вид, условия ее предоставления в интересах конкретного конечного потребителя.

Необходимо принятие Правил предоставления доступа к сети Интернет, содержащих определение услуги по доступу, права и обязанности сторон, определяющие виды услуг и соответствующих технологий доступа.

*Продолжение статьи
читайте в следующем номере журнала*