FREE attendance for all Regional Service Providers

New for 2010:
Türkiye Özel
TURKEY FOCUS day
24 MARCH 2010

The 6th Annual
EurasiaCom

23-24 March 2010
Conrad Hotel,
Istanbul, Turkey

Innovative Technologies and Services to Maximise Profitability in a Converging Market




The only regional telecoms event featuring 25+ Operator CxO speakers including these luminaries and government ministers:


Oleg Raspopov, Vice President, MTS, Russia


Mustafa Kiral, Vice President, Altimo, Russia


Sava? ? nsal, Board Member, SuperOnline A.?, Turkey


Ineke Botter, CEO, Bakcell, Azerbaijan


Maksut Sauranbekov, President, Altel, Kazakhstan


John Samarron, CTO, Vodafone Turkey


Anatoly Ten, Chief Technical Officer, KyrgyzTelecom, Kyrgyzstan


Mehmet Baser, Managing Director, Borusan Telekom, Turkey


Faz?l Esen, Managing Director, Doğan Telekom, Turkey

Boimurod Mirzoyarov, Vice-Chairman of the Board of Directors, Tajiktelecom, Tajikistan

Ministerial Delegations:


Kuanysbek Bahytbekovich Yesekeev, Chairman, Agency of Information Technologies and Telecommunication, Kazakhstan


Rovshan Gamidovich Mamedov, Minister of Information, Nachivan Autonomous Republic, Azerbaijan

Taalaibek Eshaliev, Deputy Minister, Ministry of Transport and Communications, Kyrgyzstan

NEW for 2010 Simultaneous translation in Russian, English and Turkish.

Focusing on the Evolving Dynamics of this Thriving Region, the Agenda Delivers Practical, Constructive Measures to Drive Innovation & Profits

- Determine how to position your company in Eurasia's changing telecoms ecosystem
- Encourage innovation in technologies and services to move your business forward
- Improve efficiencies to maximise profitability and deliver better services to your consumers
- Develop reliable and attractive broadband services for all end-users
- Deliver outstanding service to gain and retain customers and to improve revenues

Network with senior decision-makers from the service-providers of the Central Asia, Caspian & Black Sea markets:

- ☑ Turkey
- ☑ Afghanistan
- ☑ Albania
- ☑ Armenia
- ☑ Azerbaijan
- ☑ Belarus
- ☑ Bosnia-Herzevogina
- ☑ Bulgaria
- ☑ Cyprus
- ☑ Georgia
- ☑ Greece
- ☑ Iran
- ☑ Kazahkstan
- ☑ Kyrgyzstan
- ☑ Macedonia
- ☑ Montenegro
- ☑ Pakistan
- ☑ Romania
- ☑ Serbia
- ☑ Syria
- ☑ Tajikistan
- ☑ Turkmenistan
- ☑ Uzbekistan

Sponsored by: SmartTrust

Produced by: informa telecoms & media

Part of the: Com World Series

Take advantage of the early booking discounts and register online today Quoting VIP Code: EU10TCOM:

www.comworldseries.com/eurasia

T•Comm
Телекоммуникации и транспорт
№6-2009
"T-Comm — Telecommunications and Transport" magazine

Журнал включен в перечень периодических научных изданий, рекомендуемый ВАК Минобразования 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 Паблишер"

Главный редактор
В.О. Тихвинский

Издатель
С.С. Дымкова
ds@media-publisher.ru

www.media-publisher.ru

СОДЕРЖАНИЕ

НОВОСТИ

В рубрике представлена информация компаний:
МТС, Alcatel-Lucent, РЖД, МТТ, M2M, РНТ, Техносерв, McAfee, "Казахтелеком", ТК355, Интерэкомс,СкайЛинк
4

ТРАНСПОРТ

Козлов Л.Н., Циклис Б.Е., Урличич Ю.М.
О Концептуальных подходах формирования и развития ИТС в России
8

БЕЗОПАСНОСТЬ

Дешевый и безопасный контент-хостинг — оптимальное решение для небольших операторов
(*по материалам компании Сопах*)
16

Полещук А.В.
Построение эффективной системы защиты персональных данных
18

Алексей Чередниченко.
Системы защиты персональных данных
22

Станислав Гучия.
Системы охранного видеонаблюдения на базе IP для обеспечения безопасности здания
25

ОБОРУДОВАНИЕ

Устройства для решения задач современного общества
(*по материалам компании NXP*)
28

ТЕХНОЛОГИИ

Зелевич Е.П., Костарев А.Н.
Анализ параметров сигналов, воспроизводимых с карт с магнитной полосой
30

Зелевич Е.П., Черников К.В.
Анализ влияния свойств объектов на функционирование систем радиочастотной идентификации
33

Русаков Д.А.
Анализ перспектив применения технологии RFID для задач управления поставками и складскими ресурсами
36

Скрынников В.Г.
Две задачи по сетям UMTS-900
42

Кондрашов А.С.
Целевая функция структурно-параметрического синтеза конструктивной системы модулей радиоэлектронных средств
47

Шинаков Ю.С., Ахмат М.С.
Исследование эффективности управления мощностью подвижной станции системы стандарта IS-2000 в многолучевом канале
49

РЕПОРТАЖ

Форум "Интерком-2009: Инфокоммуникации будущего"
56

УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Продолжается подписка на журнал
"T-Comm — Телекоммуникации и Транспорт" на 2010 год

Подписной индекс журнала в агентстве "Роспечать" — 80714
Подписка через редакцию — ds@media-publisher.ru
Стоимость годовой подписки — 1200 руб.

Издание включено в реферативный журнал и базу данных ВИНИТИ РАН. Сведения о нем ежегодно публикуются в справочной системе по периодическим и продолжающимся изданиям Ulrich's Periodicals Directory.
Полнотекстовые версии журнала T-Comm размещены в eLIBRARY.RU (издание включено в систему Российского индекса научного цитирования (РИНЦ)

Требования к предоставляемым материалам

- Текст статьи в формате Word (не более 20 000 знаков).
- Иллюстрации в формате Tif или Jpeg (300 dpi, CMYK).
- Аннотация на русском и английском языках, ключевые слова.
- Пристатейный список литературы.
- Сведения об авторе (Ф.И.О. полностью, e-mail, должность, место работы).

Интернет-портал издательского дома Медиа Паблишер
www.media-publisher.ru

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 200 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; • Автотранспортные 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
111024, Россия, Москва,
ул. Авиамоторная, д. 8, корп. 1, офис 329
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

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

www.media-publisher.ru

Заседание президиума Госсовета РФ в Ульяновске

24 ноября 2009 г. в Ульяновске президент ОАО "РЖД" Владимир Якунин принял участие в заседании президиума Государственного Совета РФ по вопросам инновационного развития транспортного комплекса под председательством Президента РФ Дмитрия Медведева.

Делегация президиума Госсовета посетила выставку инновационных технологий в сфере развития транспорта, одна из экспозиций которой была посвящена новейшим разработкам в области железнодорожного транспорта. В частности, на стендах были представлены модели скоростного поезда "Сапсан", газотурбовоза, работа системы ГЛОНАСС (Глобальная Навигационная Спутниковая Система).

"Переход к "интеллектуальному" железнодорожному транспорту предусматривает развитие компьютерных систем, спутниковых технологий управления и сквозных логистических технологий перевозки грузов. Так, более 11 тысяч единиц подвижного состава холдинга "РЖД" уже используют спутниковые технологии на основе систем ГЛОНАСС/GPS. Сейчас ведутся работы по созданию полностью автоматизированной системы управления движением поездов на полигоне Москва — Санкт-Петербург", — рассказал Владимир Якунин.

По словам президента ОАО "РЖД", для дальнейшего инновационного развития транспортного комплекса, в частности, необходима общегосударственная "Программа развития отечественного машиностроения" в статусе национального проекта, доработка проекта федерального закона "Об энергосбережении и повышении энергетической эффективности", а также разработка программы по развитию отечественного дизелестроения.

Хабаровск — "Электронный город будущего". Теперь и с ГЛОНАСС

Инновационный проект на базе ГЛОНАСС/GPS был представлен администрацией города Хабаровска на выставке "Электронный город будущего", прошедшей 30 ноября 2009 г. в Москве в рамках форума "Мегаполис: XXI век". Организаторами мероприятия выступили Международная Ассамблея столиц и крупных городов (МАГ), Исполком СНГ, ЕврАзЭс, Правительство Москвы и Минрегионразвития РФ.

На экспозиции администрации Хабаровска можно было ознакомиться с проектом по созданию "Навигационно-информационной системы" города. На данный момент утверждена концепция проекта и необходимые нормативные документы. Сделаны первые шаги. Реализация проекта будет осуществляться на базе специально созданного муниципального автономного учреждения "Хабаровский межотраслевой навигационно-информационный центр".

Мэр Хабаровска Александр Соколов продемонстрировал участникам выставки, каким образом с помощью технологий ГЛОНАСС в режиме реального времени можно контролировать работу общественного транспорта и различных служб города на расстоянии нескольких тысяч километров.

Навигационно-информационная система транспортного комплекса является элементом Интеллектуальной Транспортной Системы (ИТС) и позволяет обеспечивать централизованный контроль и управление транспортом предприятий Хабаровска, повышать экономическую эффективность использования транспорта, а также безопасность пассажирских и грузовых перевозок. Система обеспечивает не только постоянный мониторинг перемещения и скорости движения транспортных средств, но и контролирует несанкционированное использование транспорта, включая сливы топлива и "левые" рейсы.

Проект по внедрению навигационно-информационной системы города Хабаровска состоит из нескольких этапов. В рамках первого этапа на общественном транспорте МУП "ХПАТП №1" были установлены абонентские ГЛОНАСС/GPS терминалы M2M-Cyber GLX, в автопарк предприятия внедрена система управления перевозочным процессом M2M-CityBus. Идет также и оснащение ряда предприятий, занимающихся благоустройством города.

В рамках дальнейшего развития "Хабаровского межотраслевого навигационно-информационного центра" планируется создание единой навигационно-информационной системы, охватывающей все сферы жизнедеятельности города (пассажирский транспорт, городское хозяйство, здравоохранение и пр.). Предполагается внедрение дополнительных информационных сервисов для местного населения.

Навигационно-информационные системы транспорта на основе технологий ГЛОНАСС/GPS активно внедряются во многих городах РФ.

В целях модернизации транспортного комплекса к предстоящей Олимпиаде 2014 г. в Сочи была внедрена автоматизированная система мониторинга и диспетчеризации (АСМД). По результатам внедрения системы экономия автопредприятий города на топливе достигла 20%, а рабочий день служб ЖКХ за счет более эффективного управления спецтехникой планируется сократить с 12 до 8 часов.

Проект "Хабаровского межотраслевого навигационно-информационного центра" вызвал большой интерес среди участников выставки, в первую очередь, у глав администраций городов России.

"Казахтелеком" готовится к внедрению высокоскоростных IP-услуг

Компания "Казахтелеком" совместно с Cisco и АМТ-ГРУП объявила о запуске в эксплуатацию IP-сети нового поколения на основе оптических сетевых решений Cisco. Разработку и внедрение проекта осуществили специалисты компании АМТ-ГРУП.

Данное решение позволяет "Казахтелекому" оказывать новые ресурсоемкие услуги предприятиям и домашним пользователям в г. Алматы. В число этих услуг входит скоростной интернет-доступ с интегрированной передачей голоса, видео и данных, создание виртуальных частных сетей (VPN) для корпоративных пользователей, проведение виртуальных конференций с применением технологии Cisco TelePresence, а также IPTV. Заложенный в систему уровень отказоустойчивости позволит "Казахтелекому" сохранять работоспособность сети даже в случае множественных отказов каналов связи и обеспечивать полное восстановление штатной емкости сети при выходе из строя любого магистрального канала.

Проект стал первой в СНГ и одной из первых в мире инсталляцией технологии Cisco IPoDWDM с использованием функциональности виртуальных транспондеров и одним из первых в мире совместных использований технологий IPoDWDM и Omni-directional DWDM. В решении уже сейчас использованы элементы архитектуры оптических сетей следующего поколения ASON/GMPLS.

На момент начала проекта компания "Казахтелеком" располагала в г. Алматы сетью Metro Ethernet. Расширение абонентской базы, стремительный рост объемов чувствительного к качеству обслуживания трафика, планы по внедрению новых ресурсоемких услуг потребовали модернизации сети, и возникла необходимость увеличения ее производительности, надежности, гибкости и управляемости.

Специалисты АМТ-ГРУП построили для "Казахтелекома" в Алматы высокоэффективную конвергентную сеть, использующую технологии спектрального уплотнения DWDM и пакетной коммутации IP/MPLS. В решении применены решения Cisco ONS 15454 MSTP и CRS-1. Оптическая магистраль имеет 40 каналов и может быть расширена до 80-канальной конфигурации без замены платформы. На момент запуска пропускная способность конвергентной транспортной сети составила 200 Гбит/с и может быть увеличена до 800 Гбит/с без замены оборудования.

Интеграция технологии DWDM в платформу IP/MPLS позволила уменьшить количество комплектующих и добиться уменьшения энергопотребления. В алматинской сети "Казахтелекома" использована функциональность "виртуальных транспондеров", которая обеспечивает единое управление оптическими ресурсами и протокольное взаимодействие между DWDM- и IP/MPLS- составляющими транспортной сети.

Это позволяет не только сократить операционные затраты, но и добиться повышения надежности инфраструктуры, сохранив при этом разграничение полномочий в управлении оптической и пакетной сетями.

Итоги заседания подкомитета ПК4 "Радиочастотная идентификация" Технического комитета по стандартизации ТК355 "Автоматическая идентификация" от 5 ноября 2009 г.

М.Н. Бескодаров, и.о. ответственного секретаря Национального технического комитета по стандартизации ТК355 "Автоматическая идентификация", выступил на заседании подкомитета ПК4 "Радиочастотная идентификация" с информацией о просьбе председателя ПК4 Смольского С.М. об освобождении от занимаемой должности по состоянию здоровья. По предложению Бескодарова М.Н. на должность председателя ПК4 была выдвинута кандидатура Зелевича Е.П. — начальника отдела ИРИС НИЧ, профессора кафедры "Инфокоммуникаций" ИПК ГОУ ВПО МТУСИ. После обсуждения кандидатуры Зелевича Е.П. состоялось открытое голосование членов ПК4, по итогам которого было принято единогласное решение утвердить Зелевича Е.П. председателем ТК355/ПК4.

М.Н. Бескодаров выступил также с информацией о работах по международной стандартизации в области радиочастотной идентификации, проводимых ИСО/МЭК СТК1/ПК31 "Технологии автоматической идентификации и сбора данных".

В докладе были затронуты вопросы, связанные с общими особенностями разработки международных стандартов и участии Национального технического комитета ТК355 "Автоматическая идентификация", представляющего Российскую Федерацию в Международной организации по стандартизации ИСО, в процессе разработки международных стандартов ИСО/МЭК в области автоматической идентификации. Подкомитет ПК4 "Радиочастотная идентификация, участвует в работах по международной стандартизации, проводимых в рамках ИСО/МЭК СТК1/ПК31 "Технологии автоматической идентификации и сбора данных" в области радиочастотной идентификации (ISO/IEC JTC1/SC31 "Automatic identification and data capture techniques"). М.Н. Бескодаров отметил, что появились новые направления работ, связанные со стандартизацией сенсорных и мобильных технологий, интегрируемых в системы автоматической идентификации и сбора данных (в данном случае — системы радиочастотной идентификации), а также направление, связанное со стандартизацией в области безопасности систем автоматической идентификации и сбора данных в части радиоинтерфейса и других компонентов беспроводных систем связи. По каждому из новых направлений началась разработка ряда проектов международных стандартов. Особое внимание было уделено динамике и ходу разработки стандартов в рамках подгрупп рабочей группы РГ4 "Радиочастотная идентификация для управления предметами" (WG4 "Radio frequency identification for item management") и РГ5 "Системы определения места нахождения в реальном времени" (WG5 "Real time locating systems (RTLS)").

Выступление Ответственного секретаря ТК355/ПК4 А.А. Гридасовой было посвящено вопросам национальной стандартизации в области радиочастотной идентификации. На настоящий момент в рамках ТК355 подготовлено и утверждено 9 национальных стандартов (ГОСТ Р) в области радиочастотной идентификации, включая стандарты по синтаксису и структурам данных, а в разработке находятся два проекта стандарта: терминологический стандарт по радиочастотной идентификации и стандарт на требования к радиоинтерфейсу для диапазона частот 860-960 МГц. В своей работе ПК4 "Радиочастотная идентификация" руководствуется принципами приоритетности разработки национальных стандартов, гармонизированных по отношению к международным стандартам ИСО/МЭК, разработанных в рамках СТК1/ПК31 "Технологии автоматической идентификации и сбора данных" в области радиочастотной идентификации (ISO/IEC JTC1/SC31 "Automatic identification and data capture techniques"), что было отражено в программе работ по национальной стандартизации в области радиочастотной идентификации на 2009-2010 гг. Также был рассмотрен вопрос формирования среднесрочной программы по национальной стандартизации в области информационных технологий Комитета РСПП по техническому регулированию, стандартизации и оценке соответствия. В части радиочастотной идентификации в среднесрочную программу стандартизации вошли предложения по гармонизации международных стандартов, касающихся требований к радиоинтерфейсу для диапазонов частот 860-960 МГц; 13,56 МГц; 2,45 ГГц, правилам кодирования данных, а также ряд стандартов на методы испытаний радиоинтерфейса и устройств систем радиочастотной идентификации для различных диапазонов частот.

Сообщение о стандартах EPCglobal было представлено Ольгой Соболевой, заместителем начальника отдела развития и информационных систем ГС1 РУС.

Сообщение содержало предварительную информацию об электронном коде продукции (EPC) и концепции глобальной системы EPCglobal. Были определены составляющие элементы системы стандартов EPCglobal, и их роль в построении глобальной системы. В настоящее время в EPCglobal разработаны и ратифицированы 12 стандартов, обеспечивающих реализацию функций: идентификации объектов в цепи поставки, сбора данных, обмена данными.

Кратко охарактеризованы все ратифицированные стандарты и стандарты, разработка которых ведется в настоящее время. Также была представлена информация о структуре и составе организации EPCglobal, о процессах разработки стандартов и их участниках.

Подробная информация о компании EPCglobal и стандартах, которые она разрабатывает, представлена на сайте **www.epcglobalinc.org.**

Популярная информация о возможностях технологии EPC/RFID представлена на **www.discoverfid.org.**

В рамках заседания члены ПК4 выступили с сообщениями о проектах в области радиочастотной идентификации.

МТТ усиливает международные направления связи

ОАО "Межрегиональный ТранзитТелеком" (МТТ) объявляет о заключении прямых договоров с 17-ю операторами связи. Новые соглашения о предоставлении международных услуг связи позволят МТТ значительно усилить свои позиции на рынках многих стран, как в ближнем, так и дальнем зарубежье, и обеспечат клиентам МТТ надежные каналы связи.

Контракты заключены с операторами по наиболее востребованным российскими пользователями направлениям: Средняя Азия (Казахстан, Кыргызстан), Восточная и Центральная Европа (Чехия, Греция, Литва, Нидерланды), а также Азия (Гонконг, Израиль, Иран) и Америка (США и Канада). В частности, прямые взаимоотношения установлены с крупными операторами Sprint Communications (США) и Phonetime (Канада), а также с испанским оператором System One World Communications и израильским Smile 012. Новые соглашения предусматривают как международный транзит трафика, так и приземление трафика на сети российских партнеров. В рамках новых договоров МТТ использует собственные точки присутствия во Франкфурте и в Гонконге.

"Постоянное расширение списка международных партнеров МТТ дает возможность предоставить нашим абонентам, как корпоративным, так и частным, более качественные услуги по привлекательным ценам на самых популярных международных направлениях. Благодаря новым партнерам мы готовы предоставить максимально широкие возможности для транзита и приземления трафика, минимизируя издержки для наших клиентов", — заявил Николай Чураев, заместитель генерального директора по коммерческой деятельности ОАО "МТТ".

В настоящее время МТТ сотрудничает в сегменте пропуска трафика с большинством национальных операторов связи Европы (Deutsche Telekom, British Telecom, Telekom Austria, France Telecom и др.), СНГ, Азии и Америки, а также со многими альтернативными операторами связи по всему миру.

"Скай Линк" планирует построить сеть GSM на оборудовании Alcatel-Lucent и Huawei и готов организовать опытную зону LTE в 2010 г.

Оператор мобильной связи "Скай Линк" по результатам тендера на строительство сетей GSM в 45 субъектах РФ будет использовать оборудование Alcatel-Lucent и Huawei: оборудование Alcatel-Lucent будет использоваться в Центральном и Южном федеральных округах РФ; оборудование Huawei будет — в Северо-Западном, Сибирском и Приволжском федеральных округах РФ.

В соответствии с условиями тендера, Alcatel-Lucent осуществит поставку, монтаж и интеграцию оборудования на базе технологии GSM в диапазоне 1800 МГц в Белгородской, Брянской, Владимирской, Ивановской, Калужской, Костромской, Курской, Липецкой, Орловской, Рязанской, Смоленской, Тверской, Тульской, Ярославской областях, Карачаево-Черкесской республике, Краснодарском крае, в Республиках: Адыгея, Дагестан, Ингушетия, Кабардино-Балкария, Северная Осетия - Алания и Чеченская Республика.

На оборудовании Huawei будет построена сеть на территории следующих регионов: Кировской области, Агинского Бурятского АО, Алтайского края, Иркутской области, Красноярского края, Новосибирской области, Республики Алтай, Республики Бурятия, Республики Тыва, Республики Хакасия, Таймырского АО, Томской области, Усть-Ордынского Бурятского АО, Читинской области, Эвенкского АО, Архангельской области, Вологодской области и Череповецкого района, Мурманской области, Новгородской области, Псковской области, Республики Карелия, Республики Коми, Ненецкого автономного округа.

В настоящее время лицензионная территория "Скай Линк" (CDMA+GSM) включает 78 субъектов РФ. Услуги "Скай Линк" в сети CDMA доступны в настоящее время на территории более 6000 населенных пунктов в 36 субъектах РФ, где обслуживается более миллиона абонентов в сетях 3G, лицензионная территория CDMA включает 73 субъекта РФ. Лицензионная территория GSM включает 45 субъектов РФ, в настоящее время сформирована стратегия и бизнес-модель развития сети CDMA+GSM, а также проведена подготовительная работа в регионах.

Система "АвтоТрекер": итоги автоэкспедиции "Великий путь российской цивилизации"

Компания "Русские Навигационные Технологии" подводит итоги своего участия в автоэкспедиции "Великий путь российской цивилизации", завершившейся 16 ноября во Владивостоке.

В ходе автоэкспедиции, для маршрута Санкт-Петербург — Владивосток впервые была получена объективная количественная информация о работе систем глобального позиционирования ГЛОНАСС и GPS, качестве покрытия сетей GSM, а также о скоростном режиме транспортного потока.

Экспедиция, стартовавшая 14 октября в Санкт-Петербурге, была организована политической партией "Единая Россия" и проходила на автомобилях, предоставленных российской автомобильной компанией Sollers (внедорожники UAZ Patriot и UAZ Pickup, коммерческий фургон российского производства Fiat Ducato). Компания "Русские Навигационные Технологии" — официальный партнер автоэкспедиции — установила на все автомобили свою систему ГЛОНАСС/GPS мониторинга и контроля "АвтоТрекер". Это позволило постоянно контролировать местонахождение каждого автомобиля, отслеживать соблюдение графика движения и скоростной режим. В дни пробега компания организовала и поддерживала специальный Интернет-ресурс, позволявший всем желающим в режиме on-line следить за перемещением автоколонны и получать информацию о мероприятиях.

Наряду с повышением безопасности участников экспедиции, важнейшей целью компании "Русские Навигационные Технологии" было объективное сопоставление реального состояния систем глобального позиционирования GPS и ГЛОНАСС как основы решения задач мониторинга автотранспорта для коммерческих и государственных заказчиков на значительной части территории страны. Компания хотела продемонстрировать, что результаты мониторинга могут служить объективной основой для количественной оценки важнейших параметров транспортной инфраструктуры, в первую очередь, средней скорости транспортного потока, а также оперативного выявления "узких мест", снижающих пропускную способность транспортной системы регионов. Такая информация имеет важнейшее значение при планировании средней продолжительности грузоперевозок, а на государственном уровне — для оптимального распределения ресурсов на развитие сети дорог.

Содержательная интерпретация результатов анализа данных опиралась на реальные события бортового журнала, который вел участвовавший в экспедиции Эдуард Андрианов, директор по региональному развитию компании "Русские Навигационные Технологии".

По данным системы "АвтоТрекер", общий пробег составил 11 484 км. Это расстояние автоколонна преодолела за 239 ч (чистое время движения), еще 601 час составили остановки в населенных пунктах, где проводилось множество мероприятий. Средняя скорость всего автопробега равна 66 км/ч, при этом водители, как правило, двигались со скоростью транспортного потока. Таким образом, эту оценку можно считать достаточно надежной для данного времени года и типа автомобилей. Анализ данных выявил наиболее скоростные и медленные участки, позволил оценить разброс средних скоростей по участкам, причем эти оценки не всегда совпадают с бытующими представлениями.

Система GPS показала лучшие результаты, чем ГЛОНАСС. Так, спутники GPS всегда были на связи, а их положение позволяло определять координаты точно и своевременно. Сопоставление данных мониторинга с бортовыми журналами выявило, что отмеченное в Нижнем Новгороде длительное отсутствие навигации GPS сразу на всех автомобилях (суммарно, 32 ч) было связано с их нахождением в гараже или специальном паркинге.

В системе ГЛОНАСС потеря спутников имела место и на трассе. Ранжированный список перерывов выглядит так: поселок Могоча Забайкальского края (3 ч 50 мин 18 с); Иркутск (3 ч 48 мин 56 с); Благовещенск (около трех часов в сумме); Чита (2 ч 10 мин 50 с в сумме); затем Омск и Красноярск (потеря спутников ГЛОНАСС на время около часа); Кострома, Нижний Новгород, Казань, Пермь и Тобольск - непродолжительная потеря спутников длительностью от 10 до 30 минут. Сопоставление этих данных с картографической информацией и бортовым журналом показывает, что наиболее вероятными причинами могли быть как "плохая видимость" спутников из-за погодных условий, рельефа местности и остановок в местах затрудненного приема спутниковых сигналов, так и нюансы работы использованных навигационных приемников.

По всему маршруту для каждого автомобиля произошло всего до 10 событий полной потери GSM-сигнала; на всей территории восточнее Урала отмечены перебои с GSM-сетью различной длительности, не превышающие одного часа. Плохое покрытие отмечено на перегоне Тобольск-Омск (особенно, между Тобольском и Ишимом). Хотя сотовые операторы "большой тройки" показали неодинаковые результаты, разрыв не был принципиальным. В системе "АвтоТрекер" временная потеря связи с диспетчерским центром не является проблемой: интеллектуальный бортовой блок в полном объеме проводит обработку первичных данных, полученных от датчиков системы, а результаты автоматически попадают на сервер системы при восстановлении связи. В момент потери GPRS-связи система сигнализирует об этом, и как только связь восстанавливается, — детально воспроизводит все события, происходившие с объектом мониторинга.

Из полученных данных можно сделать несколько практически важных выводов. Во-первых, на маршруте следования не было участков, где использование системы мониторинга невозможно в принципе. При этом в большинстве случаев вполне работоспособны обе системы глобального позиционирования. Во-вторых, предприятию, транспорт которого работает на ограниченной территории, при выборе сотового оператора необходимо исходить из местных условий, а не ориентироваться на осредненные данные о покрытии. Компаниям, занятым грузоперевозками на большие расстояния, лучше работать сразу с несколькими операторами сотовой связи, причем система "АвтоТрекер" позволяет переключаться между сетями автоматически. Не стоит также полагаться на то, что покрытие GSM предполагает работу сервиса GPRS. Система мониторинга транспорта действительно позволяет получить объективную информацию о характеристиках всего транспортного потока. Такие оценки практически не связаны с существенными затратами, т.к. являются побочным результатом нормальной работы системы мониторинга.

Конгресс организаций связи и информационных технологий "Современные направления устойчивого развития организаций на рынке телекоммуникаций"

12-13 ноября 2009 г. в Москве в рамках Европейской недели качества состоялся Конгресс организаций связи и информационных технологий "Современные направления устойчивого развития организаций на рынке телекоммуникаций", проводимый ежегодно в рамках Глобального проекта "России — новое качество роста". Понгрессу оказали Совет Федерации Федерального Собрания РФ и ОАО "Связьинвест".

Организаторы Конгресса: Федеральное агентство по техническому регулированию и метрологии, Ассоциация управления качеством связи и информатизации "Международный конгресс качества телекоммуникаций", НИИ экономики связи и информатики "Интерэкомс", Международный институт качества бизнеса, Международная академия менеджмента и качества бизнеса. Соорганизаторами Конгресса выступили саморегулируемые организации НП "СтройСвязьТелеком" и НП "ПроектСвязьТелеком".

Цель Конгресса: дать импульс развитию законодательной базы в области связи и IT, строительства и проектирования, предложить органам власти, компаниям и организациям эффективные решения, обеспечивающие устойчивое и успешное развитие в условиях финансово-экономической нестабильности, объединить на основе ключевых идей и технологий управления усилия общества, государства, организаций.

В своем приветствии участникам Конгресса Председатель Совета Федерации Федерального Собрания РФ С.М. Миронов отметил, что в современных условиях, когда глобальный экономический кризис внес свои коррективы во все ключевые направления развития как отдельной компании, так и экономики страны в целом, вопросы эффективного государственного и корпоративного управления обретают особое значение

В приветствии Министра связи и массовых коммуникаций РФ И.О. Щёголева организаторам, участникам и гостям Конгресса говорилось о том, что "для эффективного развития наукоемкой информационно-телекоммуникационной отрасли в первую очередь необходимо создание комфортной среды для работы специалистов, своего рода "экосистемы" интеллекта. Свой вклад в создание такой среды должны внести все: и государство, и отраслевые организации, и образовательные учреждения, и предприятия. Только совместными усилиями мы сможем создать микроклимат, наиболее благоприятный для основного ресурса отрасли - её кадрового капитала, людей, силами которых создаётся высокотехнологичный, инновационный, конкурентоспособный продукт.

В целях более продуктивного проведения мероприятия работа Конгресса проходила два дня и включала в себя пленарное заседания, а также "круглые столы" по злободневным вопросам сегодняшний ситуации в экономике страны.

Конгресс открылся в "Президент-Отеле" 12 ноября 2009 г. — во Всемирный день качества. Это ежегодное мероприятие отмечается во многих странах мира каждый второй четверг ноября. Этот день был учрежден по решению Европейской организации качества и Организации Объединенных Наций. Празднования по случаю этого дня впервые прошли в 1989 г. В современных условиях качество является ключом к успеху в деятельности любого предприятия, любой отрасли и каждой страны. Цель Всемирного дня качества состоит в повышении значения высокого качества продукции и услуг, а также в активизации той деятельности, которая направлена на привлечение внимания к проблеме качества — одной из самых приоритетных проблем в экономике ведущих стран мира.

Кроме того, как отметил в своем вступительном слове ведущий пленарного заседания, генеральный директор Группы компаний "Интерэкомс" Ю.И. Мхитарян, при составлении программы организаторы учитывали то, что Конгресс проводится в условиях мирового финансово-экономического кризиса, а также, что в отрасли произошли два знаменательных события: созданы саморегулируемые организации (СРО) — НП "ПроектСвязьТелеком" и НП "СтройСвязьТелеком". Ю.И. Мхитарян поздравил участников с присвоением Ростехнадзором РФ некоммерческим партнерствам "СтройСвязьТелеком" и "ПроектСвязьТелеком" статуса саморегулируемых организаций.

По итогам докладов и дискуссии в ходе Конгресса редакционная группа приступила к подготовке резолюции, направленной на поддержание и развитие отечественной экономики, организацию взаимодействия предприятий с саморегулируемыми организациями НП "СтройСвязьТелеком" и НП "ПроектСвязьТелеком" и их функционирование на телекоммуникационном рынке.

Следующий Международный конгресс "Инновационная экономика и качество управления" в рамках Глобального проекта "России — новое качество роста" будет проходить 8-9 апреля 2010 г. в Москве, в "Президент-Отеле".

На всех вокзалах Москвы заработает бесплатный беспроводной Интернет

С 7 декабря 2009 г. Дирекция железнодорожных вокзалов обеспечит все вокзалы Москвы бесплатным беспроводным Интернетом (Wi-Fi).

Зона покрытия бесплатного Wi-Fi охватит все объекты, расположенные на территории вокзальных комплексов Белорусского, Казанского, Киевского, Курского, Ленинградского, Павелецкого, Рижского, Савеловского и Ярославского вокзалов. Ожидается, что ежедневно услугой Wi-Fi будут пользоваться порядка более 1500 посетителей московских вокзалов.

"То, что пассажиры и посетители всех вокзалов Москвы теперь могут бесплатно пользоваться беспроводным Интернетом, — это очередной шаг в рамках реализации масштабной всероссийской программы модернизации вокзальных комплексов. Цель этой программы — повышение стандартов качества обслуживания и услуг, комфорта и безопасности пассажиров и посетителей вокзалов до европейского уровня", — поясняет Сергей Абрамов, начальник Дирекции железнодорожных вокзалов.

Первый пилотный проект бесплатной услуги WI-FI реализован 25 июня 2009 г. на Курском вокзале. До конца ноября эта услуга станет доступна на всех вокзалах Москвы, а в перспективе станет возможна и на вокзалах всех крупных городов России. Сейчас также прорабатывается возможность расширения пакета интерактивных сервисов на вокзальных комплексах. Например, возможности безналичной оплаты услуг через Интернет, использования электронных денег и услуги "личного кабинета".

МТС получила разрешение на использование частот для сети 3G в Москве

ОАО «Мобильные ТелеСистемы» сообщает о получении разрешения Роскомнадзора на использование радиочастот для базовых станций UMTS диапазона 2,1 ГГц на улицах Москвы, что позволит МТС запустить сеть 3G outdoor в Москве.

МТС продолжает уделять приоритетное внимание максимально широкому распространению 3G-сервисов, которые способны привнести новое качество, скорости в общение абонентов. С получением новых разрешений, компания сможет существенно расширить покрытие сети 3G МТС в столице, и обеспечить пользователям высокие скорости при работе с беспроводным Интернетом по всей территории Москвы.

МТС получила разрешение установить в Москве 783 базовых станций стандарта UMTS. В первую очередь сеть 3G outdoor от МТС покроет центральную часть Москвы в границах третьего транспортного кольца, в основных бизнес-районах столицы, на ключевых транспортных магистралях и транспортных узлах в пределах МКАД.

В мае 2009 г. МТС получила разрешение на запуск сети «нового поколения» в крупнейших бизнес-центрах и общественных местах столицы, также и на станциях и перегонах Московского метрополитена. Сегодня сеть 3G indoor от МТС действует в 39 важнейших точках Москвы, в том числе в районе «Москва-сити», Экспоцентре, Крокус-Сити, Центре международной торговли, БЦ «Новинский», «Арбат-Альфа-Центр», «Lotte Plaza», торговых центрах ЦУМ, «Атриум», «Европейский», «Москва», «Горбушкин двор», IKEA. Кроме того, МТС обеспечивает связью 3G офисы крупнейших предприятий Москвы, среди которых ОАО «РЖД», «Сбербанк России», АФК «Система» и др.

Абоненты 3G имеют возможность воспользоваться такими инновационными сервисами как видеозвонок и высокоскоростной доступ в Интернет в любой точки действия сети 3G. Высокая скорость передачи данных в сетях 3G (до 7,2 Мбит/с) обеспечит комфортное пользование сервисами по обмену данными – оперативную загрузку мультимедийного контента, удобный Интернет-браузинг, быструю работу с электронной почтой и файловыми приложениями.

О Концептуальных подходах формирования и развития ИТС в России

Позитивные изменения в облике мирового транспорта на рубеже XXI в. сопровождаются рядом негативных последствий, масштабы и значимость которых дают основания оценивать их как стратегические вызовы национального и даже континентального масштаба. К их числу относятся неприемлемый уровень людских потерь, рост потребления невозобновляемых источников энергии и негативного влияния на окружающую среду, постоянно растущие задержки людей и грузов на всех видах транспорта, связанные как с объективным недостатком мощностей транспортной инфраструктуры, так и с низким уровнем управления транспортными потоками.

Ключевые слова:
Интеллектуальные транспортные системы, ГЛОНАСС, спутниковая навигация, безопасность дорожного движения

Козлов Л.Н.,
доктор транспорта, действительный член Российской Академии транспорта, Вице-президент Международного конгресса промышленников и предпринимателей, член Совета директоров и Комитета по политике ИТС Международной Дорожной Федерации

Циклис Б.Е.,
к.т.н., Генеральный директор ФГУ "Дирекция по управлению федеральной целевой программой "Повышение безопасности дорожного движения в 2006-2012 гг."

Урличич Ю.М.,
д.т.н., член Президиума Российской академии космонавтики им. К.Э. Циолковского, Генеральный директор — генеральный конструктор ОАО "Российские космические системы", генеральный конструктор системы ГЛОНАСС, председатель Совета Ассоциации "ГЛОНАСС/ГНСС-Форум"

ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ В МИРЕ

Мировым транспортным сообществом решение найдено в создании транспортных систем, в которых средства связи, управления и контроля изначально встроены в транспортные средства и объекты инфраструктуры, а возможности управления (принятия решений), на основе получаемой в реальном времени информации, доступны не только транспортным операторам, но и всем пользователям транспорта.

Задача решается путем построения интегрированной системы: люди — транспортная инфраструктура — транспортные средства, с максимальным использованием новейших информационно-управляющих технологий. Такие "продвинутые" системы и стали называть интеллектуальными.

В последнее 10 лет словосочетание "Интеллектуальные Транспортные Системы" (Intelligent Transport Systems) и соответствующие аббревиатуры — ИТС, ITS — стали обычными в стратегических, политических и программно-целевых документах развитых стран.

При наличии определенных различий в толковании понятия ИТС в разных странах обобщающим может быть определение: "Интеллектуальные транспортные системы (ИТС) — это системная интеграция современных информационных и коммуникационных технологий и средств автоматизации с транспортной инфраструктурой, транспортными средствами и пользователями, ориентированная на повышение безопасности и эффективности транспортного процесса, комфортности для водителей и пользователей транспорта".

Идея ИТС, в своей основе, уже практически реализована в глобальном масштабе под руководством ИКАО в гражданской авиации. Благодаря стандартам и руководящим документам управление международными полетами, работой аэропортов и обслуживание пассажиров с использованием информационных и коммуникационных технологий гармонизированы. Все воздушные суда имеют средства связи, автономной спутниковой навигации, системы автоматического пилотирования, предотвращения столкновений в воздухе, управления посадкой и др. Наземные службы располагают технологиями постоянного контроля и управления в условиях плотного и эшелонированного воздушного движения.

Мировой опыт и инструменты реализации ИТС

Начиная с 80-х гг. большинство стран Европы, Азиатско-Тихоокеанского региона и США целенаправленно и систематически продвигают ИТС в качестве центральной темы в осуществлении транспортной политики.

Япония — одна из первых стран в мире, которая в 1973 г. приступила к проведению исследований по ИТС и реализации комплексной системы управления автомобильным транспортом. В 1996 г. пять министерств Японии, объединенных в Штаб, возглавляемый Премьер-министром, с участием академических кругов, промышленности, и специально созданной структуры "ИТС-Япония", начали реализовывать "Комплексный план для ИТС в Японии". Фаза развития ИТС после 2010 г. под девизом "Зрелость ИТС — Инновационное развитие социальных систем" является заключительным периодом этого проекта и позиционируется как базовая система для достижения общенациональных эффектов.

В 2003 г. обществом ИТС Япония был под-

готовлен еще один этапный документ — "Стратегия развития ИТС в Японии", в котором декларируется система трех "нулевых" целей:

1. Япония — зона нулевых потерь на дорогах; 2. Япония — зона нулевых задержек на дорогах; 3. Япония — зона комфортабельных транспортных условий (зона нулевых неудобств).

В **США** развитие ИТС базируется на национальных программах, реализуемых Министерством транспорта. В 1991 г. Конгресс США законом ISTEA впервые учредил, разработанную Минтрансом США, Федеральную программу — Пятилетний национальный программный план развития ИТС. В 1996 г. началась разработка программы стандартов ИТС по списку критических интерфейсов.

В 1998 г. в соответствии с законом TEA-21 началась разработка научно-исследовательской программы ИТС и программы развертывания ИТС, определена ведущая роль Минтранса США в продвижении интегрированной ИТС, созданы структуры федерального уровня, в т.ч. объединенный офис программы ИТС, который финансирует НИР, управляет эксплуатационными испытаниями, координирует разработку стандартов и действия Федеральных агентств.

Большинство государственных инициатив, таких как "Национальная архитектура ИТС", "Программа разработки стандартов", "Информационные системы и сети для коммерческих транспортных средств (CVISN)", "Программы общественного городского транспорта, сельские ИТС, мероприятия по безопасности пассажиров" и "Оценочная программа" создали основу, на которой в январе 2002 г. построена "План-Программа Национальной интеллектуальной транспортной системы: Видение на 10 лет" и разработан критический интерфейс для взаимодействия на региональном, штатном и национальном уровнях. Учреждена "Национальная расчетная палата ИТС" для обмена информацией и формирования политики.

Таким образом, в США создана система постоянно обновляемых официальных стратегических и программных документов по развитию ИТС, которая охватывает все уровни планирования — от стратегического до текущего, гарантируя на законодательном уровне участие государства в исследованиях, разработках и развертывании ИТС.

В **Азиатско-Тихоокеанском регионе**, дорожно-транспортные проблемы становятся все более серьезными из-за высокой концентрации населения в городах и резкого роста моторизации во многих странах. В Китае Министерство коммуникаций приступило к развитию ИТС в 1997 г. с создания лаборатории и Национального центра инжиниринга и технологий ИТС. Центр представляет команду исследователей из 40 различных институтов высшего образования типа Пекинского Университета Аэронавтики и Астронавтики, Пекинского Университета Почты и Телекоммуникаций и т.д. В 2000 г. Министерство науки и техники и более 10 заинтересованных министерств и комиссий совместно учредили Национальную группу по координации ИТС и Национальный офис ключевых проектов и предприятие ИТС-технологий, подведомственными Центру ИТС. В 2003 г. создан "Китайский Национальный технический комитет по стандартизации ИТС", в 2007 г. принята "Стратегия развития ИТС Китая". Созданы институциональные основы для поэтапного и планомерного развития ИТС.

Развитие ИТС в Китае осуществляется на плановой основе под полным контролем государства. Соответствующие задания на разработку и внедрение ИТС-сервисов отражаются в пятилетних планах развития экономики. Первоочередные проекты ИТС в Китае реализованы в системе сбора платежей на платных дорогах, что тесно связано с политикой развития сети скоростных автодорог страны, которые уже сегодня есть во всех провинциях, кроме Тибета. К декабрю 2006 г. запущено 160 систем электронной оплаты пошлин на 64 скоростных автомагистралях с общей протяженностью 3200 км.

Европейский Союз в 2006 г. принял политический документ "Европа в движении. Устойчивая мобильность для нашего континента", в котором выдвинута концепция интеллектуальной мобильности (intelligent mobility). Отмечается, что в долгосрочном периоде автомобили, поезда или суда должны иметь столь же развитое оборудование связи, навигации и управления, что и самолеты.

В феврале 2009 г. Комиссия ЕС выпуском ЗЕЛЕНОЙ КНИГИ "TEN-T: Обзор стратегии" начала процесс фундаментального пересмотра политики Трансъевропейской транспортной сети для формирования единой мультимодальной сети. Вводится новый концептуальный принцип развития приоритетной транспортной сети взамен действующего принципа приоритетных проектов, что инициирует процесс интеграции сетей и более системное использование узловых соединений (где чаще всего возникают заторы) — морских и воздушных портов в качестве пунктов входа в сеть и основных пунктов межмодального соединения. ИТС отводиться роль мостового соединения между жесткой инфраструктурой и интеллектуальным транспортом, ключа к достижению целей транспортной политики.

Понимание того факта, что реальное развертывание ИТС возможно только на основе соединения усилий государств и частного сектора (причем, роль последнего будет возрастать по мере роста рыночной привлекательности ИТС-сервисов) привело к созданию в 1991 г., одновременно с Японией и США, некоммерческой организации — общества ERTICO (ИТС Европа). Цели ERTICO состоят в содействии координированию усилий по развитию ИТС в Европе от научных исследований до рыночных инвестиций.

Общество успешно организует десятки проектов и инициатив в сфере ИТС и к настоящему времени является европейским лидером в этой сфере. Проекты ИТС включены в стратегические документы по развитию транспорта, рамочные программы исследований и разработок Евросоюза, в том числе, связанные с использованием GNSS ГАЛИЛЕО.

В качестве общеевропейской программы ERTICO выступила с инициативой по оборудованию транспортных средств специальными устройствами для определения местонахождения попавшего в аварию транспортного средства и вызова экстренных служб к месту ДТП.

Общественная инициатива ERTICO привела к принятию Еврокомиссией программы "e-call" ("экстренный вызов"), которая с 2010 г. должна стать общеевропейским законом. В странах ЕС, подписавших меморандум по внедрению программы "экстренный вызов", законодательно устанавливаются требования к автопроизводителям оборудовать поставляемые для продажи автомобили телематическими блоками, которые позволяют точно определить место ДТП по спутниковой навигации и в автоматическом режиме через диспетчерские центры вызвать необходимую помощь. В Финляндии, например, решили внедрить программу "экстренный вызов" не дожидаясь принятия общеевропейского закона.

Еще одной страной, утвердившей государственную программу "экстренный вызов", является Бразилия, где наблюдается высокая статистика погибших и пострадавших в результате ДТП.

Сфера активного развития ИТС

Реализация ИТС в глобальном масштабе стала возможной только в условиях насыщенного коммуникационного пространства, когда нет проблем с дешевой передачей значи-

тельных объемов цифровой информации в реальном времени в любой точке транспортной сети.

Сегодня наиболее активно развиваются базовые технологии для транспортной инфраструктуры и транспортных средств:

1. Интеллектуальные системы для инфраструктуры:

- управление движением на автомагистралях;
- коммерческие автоперевозки;
- предотвращение столкновений транспортных средств и безопасность их движения;
- электронные системы оплаты транспортных услуг;
- управление при чрезвычайных обстоятельствах;
- управление движением на основной уличной сети и ликвидация последствий ДТП;
- управление информацией;
- интермодальные грузовые перевозки;
- контроль погоды на автодорогах;
- эксплуатация автодорог;
- управление общественным транспортом;
- иформация для участников движения.

2. Интеллектуальные системы для транспортных средств:

- системы предотвращения столкновения;
- системы уведомления о столкновении;
- системы помощи водителю.

Одно из основных направлений развития ИТС в Европе, США и Японии, которое активно продвигается последние 15 лет — реализация концепции интеллектуального автомобиля. Работает международная программа "Транспортные средства повышенной безопасности". Уже первые опыты использования бортовых интеллектуальных систем показали, что они способны уменьшить число ДТП на 40%, а число ДТП со смертельным исходом на 50%.

Под термином "бортовые интеллектуальные системы" в ЕЭК ООН понимают системы, установленные на автомобиле в целях повышения его безопасности и использующие информацию, которая поступает как непосредственно от бортовых датчиков автомобиля, так и от дорожной инфраструктуры или других источников.

В настоящее время уже находятся в продаже или проходят полигонные испытания более десяти типов бортовых ИТС — Система поддержания дистанции в плотном транспортном потоке; Система удержания автомобиля на полосе; Система оповещения об усталости водителя; Система предотвращения боковых столкновений; Система удержания автомобиля при движении по кривой; Система обнаружения мотоциклистов и др.

Бортовые ИТС реализуют, как минимум, четыре функции:

— оказывают водителю помощь в предвидении дорожной обстановки;

— побуждают его к действиям по предотвращению опасной ситуации;

— снижают утомляемость водителя, принимая часть нагрузки по управлению автомобилем на себя;

— автоматически берут управление на себя, если водитель самостоятельно не смог выполнить необходимые действия по предотвращению ДТП, либо снижая тяжесть его последствий.

Сегодня в Японии ИТС-оборудование устанавливается как штатное на всех автомобилях высокого и среднего класса. Объем продаж постоянно растет. По состоянию на декабрь 2008 г. число продаваемых бортовых устройств достигло 23,2 млн. единиц и более 33,9 млн. единиц автомобильной навигационной системы.

Некоторые выводы из мировой практики развития ИТС

Развитие ИТС методологически базируется на системном подходе, формируя ИТС именно как системы, а не отдельные модули (сервисы). Подходы к созданию ИТС основываются на принципе модернизации, реинжиниринга действующих транспортных систем. Отсюда следуют важные принципы поэтапного развития и модульности создания ИТС.

Формируется единая открытая архитектура системы, протоколы информационного обмена, формы перевозочных документов, стандартизация параметров используемых технических средств связи, контроля и управления, процедур управления и т.д.

Организационно-методической основой развития ИТС служат национальные концепции развития ИТС, национальные архитектуры ИТС и программы развития, важным инструментом привлечения новых игроков на этот рынок стало формирование рыночных пакетов ИТС.

С 2000 г. общество стало ощущать результаты от развертывания ИТС.

Водители получили автомобили, оснащенные средствами безопасности, новые технологии, информацию о поездке и о дорожном движения в реальном времени.

Правительственные агентства увидели новые возможности систем контроля и управления дорожным движением в реальном времени.

Рынки развились до уровня использования в практической транспортной деятельности новых технологий. Начали реализовываться коммерческие проекты создания ИТС. По данным Ассоциации "ITS America" к 2015 г. мировой объем продаж ИТС составит более 400 млрд. долл. Европейский рынок оценивается величиной 100-130 млрд. евро.

Государственно-частное партнерство стало рассматриваться как средство для привлечения инвестиций частного сектора в научно-исследовательские работы и развитие ИТС, наряду с правительством, с сохранением ведущей роли последнего в формировании политики и планов развития ИТС. Около 80% инвестиций в ИТС делаются частным сектором, государство вкладывает 20% инвестиций в создание транспортной инфраструктуры, на которой ИТС-товары и услуги могут развиваться и реализовываться.

Развитие ИТС сегодня — высокоорганизованный процесс. Создана его нормативно-правовая база. Отлажен процесс стратегического и текущего планирования развития ИТС. Созданы специальные организационные структуры. Отлажен процесс бюджетного финансирования разработок и реализации пилотных проектов развертывания ИТС на национальном уровне.

Взаимодействие государства, промышленников, частного бизнеса, научного сообщества и пользователей обеспечивается созданием национальных и континентальных обществ (ассоциаций), таких как ИТС Америка, ЭРТИКО (ИТС Европа), ИТС Япония и др.

Важную роль в распространении знаний и опыта развития ИТС, установлении глобальных контактов в ИТС-сообществе играют ежегодные всемирные и европейские конгрессы ИТС, сопровождающиеся выставками и образовательными программами.

СОСТОЯНИЕ ТРАНСПОРТНЫХ СИСТЕМ В РОССИИ

В России, несмотря на отсутствие до настоящего времени планомерных работ по комплексному развитию ИТС, имелось и имеется достаточно много примеров попыток развития локальных элементов и систем, относящихся по современной терминологии к ИТС. Это, созданные в конце XX в., системы контроля и управления движением транспортных средств на всех видах транспорта, системы управления перевозками грузов и пассажиров, системы информирования и

продажи билетов и другие информационно-управляющие системы.

В настоящее время в России достаточно активно разрабатываются отдельные разрозненные элементы ИТС, что диктуется текущими потребностями рынка, а не долговременной стратегией. Наблюдается четыре процесса, связанных с развитием ИТС:

— разработка различными предприятиями и организациями собственных моделей ИТС;

— адаптация зарубежной и отечественной радиоэлектронной аппаратуры;

— предоставление локальных услуг (в основном мониторинга и дистанционной охраны автотранспорта) на основе разработок зарубежных фирм;

— широкая продажа бортовых комплексов сухопутной навигации и комплектующих.

В области ИТС действует около 200 государственных и частных предприятий (производители, интеграторы, сервисные фирмы, провайдеры, дилеры), деятельность которых никак не координируется и не регламентируется в государственном масштабе.

Каждый из видов транспорта развивает корпоративные информационные системы, направленные исключительно на решение внутренних задач, а не на интеграцию с информационными системами смежных видов транспорта.

Современное состояние рынка ИТС в России отличает разрозненность, фрагментарность, отсутствие национальных стандартов, несистемные контакты (а практически отсутствие таковых) с международными Ассоциациями ИТС.

Стихийное развитие локальных и корпоративных систем формирует среду, когда интеграция в единую интеллектуальную транспортную систему России окажется технически невозможной. Имеются и внешние угрозы — существующие проекты разрозненных элементов российских систем ИТС, в силу несогласованности с международными стандартами могут спровоцировать переключение международных транзитных перевозок в обход территории России.

Возрастание объемов грузопассажирских перевозок неизбежно приводит к нарастанию глобальных проблем:

— чрезвычайно высокому уровню аварийности и количества человеческих жертв на транспорте;

— недопустимо большой нагрузке на окружающую среду;

— резкому снижению эффективности перевозок ("пробки", задержки);

— снижению эффективности комбинированых перевозок.

Ежегодно в России в результате ДТП погибает порядка 30 тыс. человек и получают травмы более 250 тыс. человек, тяжесть дорожно-транспортных происшествий составляет 14 (человек погибших на 100 пострадавших в ДТП), тогда как в развитых странах Европы, Японии и США этот показатель не превышает 2. Из-за несвоевременного реагирования экстренных служб для оказания необходимой медицинской и технической помощи на месте происшествия погибают 56% пострадавших. В 93 случаях из 100 причиной аварий становятся неправильные действия участников дорожного движения. Ущерб экономики в результате ДТП оценивается в 2,6% ВВП, что составляет порядка 476 млрд. руб. До 80% общероссийских объемов грузовых перевозок осуществляется автотранспортом через территории крупных городов, резко увеличивая количество заторов в улично-дорожной сети.

Реализация федеральной целевой программы "Повышение безопасности дорожного движения в 2006-2012 гг." за период 2006-2008 гг.

В субъектах Российской Федерации действуют достаточно скоординированные с федеральной (или находящихся в стадии координации) 83 региональных и 1490 муниципальных программ по организации безопасности дорожного движения (ОБДД). Мероприятия, выполняемые в рамках федеральной и региональных программ, были направлены на повышение правового сознания и предупреждение опасного поведения участников дорожного движения, улучшение организации движения транспортных средств и пешеходов в городах, развитие системы оказания помощи пострадавшим в результате ДТП, совершенствование нормативно-правовых, методических и организационных основ управления деятельностью в сфере безопасности дорожного движения.

За три года на реализацию мероприятий Программы было выделено 15,5 млрд. руб., в том числе 7,8 млрд. руб. из федерального и 7,7 млрд. руб. из бюджетов субъектов РФ. В последние годы отмечается существенный рост ассигнований на мероприятия по ОБДД субъектами РФ. В 2008 г. финансовые вложения регионов России почти в 3 раза возросли по сравнению с 2006 г., что свидетельствует о повышении внимания к проблеме со стороны представительных и исполнительных органов власти на региональном уровне.

За это время сформировалась достаточно устойчивая тенденция уменьшения транспортного и социального риска, тяжести последствий ДТП, основных показателей детского дорожно-транспортного травматизма, что свидетельствует об эффективности принимаемых профилактических мер и об управляемости процесса снижения аварийности.

В 2008 г. количество лиц, погибших в результате дорожно-транспортных происшествий, по сравнению с 2004 г. уменьшилось на 4570 человек, что в 4,6 раза больше прогнозируемых показателей. При этом снижение основных показателей аварийности зафиксировано в 66 субъектах РФ. В целом с 2006 г. по 2008 г. в результате реализации программно-целевого подхода в деятельности по обеспечению безопасности дорожного движения были сохранены жизнь и здоровье более 7,5 тыс. человек.

Прошедший трехлетний этап реализации Программы (2006-2008 гг.) в значительной части можно рассматривать как информационно-поисковый, а достигнутые результаты по сокращению числа погибших при ДТП людей в сравнении с базовым 2004 г. не могут еще оцениваться как абсолютно устойчивое состояние системы ОБДД. Очевидно, что обеспечение устойчивого состояния системы ОБДД, в том числе последовательное планомерное снижение числа погибших в результате ДТП, невозможно без применения современных средств и технологий на транспорте и в транспортной инфраструктуре.

Проведенные исследования свидетельствуют о значительном ухудшении условий дорожного движения в крупных городах Российской Федерации. Скорость движения наземного транспорта упала практически до скорости пешеходного движения, количество задержек в движении, заторов превысило все допустимые нормы. Резко ухудшается экологическая обстановка. Основная причина такого положения — неподготовленность улично-дорожных сетей к приему и обслуживанию резко возрастающих транспортных потоков. Этот вывод подтверждается реальными условиями дорожного движения в Москве, Санкт-Петербурге, других городах-"миллионниках". По мнению экспертов и специалистов, главная причина сложившегося положения — интеллектуальное отставание в научной базе, производстве, проектировании, внедрении эффективных технологий в управление транспортными и пешеходными потоками.

Первоочередными задачами программы, направленными на решение указанных проблем, являются:

• создание условий для безостановочного движения на основе формирования и ввода в действие центров управления дорожным движением в городах с высокой интенсивностью и плотностью дорожного движения;

• создание условий для приоритетного движения общественного и специального транспорта;

• формирование системы предупреждения ДТП, снижения тяжести их последствий на базе современных технологий с использованием системы "ГЛОНАСС", интеллектуально-информационных конструкций, объединяющих программные разработки 2006-2008 гг.;

• максимально возможное внедрение аппаратно-программных комплексов, систем дистанционного и автоматизированного контроля за скоростными режимами дорожного движения и поведением участников дорожного движения;

• широкое применение эффективных информационных систем взаимодействия с органами и службами оказания помощи и ликвидации последствий ДТП.

Следует отметить, что в сегодня в России на государственном уровне не проработана стратегия развития как интеллектуально-информационных систем в целом и их основных компонентов, автоматизированных систем управления дорожным движением (АСУДД), так и других систем управления, интегрально входящих в систему обеспечения общественной безопасности. При этом эксплуатирующиеся в стране системы АСУДД в большинстве случаев относятся к системам "первого поколения", что объясняется попыткой простейшими средствами регулирования добиться улучшения ситуации.

Стране нужна транспортная система нового поколения, соответствующая сценарию инновационного развития. Вектор этого развития задан шестью целями транспортной стратегии РФ на период до 2030 г. Отсутствие должной активности государственных органов в этом направлении негативно скажется в ближайшем будущем на эффективности формирования ИТС и сделает проблематичным успешный переход транспорта на инновационный путь развития в стратегической перспективе.

В России отсутствует единая политика, концепция и другие атрибуты зрелого процесса развертывания ИТС. Этот термин даже не употребляется в стратегических документах по транспортной политике страны.

Более того, прошедший 7 апреля 2009 г. в Москве первый российский международный конгресс по ИТС продемонстрировал отсутствие у большинства докладчиков единого представления о том, что такое Интеллектуальные Транспортные Системы. В стране отсутствуют официальные организационные структуры, ответственные за развитие ИТС, как основного средства инновационного развития транспорта.

"Сегодняшнее состояние транспортной системы явно отстает от растущих потребностей России. Более того, неразвитость транспортной инфраструктуры уже стала "тормозом" экономики и сдерживает ее переход на инновационный путь развития. И нам жизненно важно перейти от простого поддержания транспортной системы к ее качественному развитию. ... Причем на самой современной технологической базе. Это прямая обязанность государства — развитие инфраструктуры". (В.В. Путин, выступление на совещании по вопросам развития транспорта, 20 мая 2008 г., г. Сочи)

КОНЦЕПЦИЯ, АРХИТЕКТУРА И НАЦИОНАЛЬНАЯ ПРОГРАММА РАЗВЕРТЫВАНИЯ ИТС РОССИИ

Концепция "интеллектуализации" транспорта рассматривается как главное средство для эффективного ответа на глобальные вызовы в условиях коммуникационного общества и инновационной экономики. Несмотря на наличие сложившейся и апробированной в мире общей концепции развития ИТС, практически все страны имеют свои национальные концепции ИТС, что зафиксировано в том или ином государственном документе.

Концепция ИТС представляет собой видение пользовательских услуг, идеологии построения системы, постановки задач и разработки планов системного и эффективного продвижения ИТС в России.

Концептуальную схему построения ИТС следует рассматривать как организацию системной формы взаимодействия всех видов транспорта, наиболее эффективное использование транспортного ресурса за счет совместных транспортных операций с наиболее рациональными вариантами структурно-поточных схем движения пассажиров и грузопотоков, обеспечивая качество транспортных услуг.

При разработке концепции следует учитывать возможности и этапы развития отечественной глобальной навигационной спутниковой системы ГЛОНАСС, которая являясь основой координатно-временного обеспечения Российской Федерации, уже сейчас используется в различных областях социально-экономической сферы для:

— навигации наземных, воздушных, морских, речных и космических средств, управления транспортными потоками на всех видах транспорта, контроля перевозок ценных и опасных грузов, контроля рыболовства в территориальных водах, проведения поисково-спасательных операций, мониторинга окружающей среды;

— геодезической съемки и определения местоположения географических объектов с сантиметровой точностью при прокладке нефте- и газопроводов, линий электропередач, в строительстве;

— синхронизации в системах связи;

— решения фундаментальных геофизических задач;

— персональной навигации индивидуальных потребителей.

Круг применения технологий спутниковой навигации постоянно расширяется, и сейчас даже трудно представить какие еще области применения космических навигационных систем появятся с повышением точности позиционирования в реальном времени в абсолютном пространстве. Для России, с ее обширной территорией и инфраструктурой, которая требует глубокой модернизации, значение внедрения средств спутниковой навигации возрастает многократно.

Первый Российский Международный Конгресс по ИТС (7-8 апреля 2009 г., Москва)

Успешная реализация федеральной целевой программы "Глобальная навигационная система" позволит России сохранить свой суверенитет в области навигации, сделать систему ГЛОНАСС конкурентоспособной по отношению к американской GPS и европейской GALILEO, создать нужную потребителям систему, как в России, так и за рубежом.

В качестве основы для создания ИТС в России необходимо использовать региональные навигационно-информационной системы (РНИС), создающиеся на базе ГЛОНАСС с целью повышения качества выполнения государственных функций и предоставления государственных услуг в части транспортного комплекса региона.

Основными задачами РНИС являются:

— управление транспортными средствами предприятий;

— моделирование, прогнозирование и оптимизация движения транспортных средств;

— автоматический контроль фактов нарушения регламентов работ, выполняемых транспортными средствами;

— планирование, диспетчерское управление государственным и муниципальным транспортом (пассажирский транспорт, транспорт жилищно-коммунального хозяйства (ЖКХ), скорой помощи и т.п.);

— контроль выполнения государственных и муниципальных контрактов на работы, связанные с осуществлением транспортной работы (пассажирские перевозки, вывоз отходов, очистка улиц и т.д.);

— контроль перевозок опасных и ценных грузов и крупногабаритных грузов;

— планирование и управление транспортными средствами органов внутренних дел, а также региональных и местных структур МЧС;

— информационное обеспечение специальных служб при возникновении криминальных или чрезвычайных ситуаций на транспорте для экстренного реагирования на них;

— оптимизации маршрутов движения транспортных средств;

— информирование граждан и организаций о функционировании транспортного комплекса региона.

РНИС представляет собой трехуровневую структуру:

— уровень предприятия (ПТП, АТП, ЖКХ, УВД и т.д.);

— уровень муниципального образования

— уровень субъекта РФ.

В настоящее время следует определить последовательность и этапы развертывания РНИС, а в перспективе ИТС на федеральном, региональном и муниципальном уровнях, предусматривая открытость их архитектуры.

В концепции следует определить первоочередные приоритеты: внедрение ИТС в крупных городах, развитие сети федеральных и строительство платных автодорог с обязательным развертыванием современных ИТС-компонентов, формирование международных транспортных коридоров в соответствии с принятыми в Европе стандартами ИТС, предусмотреть технические возможности развертывания коммерческих ИТС-сервисов.

ИТС — система сервисная. Поэтому в основу построения архитектуры должна быть положена информация о возможных потребностях в ее услугах для пользователей. В мировой практике определены пять основных типов пользователей ИТС: водители, пешеходы и велосипедисты, пассажиры общественного транспорта, перевозчики, транспортные операторы и службы эксплуатации транспортной инфраструктуры.

Перечень пользовательских услуг ИТС служит основой для формирования национальной архитектуры ИТС параллельно с проведением эффективной и систематической научно-исследовательской работой и деловой деятельностью. Он также дает понимание необходимости внедрения ИТС. Более полным представляется следующее определение термина: Национальная архитектура ИТС — это структура связанных подсистем, которые вместе обеспечивают предоставление пользовательских услуг с использованием своих функциональных возможностей и определенных интерфейсов между собой.

Архитектура ИТС обычно содержит более 150 пользовательских сервисов и определяет:

— функции, для выполнения данной услуги пользователю;

— физические объекты или подсистемы, где эти функции выполняются;

— интерфейсы и потоки информации между физическими подсистемами;

— требования к связи для передачи информационных потоков.

СТАНДАРТИЗАЦИЯ ИТС

Стандартизация ИТС рассматривается не только как средство гармонизации технических решений, но и как средство поддержки конкурентной среды, когда потребитель не привязан к определенному поставщику стандартизированного оборудования или программного обеспечения и может выбирать на рынке наиболее совершенные решения. Действия по разработке стандартов ИТС определяются структурой национальной архитектуры ИТС.

Процесс международной стандартизации осуществляется на мировом уровне в Международной организации по стандартизации (ISO) и на европейском уровне — в Европейской организации по стандартизации CEN. Созданные в этих организациях рабочие группы специализируются по направлениям: Архитектура; Системы возврата угнанных транспортных средств; Общественный транспорт; Управление стоянками и парковками; Общественная ближняя связь; Интерфейс человек/машина; Автоматическая идентификация транспортных средств; Широкополосная связь/протоколы и интерфейсы; Системы управления грузовым транспортом и подвижным составом и др.

К настоящему времени основная часть процессов, функций, интерфейсов, протоколов обмена данными, требований к оборудованию и другим аспектам ИТС в общем плане уже стандартизована на международном уровне, а в развитых странах — и на национальном уровне.

В России ИТС в настоящее время не регламентируются ни одним государственным стандартом. Полностью отсутствуют стандарты, которые регулируют отношения в области информации, коммуникаций и систем управ-

III Международный форум по спутниковой навигации (12-13 мая 2009 г., Москва)

ления наземными транспортными средствами в городе и в сельской местности, включая организацию дорожного движения, общественный транспорт, коммерческий транспорт, аварийные службы и коммерческие услуги в области ИТС.

РОЛЬ ГОСУДАРСТВА

Опыт стран Евросоюза, США, Японии, Китая и др. государств в продвижении проектов ИТС показывает, что в условиях рыночной экономики только единая государственная политика позволяет объединить усилия государства, субъектов Федерации, бизнеса всех уровней и секторов экономики в решении общенациональных целей в транспортном комплексе.

Государство осуществляет стратегически-инновационную функцию — поддерживает базисные технологические и экономические инновации, придавая им начальный импульс.

Концептуально важно подчеркнуть четыре основных, государственных направления:

— организующая и координирующая роль в создании институциональной основы для разработки национальной архитектуры ИТС и координационных планов развития;

— регулирующая роль — создание правового поля, стандартизация параметров в сфере безопасности и технической совместимости;

— стимулирующая роль — поддержка исследований и социально-ориентированных пионерных проектов ИТС-сервисов в сфере общественного транспорта и неотложных служб;

— инвестиционная роль — разработка и реализация ИТС-проектов, решающих задачи безопасности и производительности, которые могут создаваться и эксплуатироваться с привлечением частного капитала на условиях государственно-частного партнерства.

Эти роли реализуются путем разработки национальной концепции и программы развития ИТС, создания полномочных органов ответственных за их разработку и реализацию при Правительстве и Министерстве транспорта России.

РОЛЬ ПРОФЕССИОНАЛЬНОГО СООБЩЕСТВА

Необходимость в формировании профессиональной общественной организации логично вытекает из всей совокупности процессов, происходящих на дорогах нашей страны, является закономерным результатом развития и объединения отдельных усилий по выводу транспортной системы России на новый качественный уровень в самых различных аспектах — от организации дорожного движения до обеспечения полнейшей его безопасности.

Реструктурированное в этих целях в 2009 г. некоммерческое партнерство "ИТС-Россия" провозглашает своей миссией объединение профессионального сообщества для поддержки политики и содействия усилиям Правительства в формировании и продвижении в России Интеллектуальных Транспортных Систем.

Стратегия "ИТС-Россия" заключается в создании платформы для эффективного взаимодействия государственных институтов, частного сектора, заинтересованных кругов и общественности в проведении исследований, экспертизы, внедрения и развертывания проектов, формирование профессионального и общественного консенсуса в сфере ИТС.

"ИТС-Россия" объединяет представителей государственных органов (местного, регионального и общегосударственного уровней), промышленности, науки и образования, поставщиков услуг (транспортных и телекоммуникационных), пользователей (операторов инфраструктуры, грузоперевозчики).

"ИТС-Россия" развивает сотрудничество с национальными ИТС-сообществами и международными институтами, что позволяет изучать стратегические направления развития в области ИТС на европейском и глобальном уровнях, и открыто для всех государственных, общественных, частных и международных организаций, которые развивают активную деятельность или заинтересованы в реализации интеллектуальных транспортных систем. Это структура, способная стать лидером в области формирорвания ИТС, интегратором творческого потенциала, накопленного опыта и понимания всего многообразия стоящих задач.

ОСНОВНЫЕ ВЫВОДЫ

1. В мировой практике ИТС признаны как общетранспортная идеология интеграции достижений телематики во все виды транспортной деятельности для решения проблем экономического и социального характера — сокращения аварийности, повышения эффективности общественного транспорта и грузоперевозок, обеспечения общей транспортной безопасности, улучшения экологических показателей.

2. Разработки и развертывание ИТС — это потенциально эффективный конкурентоспособный инновационный бизнес и стимул развития нового высокотехнологичного сектора промышленности, что является важным антикризисным фактором.

3. Механизмы реализации отличаются в разных странах, однако ключевые компоненты одинаковы везде. При наличии апробированной в мире общей концепции развития ИТС, все страны имеют свои национальные концепции и приоритетные программы развертывания ИТС, что зафиксировано в том или ином государственном документе.

4. Внедрение ИТС носит стратегический характер, определяет в целом конкурентоспособность каждой страны на мировом рынке и в связи со значительной капиталоемкостью не реализуема без непосредственного участия государства. Координация и продвижение национальных программ ИТС осуществляется уполномоченным государственным межведомственным органом — лидером в выработке общеполитических и системно-архитектурных решений, технической и функциональной стандартизации.

5. Партнерство Правительства, бизнеса, науки и общественности являются ключом к успешному развитию ИТС. Это реализуется созданием обществ, типа "ИТС-Япония", "ИТС-Америка", "ERTICO" в Европе и тд. Серьезный акцент делается на демонстрационных проектах ИТС для их популяризации в обществе и маркетинге возможностей промышленности.

В национальном масштабе развитие программы ИТС в России становится одной из эффективных мер для решения серьезных социальных и антикризисных проблем, источником создания новых отраслей промышленности и движущей силой для создания передового информационно-телекоммуникационного общества.

Литература

1. Федеральная целевая программа "Повышение безопасности дорожного движения в 2006-2012 гг.".

2. Федеральная целевая программа "Глобальная навигационная система".

3. Материалы 7-го Европейского Конгресса по ИТС (04.06.2008, Женева).

4. Материалы Международного конгресса "Безопасность на дорогах ради безопасности жизни" (17.09.2008, Санкт-Петербург).

5. Материалы 15-го Всемирного Конгресса по ИТС "Связи ИТС: Экономия Времени, Спасение Жизней" (16.11.2008, Нью-Йорк).

6. Материалы Первого Российского Международного Конгресса по Интеллектуальным Транспортным Системам (7.04.2009, Москва).

7. Материалы III Международного форума по спутниковой навигации (12.05. 2009, Москва).

SPACE APPLICATIONS & TECHNOLOGIES
SAT EXPO EUROPE

HIGH PATRONAGE OF THE PRESIDENT OF THE ITALIAN REPUBLIC

PATRONAGE OF THE EUROPEAN COMMISSION

2010 SAT EXPO EUROPE

THE FIRST INTERNATIONAL MEETING IN 2010 ON SPACE SERVICES AND APPLICATIONS AND INTEGRATED TELECOMMUNICATIONS (HDTV, 3D CINEMA VIA SAT, DTT, IPTV, NEW BANDS AND NEW SERVICES)




B2B MEETINGS

ROME FAIR-ITALY, 4-5-6 FEBRUARY 2010

SAT Expo Europe 2010 will host the major players of the world aerospace industry, with a focus on space applications. It is an extraordinary business opportunity to meet with over 5,000 trade professional operators from all over the world.

SAT Expo Europe 2009: 5,400 visiting operators, 1,400 B2B meetings in the space of two days.

3ª MEDITERRANEAN SPACE CONFERENCE
The European instruments for environmental control and security in the Mediterranean Area

GEOPOLITICS:
- Space geopolitics and cooperation in the Mediterranean and in the world
- Indian Space vision and programmes

NAVIGATION:
- Ready for EGNOS: a new era for European navigation
First European EGNOS Conference
In collaboration with DG TREN of the European Commission
- The prospects of unmanned flight, from the UAV to the USV: aeronautics and space are closer

ENVIRONMENT AND SECURITY:
Earth observation: the role of Europe, national contributions to the european programme, applications

MEETINGS WITH SMEs:
- Big Players meet SMEs
- Italian and Indian companies meet

EDU DAY:
- Round table: the culture of space. An opportunity for youth education and the development of new skills
- R2R (Research to Research): meetings between Universities, Research and Enterprises

BROADCASTING:
- HD Forum Italia press conference
- 3D: the latest technology for the new language of cinema and TV
- Digital cinema distribution
- Satellite and local televisions

INSTALLER MEETING:
- Technical workshops
- TivùSAT: how to receive, install and distribute the new italian platform
- Tooway Installer Meeting
- ANACI - RAI - INSTALLERS Meeting

SCIENTIFIC CONFERENCES:
- S Band Scientific Conference
- Conference Personal Satellite Services (PSSatS)

SCIENTIFIC COOPERATION

esa · asi agenzia spaziale italiana · ASSOKNOWLEDGE

PARTNERS

ASAS · AIAD · AIPAS

MAIN SPONSORS

FINMECCANICA · eutelsat COMMUNICATIONS · Skylogic a eutelsat company

FOR FURTHER INFORMATION AND TO REGISTER: WWW.SATEXPO.IT/EN
Organisation: Promospace Tel: +39 0444 543133 – e-mail: info@satexpo.it

Pentastudio

Дешевый и безопасный контент-хостинг — оптимальное решение для небольших операторов

info@conax.com
www.conax.com

Испытанная модель безопасного хостинга Conax позволяет поставщикам услуг перейти к цифровому вещанию без крупных авансовых капиталовложений.

Полномасштабная надежность, разработанная для небольших платформ

По некоторым оценкам во всем мире более 100 миллионов абонентов подключены к небольшим телевизионным платформам.

Безопасный контент-хостинг, предоставляемый одобренными партнерами Conax, является экономичной, приспособленной ко всем сегментам, моделью защиты, предоставляющей службам цифрового телевидениям легкое и проверенное решение для "перехода в цифру", что является заведомо дорогостоящей опцией для большинства операторов.

Независимо от размера или места положения, хостинг-операторы Conax получают полномасштабные преимущества безопасности и благоприятные схемы расчета цены, и это только некоторые ключевые преимущества. Conax уже предлагает безопасный хостинг через многих одобренных хостинг-партнеров в Европе и планирует его расширение в другие регионы.

Преимущества для операторов

Начальные капиталовложения для операторов цифрового телевидения, участвующих в решениях Conax, обеспечивающих безопасность контента существенно снижаются благодаря централизации головных компонентов и совместному использованию основных сервисов.

Безопасный хостинг обеспечивает операторам:

- дополнительную стабильность;
- минимальные авансовые инвестиции;
- уменьшение расходов на эксплуатацию;
- быстрое и легкое оцифровывание;
- соответствие местным требованиям и поддержку.

Хостинговая модель защиты контента гарантирует одинаково высокий уровень известной контент-безопасности Conax, а так же предоставленную Conax свободу выбора одобренных абонентских телевизионных приставок.

"Conax предлагает отработанную модель премиальной безопасности через местных партнеров, независимо от объема услуг".

Успех партнера в безопасном контент-хостинге

История успеха LICA S.r.o. (www.lica.cz), партнера Conax по хостингу, укрепила репутацию продукции и создала портфель услуг для всестороннего сотрудничества с Conax. Телевизионным операторам предлагают лучшие в своем классе комплексные решения, включая доступную в настоящее время контент-безопасность. Посредством решения безопасного контент-хостинга LICA от Conax, местные операторы извлекают равнозначную пользу из аналогичной премиальной модели контент-безопасности как и при полномасштабном обслуживании. Кроме того, они получают прибыль от совместных централизованных затрат.

Объединение безопасности продукции Conax с экспертизой рынка LICA позволило LICA обеспечить весьма успешное и гибкое предложение хостинга — облегчающее службам цифрового телевидения, вне зависимости от их размера и деловой модели, получение защиты контента. Телевизионные операторы, работающие с LICA и эксплуатирующие контент-безопасность Conax имеют возможность широкого выбора одобренных потребителем устройств безопасности Conax.

"Сотрудничество с Conax в совокупности с надежностью ее продукции позволило LICA обеспечить успешное и гибкое предложение хостинга — облегчающее службам цифрового телевидения, вне зависимости от их размера и деловой модели, получение защиты контента", — заявил г-н Петр Линк, главный администратор, LICA.

Телевизионные операторы, работающие с LICA и эксплуатирующие контент-безопасность Conax имеют возможность широкого выбора одобренных потребителем устройств безопасности Conax."

Хостинг обеспечивает стабильность

Большой опыт и надежность работы позволяет LICA предложить равнозначную стабильность системы как для централизованной так и для локальной работы, делая выбор рабочей модели простым коммерческим решением. LICA предоставляет телевизионным операторам беспрецедентную свободу выбора.

Уменьшение инвестиций

Одним из ключевых моментов использования безопасного контент-хостинга LICA является существенное снижение затрат на ввод в эксплуатацию по сравнению с обособленными операционными системами. Системные издержки делятся между операторами системы, таким образом издержки связанные с обучением и укомплектованием персоналом также уменьшаются.

Быстрое и легкое оцифровывание

Эксплуатация аналоговой кабельной сети существенно отличается от цифровой сети. Небольшие бизнес-модели позволяют получить большую пользу и максимальные доходы от привлечения посредников.

Перспективные решения

LICA обеспечивает гибкий сервис защиты контента, приспосабливаемый как к изменению рабочих потребностей, так и к росту бизнес-моделей. Conax оказывает содействие LICA через всестороннее обучение, передовую техническую поддержку, непрерывное развитие продукта, внесение перспективных сервисных предложений и эффективный возврат инвестиций.

Большинство партнеров в рамках глобальной сети Conax предлагают дополнительный сервис, например EPG (электронное расписание программ) и SMS (служба коротких сообщений), предоставляя рентабельную системотехнику и соглашение об общей поддержке. Безопасный контент-хостинг Conax легко интегрируется с деловыми моделями, включая дополнительные услуги, например повременная оплата, визуализация по требованию и ваучеры.

Доступность только лучшего

Стратегия Conax, направленная на свободыу выбора, обеспечивает телевизионным операторам и их партнерам разнообразные, надежные и одобренные телевизионные абонентские приставки для принятия лучшего решения, соответствующего их бизнес-модели.

Телевизионные операторы, работающие с LICA и использующие безопасность контента Conax имеют широкий выбор одобренных Conax устройств. LICA также является официальным дистрибьютором телевизионных абонентских приставок Handan и поставщиком модуля условного доступа Technisat.

Несколько слов о Lica (www.lica.cz)

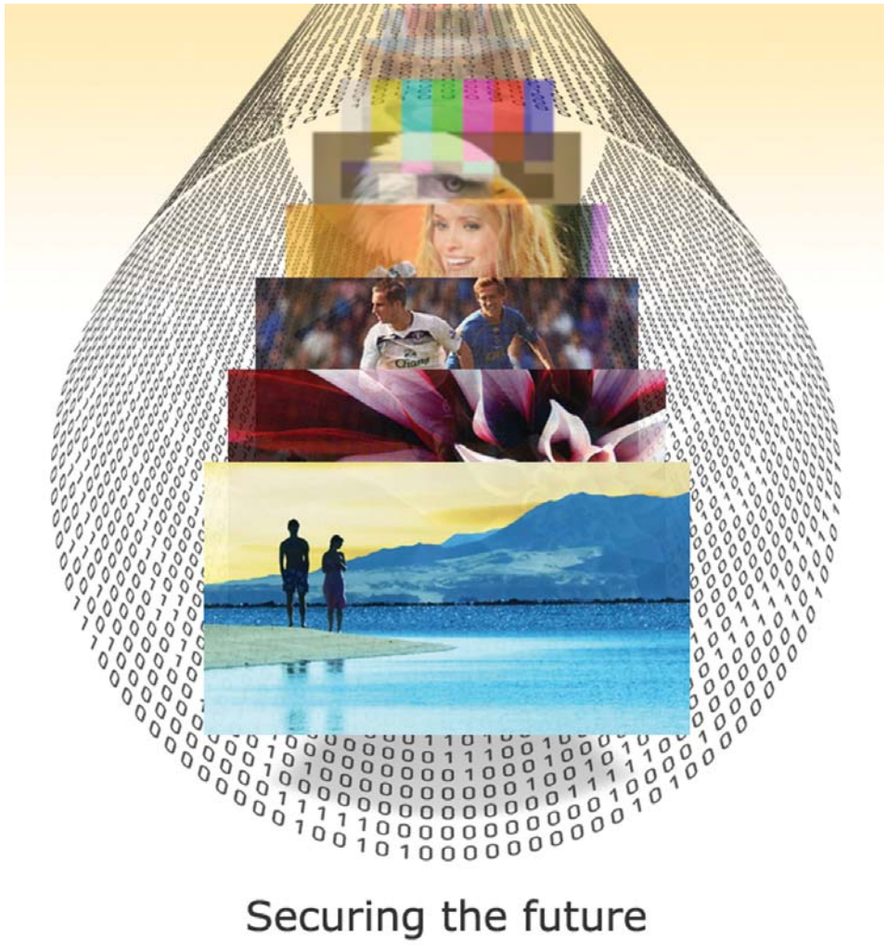
LICA, ведущий интегратор технологии, расположенный в Нимбурк, Чешская республика. Основная деятельность LICA — поставка, сборка, установка и поддержка эксплуатации сложного вещания стандартов DVB-C и DVB-T от головного узла до абонентской приставки, через цифровую ТВ-трансляцию DVB или IPTV. Для защиты контент-поставки, LICA предоставляет своим заказчикам безопасность контента Conax и опцион хостинга системы сервера SAS.

Несколько слов о Conax

Conax, ведущий мировой поставщик решений безопасности в области цифрового телевидения и распределения контента, обеспечивающий защиту оплачиваемого телевизионного контента, передаваемого через все типы сетей — кабель, спутник, IP, наземный и MMDS (многоканальную многопунктовую распределительную сеть). Через глобальную сеть партнеров, Conax предлагает современный уровень безопасности контента для более 350 операторов цифрового телевизионного вещания в более 80 странах по всему миру. Conax имеет сертификаты соответствия ISO 9001 (система качества) и ISO 27001 (обеспечение безопасности). Все изделия Conax соответствуют открытым стандартам.

Штаб-квартиры Conax размещены в Осло, Норвегии, с филиалами в США, Индии и Германии, с офисами продаж и поддержки в России, Сингапуре, Китае, Южной Корее, Бразилии и Канаде.

Conax входит в состав Telenor Group (www.telenor.com). Telenor Group вещает в 13 странах, имеет 168 миллионов мобильных абонентов по всему миру и является одним из крупнейших операторов мобильной связи в мире.



Построение эффективной системы защиты персональных данных

После изменений, внесенных в Кодекс об административных нарушениях (КоАП) 20 июня 2009 г., для всех стало очевидным, что затраты за защиту персональных данных (ПДн) неизбежны. В нынешних условиях финансового кризиса становится актуальной задача разумного и эффективного расходования средств — как затратить ресурсы не столько на покрытие требований регуляторов, сколько на укрепление собственной безопасности, и таким образом превратить вынужденные потери во вложения в повышение конкурентоспособности компании.

Ключевые слова:
защита персональных данных, информационная безопасность

Полещук А.В.,
ООО "Безопасные телекоммуникации",
руководитель отдела консалтинга,
pol@sectel.ru

Для обеспечения безопасности ПДн, в соответствии с требованиями федерального закона 152-ФЗ "О персональных данных" и его подзаконных актов, надо разработать и внедрить Систему защиты персональных данных (СЗПДн). Таким образом, основным вопросом является "Как построить эффективную СЗПДн?".

Поиски ответа на этот вопрос приводят нас к основному подзаконному акту — "Положению об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" (781-ПП). Внимательное прочтение п.12, содержащего перечень из 10 основных мероприятий по обеспечению безопасности ПДн, напоминает требования международного стандарта ISO/IEC 27001:2005 "Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования" (далее — Стандарт) к построению Системы управления ИБ (СУИБ) и ее основным процессам.

Почти всем подпунктам п.12 781-ПП можно найти соответствующие им по требованиям пункты раздела 4 Стандарта, приведенные в табл. 1.

В тексте Стандарта не удалось найти какого-либо прямого соответствия требованию п.12.в) 781-ПП о "проверке готовности СЗИ". Данный функционал должен выполняться в рамках внедрения защитных мер, либо может

Таблица 1

Соответствие требований 781-ПП и Стандарта ИСО 27001

781-ПП п.12	ИСО 27001 п.4
а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз	4.2.1 d) Определение рисков ИБ Организация должна идентифицировать ресурсы и угрозы для этих ресурсов
б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;	4.2.1 g) Выбор мер реагирования на риск Задачи управления и защитные меры должны быть выбраны и реализованы таким образом, чтобы удовлетворялись требования, определенные в результате процесса оценки риска и реагирования на риск. При их выборе следует принять во внимание критерии принятия риска, а также законодательные, нормативные и договорные требования.
в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;	соответствий нет
г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;	4.2.2 c) Реализация мер защиты Организация должна реализовать меры контроля, выбранные по результатам оценки риска, чтобы обеспечить решение задач управления
д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;	4.2.2 e) Повышение осведомленности Организация должна реализовать программы подготовки и обеспечения осведомленности
е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных; ж) учет лиц, допущенных к работе с персональными данными в информационной системе;	4.2.2 g) Управление ресурсами Управлять ресурсами для СУИБ 4.2.2 f) Управление функционированием Управлять функционированием СУИБ
з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;	4.2.3 e) Внутренний аудит Организация должна проводить внутренние аудиты СУИБ с запланированной периодичностью
и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;	4.2.2 h) 4.2.3 a) Управление инцидентами Реализовать процедуры и другие защитные меры, способные обеспечить оперативное обнаружение событий информационной безопасности и реагирование на инциденты информационной безопасности. Оперативно обнаруживать ошибки в результатах обработки. Оперативно выявлять попытки и состоявшиеся нарушения безопасности и инциденты.
к) описание системы защиты персональных данных.	(4.1), 4.3.1 c), 4.3.1 g) Требования к документированию Система управления информационной безопасностью (СУИБ) должна быть надлежащим образом документирована.

быть реализован позднее, в рамках задач внутреннего аудита организации. Сходным образом можно ассоциировать проверки СЗПДн регуляторами с сертификационными аудитами СУИБ третьей стороной.

Таким образом, можно отметить, что 781-ПП содержит почти все требования Стандарта ISO/IEC 27001:2005 к разработке и эксплуатации СУИБ, за исключением следующих:

1. Определение области действия СУИБ.
2. Определение политики СУИБ.
3. Выбор методологии управления рисками.
4. Частично, управление рисками.
5. Измерение эффективности мер контроля и функционирования СУИБ.
6. Регулярные ревизии эффективности СУИБ.
7. Пересмотр с запланированной периодичностью оценки риска.
8. Регулярные ревизии СУИБ со стороны руководства.
9. Соответствующие корректирующие и профилактические меры.

Если принять во внимание, что областью действия СЗПДн являются все ИСПДн, политика СУИБ явно определена в Законе и 781-ПП (п.п. 2 и 11), а в области методологии управления рисками регуляторами разработаны документы по классификации систем, определению угроз и выбору защитных мер, то аналогия между этими документами становится более чем заметной.

Проводя дальнейший анализ, можно найти и другие пункты нормативных требований подзаконных актов 152-ФЗ в той или иной мере соответствующих частным требованиям Стандарта к разработке, документированию, внедрению, эксплуатации и контролю СУИБ, включая особые требования к управлению инцидентами. Если степень соответствия требований условно разделить на категории "да/нет/частично" и ввести их цветовое обозначение, то можно составить условную карту соответствия. В карте, приведенной в табл. 2, частные требования и подпункты, условно представленные клетками соответствующих пунктов, раздела 4 Стандарта ИСО 27001, и обозначены цветом по следующему принципу:

- зеленый — есть соответствующее требование;
- красный — аналогичных требований нет;
- желтый — есть требования соответствующие частично/не в полной мере.

Таблица 2

Карта относительного соответствия требований ИСО 27001:2005 и нормативных требований подзаконных актов 152-ФЗ

ИСО 27001, р.4 «Система управления информационной безопасностью»	
Пункты раздела 4	Подпункты/частные требования
4.1 Общие требования	
4.2 Создание и управление СУИБ	
4.2.1 Создание СУИБ	a b c d e f g h i j
4.2.2 Внедрение и эксплуатация СУИБ	a b c d e f g h
4.2.3 Мониторинг и анализ СУИБ	a b c d e f g h
4.2.4 Сопровождение и совершенствование СУИБ	a b c d
4.3 Требования к документированию	
4.3.1 Общие требования	a b c d e f g h i
4.3.2 Управление документами	a b c d e f g h i j
4.3.3 Управление записями	

Как известно пункты 4.2.1-4.2.4 Стандарта — это требования к соответствующим фазам циклически повторяющегося процесса, используемого в управлении качеством, т.н. цикла PDCA или Деминга-Шухарта.

Если спроецировать интегральную оценку соответствия частных требований на соответствующие фазы PDCA (с аналогичной введенной выше цветовой маркировкой), то наглядно видно (рис.1), что коренным отличием СЗПДн (по требованиям) от СУИБ является отсутствие управленческого контроллинга, замыкающего классический цикл Деминга-Шухарта, присущего организациям с высоким уровнем зрелости и обеспечивающего поддержание процесса на заданном уровне с течением времени.

Можно предположить, что, в зависимости от уровня зрелости организации, СЗПДн, построенная по существующим нормативным требованиям, будет развиваться по одному из двух путей:

- если процессы защиты ПДн будут иметь вид замкнутого цикла с обратной связью, то рано или поздно СЗПДн станет частным случаем применения Стандарта, с учетом специфики российских законодательных требований;
- при отсутствии сложившейся корпоративной культуры управленческого контроллинга замкнутости цикла не будет, что может привести к снижению уровня защиты ПДн, возникновению соответствующих рисков и необходимости проведения повторных работ.

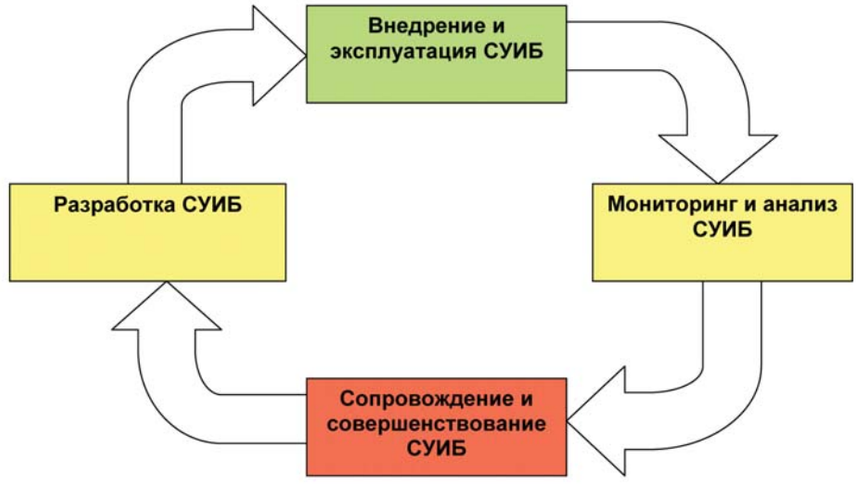


Рис. 1. Фазы СУИБ в цикле Деминга-Шухарта PDCA

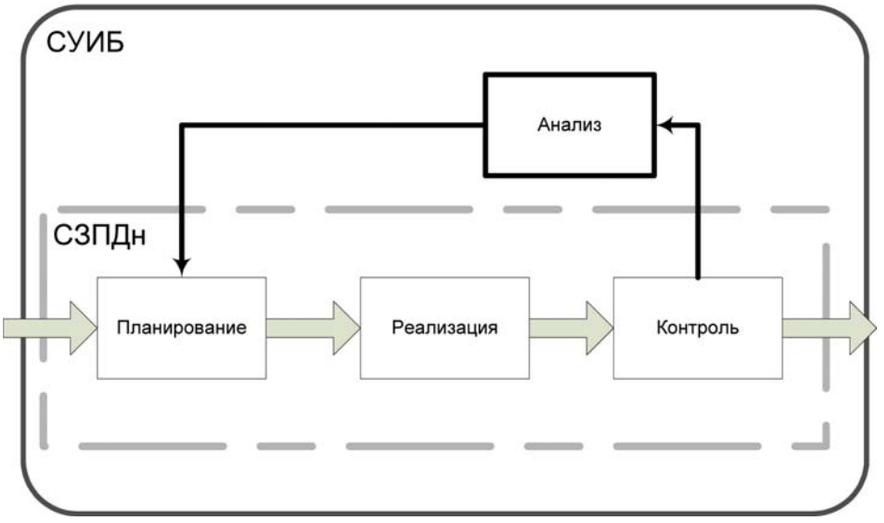


Рис. 2. Организация обратной связи по управлению в СУЗПДн

Таким образом, очевидно, что эффективность защиты ПДн, прежде всего, зависит от наличия адекватной системы управления. Для построения такой системы достаточным условием является интеграция СЗПДн и СУИБ, в рамках которой и организуется обратная связь, замыкающая цикл управления (рис. 2).

Будем называть такую интегрированную систему Системой управления защитой персональных данных (СУЗПДн). Попробуем перечислить возможные преимущества интегрированной СУЗПДн.

Во-первых, появляются новые комплексные рекомендации по построению СУЗПдн и ответы на частные вопросы: "Как организовать контроль за эксплуатацией средств защиты информации?", "Какое и как организовывать обучение?", — что позволяет, в условиях ограниченности оставшихся сроков, от диспутов перейти непосредственно к делу.

Во-вторых, поскольку частные вопросы полностью покрываются соответствующими процессами СУИБ: внутренний аудит, управление компетенциями и повышение осведомленности, управление инцидентами — можно использовать накопленный опыт и сложившиеся рекомендации, что позволит сократить сроки разработки и внедрения СУЗПДн.

В-третьих, это позволяет привлечь к разработке СУЗПДн специалистов по СУИБ 27001 (которых в стране больше) снижая нагрузку на ограниченный контингент экспертов по ПДн, что, в свою очередь, положительно скажется как на качестве систем, так и на их количестве.

В-четвертых, применение технологий управленческого контроллинга даст руководителям организаций прямую возможность влиять на ключевые моменты внедрения и эксплуатации СУЗПДн, что доказано многолетней практикой СУИБ.

В-пятых, практика регулярной оценки, пересмотра и совершенствования СУИБ привнесет в СЗПДн способность не терять актуальности с течением времени и всегда быть готовыми к очередной проверке регулятора.

В-шестых, подход к управлению рисками СУИБ подразумевает такие эффективные методы его обработки как избегание, снижение или его передача. Логика построения СЗПДн, представленная в большинстве нормативных документов, полностью ориентирована на обработку угроз путем внедрения комплекса защитных мер. В результате, альтернативные пути защиты ПДн (отказ от обработки, передача обработки третьим лицам, минимизации перечня данных) ставятся на повестку дня в организациях крайне редко, несмотря на их экономическую эффективность и наличие требования.

Очевидно, что организациям, уже внедрившим у себя СУИБ на разработку и внедрение СУЗПДн, при привлечении соответствующих специалистов, потребуется всего 2-3 месяца для интеграции методологий управления рисками и доработки некоторых внутренних документов. Для остальных организаций внедрение СУЗПДн станет основным шагом для переоценки подходов и принципов управления ИБ и выстраивания качественно новой, управляемой системы обеспечения безопасности.

С практической точки зрения, в рамках интеграции СЗПДн в СУИБ необходимо, как минимум, решить следующие моменты:

1. Дополнить политику СУИБ целями и задачами обеспечения безопасности ПДн и соответствия требованиям 152-ФЗ, его подзаконных актов, КЗоТ (гл.14).

2. Дополнить методологию инвентаризации активов таким образом, что бы она охватывала ПДн, ИСПДн и отношения с персоналом и третьими лицами. При инвентаризации АС должна проводиться классификация ИСПДн.

3. Расширить Область действия СУЗПДн на все ИСПДн.

4. Переработать методику анализа рисков с тем, что бы рассматривались все актуальные угрозы ИСПДн, определяемые по методике ФСТЭК.

5. При выборе защитных мер руководствоваться не только приложением "А" Стандарта, но и рекомендациями ФСТЭК.

6. Определить показатели функционирования и эффективности СУЗПДн.

Наиболее сложным является адекватно интегрировать методики оценки угроз из-за их идеологической разнонаправленности: угрозы ПДн оцениваются по качественной шкале ущерба для субъектов ПДн, а оценка рисков в СУИБ, как правило, оценивается в количественном размере материального и репутационного ущерба для организации (которого от утечки ПДн можно и не усмотреть в связи с небольшой величиной существующих штрафов или судебных издержек для крупных компаний). В связи с этим следует вспомнить, что по некоторым пунктам КоАП нарушение требований защиты ПДн может повлечь за собой изъятие технических средств или приостановление деятельности организации на срок до 90 дней. Для оператора ПДн, в таком случае, максимальный размер ущерба становится весьма значимым риском и вопросы защиты ПДн получают большую значимость. Остальные процессы СУИБ, при их правильной организации и налаженны-

Рис. 3. Фаза планирования интегрированной СУЗПДн

ми связями с процессом управления рисками, доработки не потребуют.

Фаза планирования СУЗПДн, учитывающая существующие нормативные и методические документы в области защиты ПДн, может принять следующий вид, приведенный на рис. 3.

Как уже говорилось ранее, одним из наиболее существенных преимуществ такой интегрированной системы СУЗПДн может стать ее эффективность и рационализм в области управления рисками, основанные на классической парадигме ИБ: "стоимость защитных мер должна быть соизмерима с размером ущерба". Благодаря этому система должна приобрести экономическую обоснованность.

Система становится управляемой и понятной для топ-менеджмента в результате трансляции угроз ИБ на уровень актуальных операционных рисков организации.

Ключевые показатели СУЗПДн должны охватывать количественные и качественные характеристики функционирования системы, и отражать ожидаемую величину выбранного показателя эффективности. Как вариант, можно предложить следующий набор показателей СУЗДПн:

• Количественные показатели функционирования за период времени:

— количество ИСПДн;

— количество произошедших инцидентов;

— количество реализованных мероприятий;

— количество выявленных недостатков на внутренних аудитах;

— затраты за защиту ПДн;

— размеры фактического ущерба по каждому инциденту и за период времени.

• Степень готовности к проверке:

— процент реализации планов и мероприятий;

— процент реализации требований по каждой ИСПДн.

• Соотношение ожидаемого ущерба и затрат на защиту:

— по каждой ИСПДн;

— по СУЗПДн в целом.

Непрерывный мониторинг и внутренний контроль (аудит) позволят всегда знать объективную степень готовности к проверкам и своевременно выявлять несоответствия требованиям.

Распределение и документирование обязанностей по процессам снизят нагрузку на руководящий состав и сделают систему гораздо устойчивее к ошибкам персонала.

В качестве примера можно рассмотреть типовую ошибку классификации ИСПДн — зачастую в организациях общедоступные корпоративные справочники классифицируются на К2 (вместо К4). В большинстве случаев подобные ошибки проходят мимо руководства и приводят к необоснованным затратам. В СУЗПДн такая ошибка может быть выявлена без привлечения эксперта по ПДн — на этапе управления рисками ввиду явного несоответствия размера ущерба и стоимости его обработки.

Еще одним ключевым преимуществом может стать периодическая основа и контроллинг. В рамках предупреждающих и корректирующих действий по совершенствованию системы можно получить не только экономию бюджета, но и доработку методик, пересмотр и поиск аналогичных ошибок, обучение сотрудников и т.д. — т.е. комплекс мероприятий, после которого такая ошибка не должна повториться.

Таким образом, есть все основания полагать, что такая интегрированная СУЗПДн:

• окажется экономически выгодной, за счет снижения совокупной стоимости владения (ТСО) СУЗПДн и повышения отношения чистой приведенной выгоды к совокупным расходам (т.н. возврат на инвестиции — ROI);

• должна обеспечить соответствие требованиям 152-ФЗ с течением времени, в том числе и после внесения изменений в его подзаконные акты.

Системы защиты персональных данных

Статья посвящена актуальному вопросу защиты персональных данных в преддверии вступления в силу ФЗ №152. Автор анализирует причины необходимости защиты данных такого рода, приводит классификацию типовых утечек информации. Особое место в статье отводится обзору технологии DLP (Data Loss Prevention), направленных на защиту критичных данных. Подробно раскрыты подходы, которые используют разработчики при создании DLP систем, а также ключевые проблемы, с которыми приходится сталкиваться при их внедрении.

Ключевые слова:
Защита персональных данных, утечка информации, технология DLP, информационная безопасность

Алексей Чередниченко,
ведущий специалист McAfee в России и СНГ,
Alexey_Cherednichenko@McAfee.com

2009 г. прошел на российском рынке информационной безопасности под знаком закона о персональных данных. Согласно его положений все организации, так или иначе использующие персональные данные (см. врезку) обязаны привести свои процессы их обработки и хранения в соответствие с требованиями закона к январю 2010 г. Это в равной степени касается процедур проверки и фиксирования данных удостоверения личности посетителей бизнес-центров, и процедур хранения и анализа баз данных о клиентах оператора сотовой связи. Одним из наиболее дискуссионных аспектов новых требований к процедурам стал вопрос о надлежащей защите персональных данных в распоряжении компании.

Корпоративные ИТ-службы, команды IT-специалистов системных интеграторов и компаний-вендоров решений информационной безопасности приложили массу усилий к созданию и внедрению систем управления и защиты персональных данных, однако в течение года мы видели не так уж и много успешных кейсов. На момент написания статьи, окончательное решение о переносе сроков вступления в силу положений о санкциях против компаний-нарушителей еще не принято. Однако очевидно, что 2011 г. также будет годом внедрения систем защиты данных.

Необходимость качественной защиты такого рода информации очевидна. Любая комбинация данных о прописке, страховке, семейном положении в руках мошенника напрямую угрожает вашей личной безопасности человека. И сегодня такие данные более чем доступны. Достаточно просто посетить любой крупный компьютерный рынок или электронный торговый центр. Конечно, диски с базами не стоят на прилавках, вместе с популярным программным обеспечением и новыми играми, но, как правило, после нескольких правильно заданных вопросов за 2-3 тыс. руб. можно получить все необходимое. И в том числе данные о местах работы, транспортных средствах и взятых кредитах.

Доступные базы уже подготовлены для удобной работы с ними, они грамотно структурированы и имеют удобный интерфейс. Например, можно в окне поиска ввести имя и фамилию и получить полную информацию о данных паспорта, прописке, домашнем и мобильном телефоне.

Происхождение таких баз, тоже по большому счету очевидно. Практически каждый из многих миллионов россиян вольно или невольно предоставляет персональные данные о себе в государственные структуры и частные компании, которые уверяют нас в полной конфиденциальности предоставленных данных. На деле же очень часто базы, предназначенные исключительно для служебного пользования становятся достоянием третьих лиц, которые успешно продают их.

Для мошенников подобная информация весьма ценна, фактически им в руки дан список потенциальных жертв на выбор, с адресами и номерами телефонов. В лучшем случае вас могут досаждать назойливые продавцы различных товаров "первой" необходимости. В худшем вас могут начать шантажировать или банально ограбить. На ваше имя могут зарегистрировать предприятие и совершать через него мошеннические действия, причем по российскому законодательству вы окажетесь не пострадавшим, а соучастником преступлений, опровергнуть это бывает чрезвычайно сложно.

Впрочем, эта проблема отнюдь не "российская специфика". Проблема утечки, хищения и злоупотребления конфиденциаль-

"Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация" (Федеральный закон РФ №156, статья 3).

"Персональные данные означают любую информацию об определенном или поддающемся определению физическом лице (субъект данных)" (Федеральный закон РФ №160).

ными персональными данными в странах с развитыми ИТ и финансовыми процессами стала настолько актуальной, что в результате появилась отдельная прикладная область информационной безопасности, которая была названа DLP (Data Loss/Leakage Prevention) или предотвращение утечек информации. Она вызвала бурное развитие сегмента рынка продуктов и услуг в области борьбы с утечками и обеспечения безопасности критичных данных. К этому необходимо добавить сопутствующие продукты рынка, такие как обучение и сертификация.

До недавнего времени в России, к сожалению, уделялось крайне недостаточное внимание данной проблеме. Поэтому сегодня даже у специалистов еще нет достаточно глубокого понимания средств информационной безопасности, построения правильных процессов обеспечения защиты критичных данных.

Классификация утечек.

Концептуально существует два канала утечки данных в информационных сетях; это сеть передачи данных и, мобильные устройства, к ним же следует относить и мобильные носители данных. Далее можно продолжать деление на типы сетей и устройств, но это уже подробности в которые мы вдаваться не будем.

По причинам утечки можно условно разделить на внутренние и внешние. К внешним утечка относят, например, успешную DDoS атаку с дальнейшим проникновением внутрь периметра корпоративной безопасности и получением доступа к искомым данным. К внутренним утечкам, а именно к ним относится на сегодняшний день более 90% всех утечек данных, относятся ситуации с умышленными или неумышленными действиями сотрудников компаний и организаций, в результате которых конфиденциальность данных была нарушена. В качестве примера неумышленной компрометации можно назвать, наиболее часто встречающуюся ошибочную отсылку конфиденциальной информации по электронной почте. Что же касается сознательного хищения данных, это куда более сложные и интересные с точки зрения ИБ-специалиста случаи, требующие значительно большей экспертизы, опыта, да и инженерной смекалки.

Как уже было отмечено данное деление условное, так как в последнее время наблюдаются смешанные причины утечек. Примером может служить внедрение "троянской" программы используя уязвимости web-браузеров и социальный инжиниринг в спамовых рассылках. Данные письма имеют ссылки на зараженный web-сайт, с которого и производится загрузка данного вредоносного ПО, которое уже осуществляет непосредственно хищение данных.

Подходы к созданию DLP систем.

К сожалению, защитить критичные данные, в том числе и персональные данные клиентов и контрагентов, на 100% не сможет ни одна компания. Нынешнее развитие технологий DLP позволяет лишь минимизировать риски.

Один из подходов, используемый в DLP — анализ контента. Данный принцип не зависит от специфики канала утечек, и основан на анализе содержимого файлов или потоков при передаче их по сети или при операциях сохранения, копирования или переносе на различные носители информации. Целью данного анализа является локализация конфиденциальных данных и предотвращение их нелегального выхода за периметр безопасности. Тут следует пояснить, что периметр безопасности и "стены офиса" далеко не всегда обозначают одно и то же. Так, данные на корпоративном ноутбуке даже вне пределов корпоративной сети могут быть надежно защищены средствами шифрования и политиками безопасности, за соблюдением которых следит установленная на ноутбуке программа-агент.

Определение конфиденциального содержимого производится, как правило, по списку ключевых слов, составляющих основу конфиденциальной информации. Различные производители по разному подходят к этому вопросу и реализуют эти механизмы на основе алгоритмов фильтрации контента, либо контекстной фильтрации. Эти методы использовались как основные в первых версиях систем DLP. Но все они имеют несколько недостатков, в числе которых сравнительно низкая скорость работы и сравнительно низкая точность определения. Кроме этого, система фильтрации контента допускает ошибки ложного срабатывания, определяя открытые данные как конфиденциальные.

Более совершенная система основана на принципе "грифования" электронных документов, названная так по аналогии с тем, как грифуются бумажные документы. Технически это реализовано в виде пометки файлов. Многие системы грифуют данные, вводя специальный тег в имя файла. Однако такой способ значительно ограничивает работу с документами и оставляет лазейки для злоумышленника.

Наиболее эффективной оказалась техника установки метки внутрь файла, скажем в виде служебного заголовка. Применяя такой подход в качестве основного, удалось резко повысить скорость и точность определения конфиденциальных документов. Когда такой документ пытается покинуть корпоративную сеть, или, например, записаться на сменный носитель, контролирующему модулю не нужно анализировать содержимое. Достаточно лишь считать гриф и применить соответствующие правила политики безопасности. Зная метку, защитный механизм может теперь безошибочно определить, является файл секретным или нет.

Очевидно, что для использования подхода грифования требуется провести полный анализ и классификацию всех электронных документов в организации и пометить все секретные файлы соответствующим образом. Главным недостатком таких методов является то, что пометить все конфиденциальные документы, как правило, очень сложно. Еще труднее постоянно поддерживать базу данных грифованных документов. Чтобы решить эту проблему, к примеру, продукт компании McAfee переносит грифы в новые файлы из старых документов при их трансформации и таким образом существенно упрощает процесс.

Оптимальным же сегодня является метод комбинации описанных выше подходов. Так McAfee, используя анализ контента при со-

Одна из сложностей, с которыми столкнулась отрасль информационной безопасности в 2009, это "преднамеренное заблуждение" относительно систем и решений, внедрение которых требует закон о персональных данных. Многие производители легко манипулируют им. Например, DLP-системой можно легко назвать антивирус, поскольку он позволяет избежать "троянов", которые отсылают информацию своим заказчикам, и программу для контроля устройств в операционной системе, поскольку она борется с утечками через мобильные устройства и накопители. Однако и антивирус, и система контроля устройств закрывают лишь один из каналов утечек.

здании документов и в процессе их грифования, в дальнейшем контролирует процесс по созданным меткам, добилась высокой скорости, точности определения и низких показателей ложного срабатывания, а также возможности гибко и легко управлять своей платформой DLP.

Однако простая интеграция подходов не может быть основанием для появления очередного поколения продуктов. Развитие отрасли показало, что концептуально новые DLP-системы должны поддерживать функционал шифрования для защиты информации на мобильных носителях и устройствах. Эксперты утверждают, что практически половина современных утечек происходит в результате кражи мобильных устройств. В этом случае единственным эффективным способом защиты является шифрование данных. В состав продукта от McAfee, специально входит как опция, средство шифрования данных "Safe Boot", которое позволяет надежно защитить данные на дисках мобильных устройств — ноутбук, КПК, смартфонов, сменных носителей.

Итак, практически идеальным средством защиты персональных и конфиденциальных данных в условиях реальной действительности может быть решение, которое комбинирует основные подходы к анализу и контролю контента, позволяет устранить утечки по классическим каналам, а также минимизировать ущерб от украденных мобильных устройств за счет шифрования дисков. В таком решении должна присутствовать централизованная система аудита и доказательная база всех действий с конфиденциальными документами. Кроме того, решение должно учитывать специфику организаций и быть подстроено под основные бизнес-процессы организаций.

Внедрение систем предотвращения утечек данных.

Ключевой проблемой при внедрении систем DLP, стало то, что к моменту начала внедрения системы компания заказчик уже должна иметь четкое и ясное представление о том, какие конфиденциальные данные находятся в ее распоряжении, как и где они хранятся, какие действия с ними производятся. То есть, еще до начала внедрения, в рамках проекта необходимо провести тщательный аудит; и большинство компаний-внедренцев предлагают этот подготовительный этап проводить заказчику своими силами, который, очевидно, просто не готов и не способен провести аудит необходимого качества.

В некоторых организациях, государственных и коммерческих, не один год может уйти на поиск ответов на эти ключевые для успешного внедрения вопросы. Более 70% организаций вообще не представляют, какие данные следует отнести к категории критичных.

В этом случае очень может помочь применение продукта DLP, который имеет функциональность при задании правильного классификатора данных по степени их конфиденциальности и определении четких критериев идентификации этих данных, позволит автоматически произвести процедуру анализа всех данных и действий над ними.

Обладающий такой функциональностью продукт позволит сильно сократить и упростить процесс внедрения технологии защиты от утечек

Несмотря на все усилия, сегодня большинство компаний все же не готовы защищать имеющиеся в их распоряжении данные так хорошо, как того требует 152-й федеральный закон. Но в данной ситуации есть и позитивные стороны. Так, на нашем рынке информационной безопасности существует большое число опытных игроков, которые рассматривают формирующуюся нишу как стратегически важное направление развития своих компаний. Исходя из многолетнего опыта и проводя непрерывные консультации с ответственными за развитие этого направления государственными структурами компании-интеграторы, без сомнения, внесут свою лепту "первопроходцев" и смогут достаточно быстро заполнить недостающие пробелы.

Кроме того, 2009 г. не прошел зря: множество белых пятен и узких мест было выявлено на практике разработки и внедрения систем, многие системные противоречия были разрешены, а вендоры готовят новые продукты, более заточенные под поставленные задачи.

McAfee предупреждает о наступлении эпохи кибернетических войн

McAfee, Inc. опубликовала свой пятый ежегодный "Отчет о виртуальной преступности", согласно которому международная гонка кибервооружений стала реальностью. В ходе подготовки отчета компания обнаружила, что количество политически мотивированных кибератак выросло, а пять стран — США, Россия, Франция, Израиль и Китай — теперь обладают кибероружием. В отчете о виртуальной преступности отражены мнения более двадцати ведущих экспертов в области международных отношений, включая советника посла Великобритании в США Джеймса Сандерса, специалистов Управления национально безопасности США, Генеральной прокуратуры Австралии. За составление отчета в McAfee отвечал бывший советник президента США Пол Куртц.

В отчете впервые дано определение кибервойны, названы страны, разрабатывающие стратегии проведения атакующих и оборонительных действий в киберпространстве, рассмотрены примеры политически мотивированных кибератак и показано, что ждет частный сектор в случае кибервойны. Отдельно выделена проблема раскрытия информации о виртуальной преступности. Поскольку данные о борьбе с киберпреступностью, как правило, засекречены, государственный и частный сектор не могут разработать адекватные меры защиты.

Эксперты призывают к разработке четкого определения виртуальной войны. Без открытого обсуждения проблем киберпреступности с участием государственного и частного сектора, а также общественности, в будущем кибератаки против ключевых объектов жизнеобеспечения могут привести к огромным жертвам и разрушениям.

В отчете приводится мнение Вильяма Кроуэла, бывшего заместителя директора Управления национальной безопасности США. "В течение следующих 20-30 лет кибератаки станут неотъемлемой частью военной стратегии. Остается только неясным, будут ли компьютерные сети настолько вездесущими и незащищенными, что военные действия полностью переместятся в виртуальное пространство", — заявил он.

Ознакомиться с отчетом McAfee о виртуальной преступности 2009 можно по адресу http://www.mcafee.com.

Дополнительную информацию о результатах исследования и мнениях экспертов, можно прочитать в блоге McAfee Security Insights http://siblog.mcafee.com.

Системы охранного видеонаблюдения на базе IP для обеспечения безопасности здания

Ключевые слова:
Охранное видеонаблюдение, безопасность здания, аутентификация, авторизация

В статье приводятся описания методов и инструментов для создания защищенной системы охранного видеонаблюдения на базе IP.

Станислав Гучия,
Генеральный директор
ООО "Аксис Коммуникейшнс"

Действительно ли охранное видеонаблюдение на базе IP обеспечивает должную безопасность? Этот вопрос часто задают клиенты, перед которыми встает вопрос выбора системы охранного видеонаблюдения. Охранное видеонаблюдение на базе IP обладает многими преимуществами по сравнению с аналоговыми системами, с другой стороны, многие опасаются, что они подвержены риску атаки хакеров. Подобные опасения вызваны по большей части газетными статьями, где описывается, как легко получить несанкционированный доступ к охранной системе.

Во-первых, система на базе IP может быть настолько открытой или защищенной, насколько вы сами этого хотите. Многие пользователи хотят иметь открытый доступ к изображению в режиме реального времени, чтобы распространять эту информацию среди членов семьи, друзей, а также в рекламных веб-приложениях. Однако охранные системы необходимо защищать от несанкционированного доступа как извне, так и изнутри.

Использование стандартной сетевой инфраструктуры для системы охранного видеонаблюдения, несомненно, имеет множество преимуществ. Прежде всего, установка и обслуживание становятся менее затратными, поскольку общая инфраструктура может использоваться несколькими различными системами, в том числе и IP-сетью для голосового оповещения (VoIP), системой управления зданием и т. д. У видеосистем на базе IP нет ограничений по разрешению и частоте кадров, которые присущи аналоговым системам.

Уровни безопасности

Сетевая безопасность осуществляется на трех уровнях. Необходимо начать с определения требуемой степени безопасности системы, а также того, кто будет ей пользоваться, и какова вероятность получения несанкционированного доступа. На основе этой информации можно принимать физические меры по обеспечению безопасности. Самое главное — постоянно контролировать эффект принятых мер. Одно из недооцененных достоинств систем охранного видеонаблюдения на базе IP состоит в том, что они используют уже существующие технологии. Эти технологии нехарактерны для видео, потребовались годы развития, чтобы доказать, что они действительно работают.

Создание безопасной системы охранного видеонаблюдения на базе IP напоминает охрану дома. В доме есть двери с замками. Когда вы уходите из дома, то тщательно запираете окна и двери, чтобы в него не пробрались воры. Если в доме есть ценные вещи, вы устанавливаете сигнализацию. Защита видеосистемы работает точно так же. Обычной камере, расположенной на виду и показывающей окружающие красоты и погоду, не нужны специальные меры защиты. Достаточно установки пароля для раздела администрирования камеры. Охранное видеонаблюдение с использованием корпоративной сети требует дополнительных мер безопасности. А системы охранного видеонаблюдения в зонах особой важности требуют усиленных мер, таких как аутентификация сетевого устройства, предотвращающая возможность использования другого источника. Трафик данных необходимо шифровать, чтобы посторонние лица не могли прочитать и использовать информацию. Любые манипуляции в сетевой инфраструктуре приведут к включению сигнала тревоги и отключению части оборудования.

Аутентификация и авторизация: кто вы и есть ли у вас разрешение здесь находиться?

Безопасная передача данных означает не только обеспечение защиты внутри сети, но также и между различными сетями и клиентами. Эффективные решения должны контролировать все, начиная от данных, отправленных через сеть, и заканчивая определением личности, использующей канал и получающей к ней доступ. Они должны не только идентифицировать и авторизовать источник сообщения, но также и гарантировать конфиденциальность передачи данных во время ее прохождения по сети.

Во время первого этапа необходима идентификация пользователя или устройства в сети и на удаленной конечной точке-получателе. Существует несколько способов идентификации в сети или системе. Наиболее типичным является имя пользователя и пароль. После окончания идентификации необходимо проверить, имеет ли пользователь или устройство разрешение на запрашиваемые действия. После подтверждения этого права пользователь получает полное соединение и возможность передачи данных.

Представляя собой базовую защиту, эта технология хорошо подходит для систем, которым не требуется высокая степень безопасности, а также в случаях, когда видеосеть отделена от основной сети в целях предотвращения к ней физического доступа для авторизованных пользователей.

Конфиденциальность: можете ли вы скрыть передачу данных от посторонних?

Второй этап включает в себя шифрование данных, чтобы во время передачи по сети никто не мог прочитать их или использовать. Существует несколько различных технологий, которые могут использовать интеграторы. Рассмотрим четыре из них:

- фильтрация IP-адресов;
- виртуальная частная сеть;
- протокол HTTPS;
- стандарт 802.1X.

Ограничивающий брандмауэр: фильтрация IP-адресов

Некоторые сетевые камеры и видеокодеры используют фильтрацию IP-адресов, чтобы предотвратить доступ к компонентам сетевого видео со всех IP-адресов, кроме одного или нескольких. Фильтрация IP-адресов по своему действию напоминает встроенный брандмауэр.

Эта технология подходит для систем, требующих более высокого уровня безопасности. Как правило, сетевую камеру требуется настроить таким образом, чтобы она принимала команды только с IP-адреса или сервера, на котором установлено ПО для управления видео.

Безопасный маршрут: виртуальная частная сеть

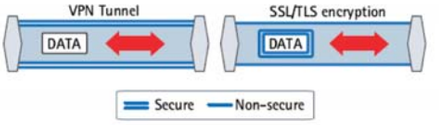
Еще более безопасная альтернатива — это виртуальная частная сеть (VPN), использующая протокол шифрования для обеспечения безопасного тоннеля между сетями, по которому данные могут передаваться незаметно для посторонних наблюдателей. Это позволяет безопасно передавать данные через общую сеть, например Интернет, потому что только устройства с правильным "ключом" могут работать в самой сети VPN.

VPN, как правило, зашифровывает пакеты на уровнях IP или TCP/UDP и выше. Протокол защиты IPSec является наиболее часто используемым протоколом шифрования в сети VPN. В протоколе IPSec используются различные алгоритмы шифрования: стандарт тройного шифрования данных (3DES) или стандарт усовершенствованного шифрования (AES). Стандарт AES, использующий 128- и 256-битные ключи, обеспечивает более высокую степень безопасности и требует заметно меньше мощности компьютера для шифрования и расшифровки данных, чем стандарт 3DES.

Сети VPN часто используются в разных офисах в пределах одной организации или работающими удаленно сотрудниками, имеющими доступ к сети. Удаленные камеры образуют корпоративную систему охранного видеонаблюдения подобным образом.

Шифрование данных: протокол HTTPS

Еще более высокого уровня конфиденциальности можно достигнуть с помощью шифрования данных. Протокол защиты HTTPS — это наиболее часто употребляемый протокол шифрования данных, использующийся, к примеру, в приложениях для банковских операций, осуществляемых через Интернет, для обеспечения безопасности при финансовых транзакциях. Протокол HTTPS отличается от HTTP только одной ключевой особенностью: шифрование передаваемых данных осуществляется с помощью протокола безопасных соединений (SSL) или протокола защиты транспортного уровня (TLS).

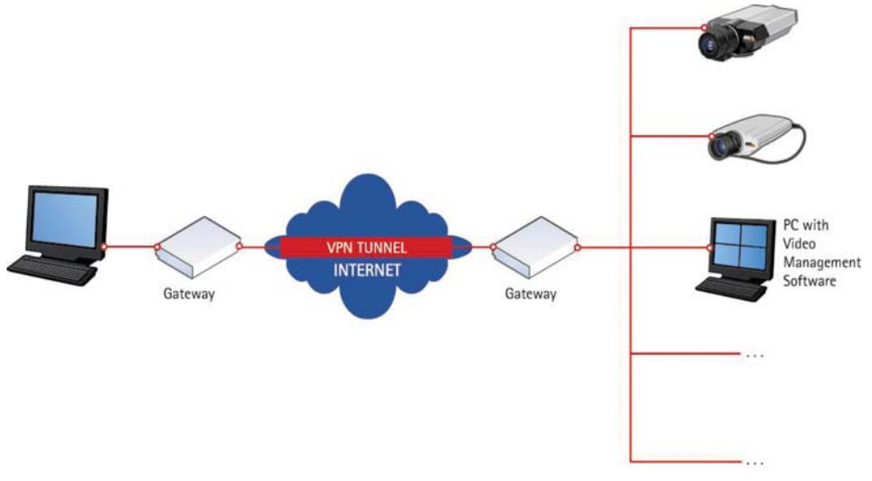


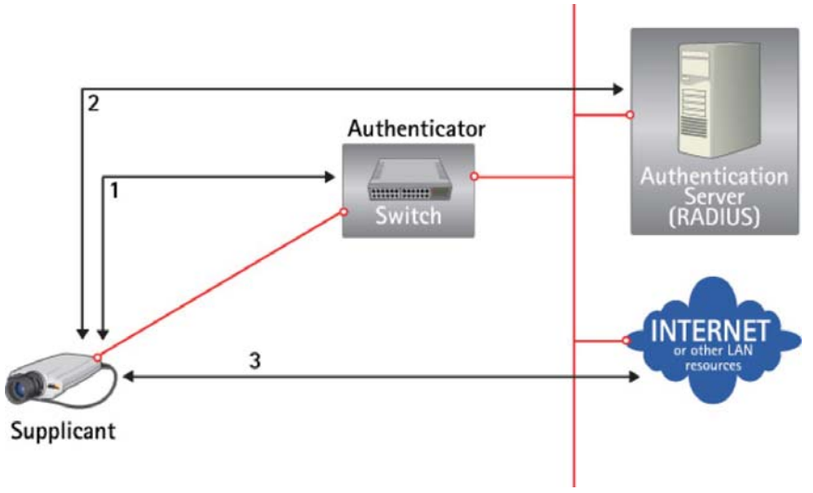
Протокол SSL разработан компанией Netscape и выпущен в 1994 г. Безопасность, обеспечиваемая протоколами SSL/TLS, основана на трех основных элементах: 1) аутентификация партнера по обмену данными, 2) симметричное шифрование данных, 3) защита от манипуляций с передаваемыми данными.

При осуществлении соединения SSL/TLS протокол приветствия определяет, какие методы шифрования должны быть использованы получателем и отправителем: алгоритмы шифрования, основные настройки, генерация случайных чисел и т. д. Затем протокол подтверждает идентификационные данные партнера методом использования сертификата веб-сервера для идентификации в веб-браузере. Сертификат представляет собой нечто вроде удостоверения личности, которое используют люди. Это документ в двоичном формате, который центр сертификации часто выпускает как идентификационный знак (Verisign). Пользователи также могут выпускать собственные сертификаты для закрытых групп, таких как web-сервер локальной сети, к которому имеют доступ только сотрудники компании.

На следующем этапе партнеры по обмену данными обмениваются предварительным кодом, который зашифрован перед передачей на сервер с помощью общего ключа, полученного в виде сертификата ключа от сервера (метод ассиметричного шифрования) или обмениваются ключами Диффи-Хеллмана. Обе стороны вычисляют главный код локально и на его основе создают сеансовый ключ. Если сервер может расшифровать эти данные и завершить протокол, клиент может быть уверен, что на сервере правильный частный ключ. Этот этап является самым важным в процессе аутентификации сервера. Только сервер с частным ключом, соответствующим общему ключу в сертификате, может расшифровать эти данные и продолжить согласование протокола.

Многие продукты сетевого видео имеют





встроенную поддержку протокола HTTPS, которая позволяет безопасно просматривать видеоизображение через web-браузер.

Защита от хищения данных для сетевых портов: стандарт 802.1X

Одним из наиболее популярных и безопасных методов аутентификации для беспроводных сетей является стандарт IEEE 802.1X. С его помощью осуществляется аутентификация устройств, подсоединенных к портам сети LAN, установка соединения типа "точка-точка" или предотвращение доступа с порта в случае неудачной аутентификации. Стандарт 802.1X часто называют контролем доступа к сети на базе портов, потому что он позволяет предотвратить хищение данных, когда неавторизованный компьютер получает доступ к сети в результате подсоединения к сетевому разъему внутри или вне здания.

В стандарте 802.1X предусмотрена аутентификация на трех уровнях: запрашивающий, аутентификатор и аутентификационный сервер. Запрашивающий сообщает устройству сети, например, сетевой камере, что ему необходим доступ к сети. Аутентификатором может выступать коммутатор или точка доступа. Последовательные порты аутентификатора разрешают передачу видеоданных от запрашивающего устройства после его идентификации. Аутентификационный сервер обычно представляет собой специализированный сервер в локальной сети LAN, перед которым в процессе аутентификации другие серверы должны быть идентифицированы.

Аутентификационный сервер, например, Microsoft Internet Authentication Service, называется службой дистанционной аутентификации пользователей по коммутируемым линиям (RADIUS). Если устройству необходимо получить доступ к сети, оно запрашивает разрешение на доступ через аутентификатор, которые перенаправляет все запросы в очередь на аутентификационный сервер. Если аутентификация осуществляется успешно, сервер отправляет аутентификатору команду авторизовать доступ к сети для ожидающего сервера.

Поддержку стандарта 802.1X часто встраивают в сетевые камеры и видеокодеры. Она очень полезна в случаях, когда сетевые камеры расположены в общественных местах, таких как приемные, коридоры, комнаты переговоров, или даже вне помещений. Без поддержки стандарта 802.1X риск повреждения сетевого разъема, находящегося в легкодоступном месте, очень высок. В современных корпоративных сетях, где внутренние пользователи и внешние партнеры постоянно получают доступ к данным, поддержка стандарта 802.1X становится основным требованием для любых компонентов, подключаемых к сети.

Стандарт 802.1X обеспечивает безопасность на базе портов, при этом в процессе участвуют запрашивающее устройство (например, сетевая камера), аутентификатор (например, коммутатор) и аутентификационный сервер.

Лучшие показатели

Защита системы сетевого видео — это непрерывный процесс, требующий постоянного внимания. Этот процесс начинается уже в фазе разработки проекта. Используйте следующую контрольную таблицу для оценки безопасности системы.

- Определили ли вы, кто и как будет использовать систему? Вам необходимо определить роли администратора, оператора и наблюдателя.
- Определили ли вы, что происходит с хранящимся в архиве материалом? Как долго вы хотите хранить видеоматериалы, и кто будет иметь доступ к записям?
- Проверили ли вы физическую безопасность установки? Кабели и сетевое оборудование необходимо тщательно защитить.
- Есть ли у вас способ проверки безопасности системы на месте через определенные промежутки времени? Удостоверьтесь в том, что определенные вами процессы действуют, и система исправно работает.
- Определили ли вы и приняли ли меры для безопасности сети? В их число входит программное и аппаратное обеспечение, такое как брандмауэры.

Необходимо время от времени осуществлять проверку всех важных позиций перед запуском системы.

Какой тип защиты вам подходит?

Система сетевого видео может быть гораздо более безопасна, чем аналоговая система. Вы можете отключать ее от Интернета и корпоративной сети и использовать шифрование данных для каждой камеры. Но часто бывает выгодно объединять работу системы сетевого видео с операциями в корпоративной сети и доступом к видео из удаленных мест через Интернет.

Нет однозначного ответа по поводу того, какая степень защиты вам необходима. Все зависит от среды, сценария использования и ценности передаваемых данных. Это очень похоже на выбор защиты для здания. Можно использовать один замок или несколько. Если риск взлома в районе велик и в здании хранятся ценные вещи, то можно установить решетки на окна, сигнализацию, соорудить забор и даже поставить охранников.

Прежде чем принять какое-либо решение, нужно тщательно оценить потенциальные опасности и определить, какая технология защиты наиболее соответствует вашим условиям.

Устройства для решения задач современного общества

Ключевые слова:
Цифро-аналоговые устройства, идентификационные технологии, биометрическая идентификация

Примеры решений на основе высокопроизводительных цифро-аналоговых устройств (high-performance mixed signal, HPMS), разработанных NXP совместно с партнерами по НИОКР в рамках инновационного подхода под названием "More-than-Moore" ("за пределами закона Мура").

Для NXP "More-than-Moore" — это приоритет функциональности устройств над исключительно высокой производительностью. Подход "More-than-Moore" позволяет компании внести свой вклад в решение таких социально-важных проблем как энергосбережение, контроль загрузки автодорог, старение населения и др.

Анализируя факторы развития общества и индустрии полупроводников, NXP Semiconductors обозначила новую корпоративную стратегию — производство высокопроизводительных цифро-аналоговых устройств.

Примеры таких разработок компания впервые представила российскому потребителю на выставке "Инновации и технологии 2009". Были представлены: автомобильная бортовая телематическая платформа ATOP, решения в области идентификации на основе технологии NFC, интеллектуальный счетчик электроэнергии, микросхема для управления напряжением в энергосберегающих лампах, слуховой аппарат с рекордно низким энергопотреблением.

Эти разработки отличает высокая функциональность и энергоэффективность, при этом они удобны в использовании и позволяют сокращать расходы на медицинское обслуживание, транспорт и коммунальные услуги, а также значительно экономить время, необходимое для проведения платежей или затрачиваемое в длительных дорожных пробках.

Стенд NXP Semiconductors посетил Председатель Государственной Думы Федерального Собрания РФ, руководитель фракции "Единая Россия" Борис Грызлов.

Автомобильная бортовая телематическая платформа ATOP (Automotive telematics onboard-unit platform)

Готовое решение, оптимизированное по стоимости, энергопотреблению и габаритам (корпус BGA размером 33x33 мм и высотой 3 мм), Устройство объединяет в себе модули GSM/GPRS, GPS, память SRAM и Flash, микроконтроллер ARM с интерфейсами CAN, USB и другими, контроллер безопасности данных SmartMX, обеспечивающий защиту на уровне банковских стандартов, и RFID (NFC) интерфейс. Устройство обеспечивает возможность реализации целого комплекса задач: дорожные платежи, экстренный вызов (eCall), управление и мониторинг транспорта и т.д.

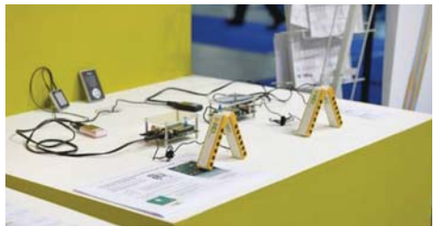
Интеллектуальный счетчик электроэнергии

Решение демонстрирует доступность информации о потреблении электричества потребителю и ведет к снижению энергопотребления. Мониторинг потребления электроэнергии позволяет проводить мгновенное отслеживание пиковых нагрузок, что предотвращает отключения. Снятие информации реализовано по проводным (CAN, PLC, RS485, Ethernet) и беспроводным (RF, ZigBee, Bluetooth) каналам. Благодаря высокотехнологичным компонентам обеспечивается снижение энергопотребления самого счетчика как устройства при одновременном увеличении вычислительной мощности.

Система управления LED-освещением

LED-светильники позволяют экономить до 80% электроэнергии по сравнению с обычными лампами накаливания. Решение позволяет плавно управлять светом без мерцания и шумов. Схема содержит встроенный модуль, позволяющий работать с недорогими TRIAC диммерами. В основе схемы лежит микросхема SSL2102, ее схемотехника дает возможность реализации различных видов подключения: изолированный, неизолированный, повышающий, понижающий.

Устройства с ультранизким энергопотреблением — слуховые аппараты



Представлена реализация слухового аппарата на основе уникального беспроводного энергоэффективного решения NXP, разработанного с использованием радиотехнологии магнитной индукции (пропускная способность 300 кбит/с). Беспроводное решение с минимальным количеством внешних компонентов реализовано в виде микросхемы с шариковыми выводами. Технология NXP Coolflux™ DSP используется в радио на основе магнитной индукции в качестве программируемого ядра. Непосредственно демонстрируется улучшение качества звука при беспроводной передаче между правым и левым устройством.

"Умный" автомобильный ключ

Ключ от автомобиля, кроме стандартного функционала (центральный замок, иммобилайзер ит.д.), также обеспечивает связь с мобильным устройством через интерфейс NFC, что позволяет использовать мобильный телефон (с поддержкой NFC) для отображения более подробной информации о статусе и местоположении автомобиля. Данный ключ можно использовать для осуществления бесконтактных платежей (в частности, безналичная оплата на парковках, в ресторанах быстрого питания, платных автодорогах, метро).

Биометрическая идентификация

Концепция для использования в системах контроля доступа демонстрирует возможность идентификации отпечатка пальца путем сравнения конфиденциальной информации (отпечаток пальца) в безопасном устройстве — непосредственно внутри карты на базе микросхемы семейства SmartMX, без необходимости обращения в специальные процессинговые центры. Это позволяет избежать значительных затрат по построению высокозащищенной инфраструктуры хранения и обработки конфиденциальных данных и проводить сравнение отпечатков пальцев непосредственно на карте владельца.

Платформа STB225 для телевидения высокой четкости

Полупроводниковая платформа STB225 для телевидения высокой четкости (ТВЧ) с реализованным функционалом PVR LAN/USB, Time Shift и Media Player. На базе данного решения отечественные производители цифровых приставок получают уникальную возможность в сжатые сроки запустить массовое производство оптимизированного по цене MPEG4 HD изделия с богатым функционалом, который реализован на уровне ПО при активном участии российских разработчиков.

Начинает работу европейский исследовательский проект "BioP@ss", нацеленный на повышение безопасности чиповых карт для создания общеевропейских электронных ID-карт

Производители микросхем Infineon Technologies AG и NXP Semiconductors Germany GmbH (NXP), а также производитель чиповых карт компания Giesecke & Devrient GmbH (G&D) вошли в состав 11 компаний из 6 стран ЕС, которые приняли участие в европейском исследовательском проекте по разработке платформы чиповых карт с высокой степенью защиты BioP@ss.

BioP@ss — крупнейший в Европе исследовательский проект в области чиповых карт. Его целью является проведение технических изысканий для введения в действие электронных идентификационных карт в виде карточек со встроенной микросхемой, действительных во всех странах ЕС. Помимо выполнения функции идентификационной карты, это решение будет являться безопасным средством аутентификации для услуг, предоставляемых правительствами или общественными организациями, а держатели карт BioP@ss смогут электронным образом подтвердить свою личность и проводить биометрическую аутентификацию в сети Интернет. В 27 странах Европейского Содружества проживает около 500 млн. граждан, и около 380 млн. ID-карт находятся в обращении в настоящее время.

Целью проекта является обеспечение еще большей безопасности и простоты использования чиповых карт, чтобы граждане ЕС могли пользоваться сервисами, предусмотренными правительством и общественными организациями, с помощью своих ID-карт через Интернет. Такими сервисами являются, например, регистрация изменения адреса, регистрация автомобилей, заполнение налоговых деклараций (электронное правительство), голосование на выборах (электронное голосование) и другие услуги, предоставляемые в области розничных продаж, сфере страхования и банковском секторе (электронный бизнес). Исследовательский проект BioP@ss призван стимулировать дальнейшую разработку микросхем с высокой степенью защиты, операционных систем для смарт-карт и защищенного программного обеспечения для персональных компьютеров, подключенных к сети Интернет, которыми пользуются как обычные граждане, так и общественные организации. Задачей проекта является обеспечение поддержки разнообразных стандартов, используемых в национальных идентификационных документах, уже существующих в странах ЕС, на уровне микросхем, операционных систем и программного обеспечения. Одним из примеров стандарта такого ID-документа является стандарт карты гражданина ЕС (European Citizen Card), который разработан для граждан ЕС для подачи налоговых деклараций из любой точки Европы. Эта карта позволяет проводить электронную идентификацию, аутентификацию и использовать электронную подпись в Интернет.

В качестве участников проекта BioP@ss, компании — производители компонентов Infineon и NXP работают над усовершенствованием технологии шифрования для микросхем. Другим направлением работы является повышение скорости обмена данными между картой и считывателем. Компания G&D занимается разработкой инновационной операционной системы для карты, которая с помощью протоколов согласования Интернет (TCP/IP, HTTP, TLS и SOAP) позволит использовать чиповые карты с Интернет-ПК без необходимости установки дополнительных программных компонентов. Соединение между картой и ПК может быть установлено как бесконтактным способом, так и через USB-интерфейс.

Ряд европейских государств — Болгария, Чешская Республика, Франция, Германия, Румыния, Швейцария и Великобритания — уже объявили о своем намерении в течение последующих нескольких лет внедрить электронные ID-карты, соответствующие международным стандартам.

Бюджет исследовательского проекта BioP@ss, завершение которого планируется к концу июня 2011 г., составляет около 13 млн. евро, и половина всех средств предоставлена бизнес- и отраслевыми партнерами-участниками проекта. Вторая половина обеспечена европейскими фондами кластеров EUREKA CATRENE/MEDEA+, которые предоставлены национальными правительствами. В рамках стратегии развития высоких технологий Федерального Правительства Германии и инвестиционной программы "Informations- und Kommunikationstechnologie 2020 (IKT 2020)", Министерство Образования и Исследований Германии (BMBF) предоставило поддержку проекту BioP@ss в размере 2,8 млн. евро. Одной из задач программы IKT 2020 является укрепление технологического лидерства Германии в области информационных и коммуникационных технологий. Поддержка проекта BioP@ass поможет дальнейшему выходу чиповой карты, разработанной при участии Германии, на международный рынок.

Информацию о проекте BioP@ss и его партнерах можно получить на сайте www.biopass.eu

Анализ параметров сигналов, воспроизводимых с карт с магнитной полосой

Инфраструктура систем безналичных расчетов, использующих карты с магнитной полосой, продолжает доминировать над комплексами, ориентированными на применение более перспективных контактных и бесконтактных электронных карт. При эксплуатации систем с магнитными картами возникает ряд проблем, например в цифровых сигналах, считываемых с магнитной полосы карт, из-за явления неконтакта с ней блока магнитных головок, могут возникнуть ошибки. Это связано с тем, что воспроизводимые сигналы подвергаются достаточно глубокой паразитной амплитудной модуляции, влияющей на процессы порогового формирования в тракте записи-воспроизведения. По этой причине актуально исследование характеристик сигналов, получаемых с магнитной полосы карт, вводимых в эксплуатацию.

Ключевые слова:
Карты с магнитной полосой, идентификационные документы, аппарат контроля продукции, банковские карты

Зелевич Е.П.,
профессор МТУСИ
Костарев А.Н.,
соискатель МТУСИ
e-mail: oiris.mtuci@gmail.com

Носители, применяемые для точной магнитной записи не испытывают таких климатических и механических воздействий, которые возникают при использовании магнитных карт (МК), незащищенных от различных внешних воздействий. Характеристики карт с магнитной полосой определены стандартами ИСО/МЭК 7810 и 7811. Стандарт ИСО/МЭК 7810 регламентирует основные физические свойства, включая материалы, конструкцию, характеристики и номинальные размеры карт, а стандарт ИСО/МЭК 7811 устанавливает характеристики магнитной полосы карты, метод кодирования информации, формат записи данных и др. [1].

В число контролируемых параметров входят: физические характеристики магнитного материала (толщина магнитного слоя, шероховатость поверхности, профиль поверхности, сцепление магнитной полосы с картой), эксплуатационные характеристики магнитного материала (амплитуда сигнала воспроизводимого с магнитной полосы, стирание информации, плотность записи и др.) и технические характеристики кодирования информации на дорожках.

Стандарт ИСО/МЭК 7811, содержащий методику определения эксплуатационных характеристик магнитного материала карт, отсылает к образцовой эталонной карте, магнитный материал которой соответствует по своим характеристикам первичному эталону Standard Reference Material 3200 (SRM 3200). Значение коэрцитивной силы магнитного материала не регламентируется. При необходимости стандартные значения этого параметра (300...500 Э) задается фирмами изготовителями карт. Более высокие значения коэрцитивной силы магнитного материала обеспечивают повышенную стойкость к случайному стиранию информации в процессе эксплуатации. Однако это увеличивает стоимость карты и осложняет процедуру коррекции записанной информации, необходимую, например, при списывании использованного ресурса в автономных устройствах. Это связано с тем, что в этом случае следует использовать специальные блоки магнитных головок и усилители записи, развивающие большие токи [3].

Для сигналов, записываемых на магнитную полосу, используется метод двухчастотной синфазной записи, обеспечивающий последовательную запись данных с самосинхронизацией на каждой дорожке.

В состав записанной таким кодом информации входят данные и синхросигнал. Изменение потока намагниченности между перепадами синхронизации означает логическую единицу, а его отсутствие — логический ноль. Данные в виде непрерывной синхронной последовательности сигналов записываются в режиме насыщения, причем вектор намагничивания должен быть параллельным дорожке на магнитной полосе с допустимым отклонением.

На способность магнитной полосы карт хранить и воспроизводить информацию существенно влияют изменения в процессе производства. Для того чтобы гарантировать совместимость и качество, соответствующее стандарту, магнитные полосы регулярно тестируют. Оценка качества магнитных носителей по стабильности уровня воспроизводимого сигнала ведется на двух этапах: в процессе отбраковки магнитных лент, используемых для производства карт, и после их нанесения на поверхность пластиковых карт. На первом этапе производится полный контроль магнитного слоя ленты путем организации непрерывного процесса записи-воспроизведения сигнала прямоугольной формы (меандра).

Воспроизведенный сигнал оценивается пороговым формирователем. В случае занижения уровня сигнала на его входе относительно установленного порога на контролирующее устройство поступают сигналы об отбраковке того или иного участка магнитного носителя. По результатам контроля может быть принято решение о полной отбраковке всей испытуемой кассеты или части магнитной ленты.

Повторное испытания магнитного носителя производятся при персонализации карт, предполагающей воспроизведение сформированной по трем дорожкам информации и сравнение ее с исходной. В случае несовпадения результатов сравнения производится повторное воспроизведение информации и, в случае необходимости, отбраковка карты, после чего процесс повторяется для следующего образца карты.

Ввиду значимости определения соответствия параметров карт существующим требованиям, контроль эксплуатационных электромагнитных характеристик МК принятый в международной практике производится при техническом контроле качества готовой продукции на предприятии-изготовителе (выборочный контроль) и при поставках карт клиенту, например,

в банковском учреждении.

Низкий уровень выходного сигнала, размагничивание, неполное стирание сигнала, дефектный магнитный носитель и т.п. могут серьезно повлиять на надежность работы системы в процессе эксплуатации. Выпуск даже единственного пакета, средних объемов, с некачественными или бракованными картами вызовет резкое недовольство пользователей и может повлечь значительные издержки. По этой причине было бы целесообразно, при использовании МК в системах безналичных расчетов, контролировать их качество полностью, а не выборочно.

Основным показателем качества магнитного носителя является уровень сигнала воспроизводимого с карты, при заданных токах записи. Соответствие амплитуды сигнала требованиям стандарта проверяется при помощи "окна" ИСО/МЭК определяемого стандартом ИСО/МЭК 7811-2 ИСО/МЭК 7811-6.

Амплитуда сигнала, считываемого с эталонной карты, принимается за 100%. После этого рассчитывается "окно" ИСО/МЭК. При записи информации на магнитном материале с любыми защитными покрытиями номинальными токами записи с плотностью, равной 8 ипн/мм, амплитуда воспроизводимого сигнала должна лежать в пределах от 80 до 130% эталонной амплитуды.

Амплитуда воспроизводимого сигнала, полученная при указанной выше плотности записи, при токе записи, равном 500% от величины номинального значения IR, не должна превышать амплитуду сигнала, полученного при той же плотности, но при токе записи, равном 350% от величины номинального тока. Между этими двумя точками траектория кривой не должна иметь подъем.

При тех же токах записи информации, но при плотности 20 ипн/мм, амплитуда воспроизводимого с магнитной полосы сигнала не должна быть меньше 70% амплитуды сигнала, полученного при плотности записи 8 ипн/мм.

Магнитный материал карты должен обеспечивать стирание информации до уровня остаточного сигнала не более 3% эталонной амплитуды сигнала постоянным током, равным 350% номинального тока.

Главный параметр, который необходимо контролировать, — уровень воспроизводимого сигнала. Заниженный уровень воспроизводимого сигнала приводит к некорректному считыванию информации с магнитной полосы.

Полная оценка качества магнитных носителей на пластиковых картах выполняется также с учетом такого важного показателя как джиттер. Его параметры на выходе канала записи-воспроизведения, зависят как от качества магнитного носителя и его взаимодействия с блоком магнитных головок, так и от принципов построения канала записи-воспроизведения. Для контроля джиттера разработаны специализированные измерительные устройства, аналогичные используемым в системах передачи данных.

Отметим, что некоторые аппараты для считывания информации с магнитной полосы, могут работать только в условиях, когда значения джиттера лежат в определенных пределах.

Причиной неправильного считывания информации с карты также могут быть отклонения в плотности записи, приводящие к эффектам, аналогичным тем, которые характерны в случае возникновения аномально высоких значений джиттера.

Отметим, что обеспечение взаимозаменяемости магнитных носителей является одним из основных требований для любых типов ЗУ, использующих сменный носитель информации, к которым также относятся магнитные карты. Для магнитных лент эта задача решена на основе системы эталонирования, базирующейся на Главном международном эталоне магнитной ленты (ГЭЛ). Через вторичные эталоны характеристики ГЭЛ передавались контрольным лентам, с помощью которых непосредственно проверялась серийная продукция. В системе эталонирования участвовали два вида контрольно-измерительной аппаратуры: для эталонов и для контрольных лент. Такая система эталонирования позволяла "привязать" характеристики серийной продукции к характеристикам эталона для каждого производителя, гарантируя необходимый уровень взаимозаменяемости магнитных лент.

Задача обеспечения взаимозаменяемости МК во многом сложнее, чем для магнитных лент. В первую очередь она объясняется широкой номенклатурой МК и технологий их изготовления, обусловленной многообразием областей применения МК. Это делает затруднительным, а в ряде случаев невозможным, обеспечение характеристик МК с помощью одного и того же контрольно-измерительного средства, что приводит к расширению их номенклатуры. Вместе с тем, каждое из этих контрольно-измерительных средств должно быть "привязано" к международному эталону, принятому ISO, — магнитной ленте SRM 3200, что дает право производителю МК сертифицировать свою продукцию.

Аппарат контроля продукции (АКП) является малосерийной продукцией. Он должен быть автоматизирован как в смысле автоматической подачи карт (из стопки в стопку), так и в плане автоматического съема и анализа всей совокупности параметров, по которым производится отбраковка магнитной ленты с обработкой информации для набора полных статистических данных по качеству продукции. С этой целью аппарат контроля параметров МК оснащается встроенным компьютером. АКП калибруется с помощью специальных эталонной и

Рис. 1. Сигнал с выхода усилителя воспроизведения канала цифровой магнитной записи (ЦМЗ), считанный со второй дорожки банковской МК, бывшей в длительном обращении и имеющей значительную степень износа магнитной полосы

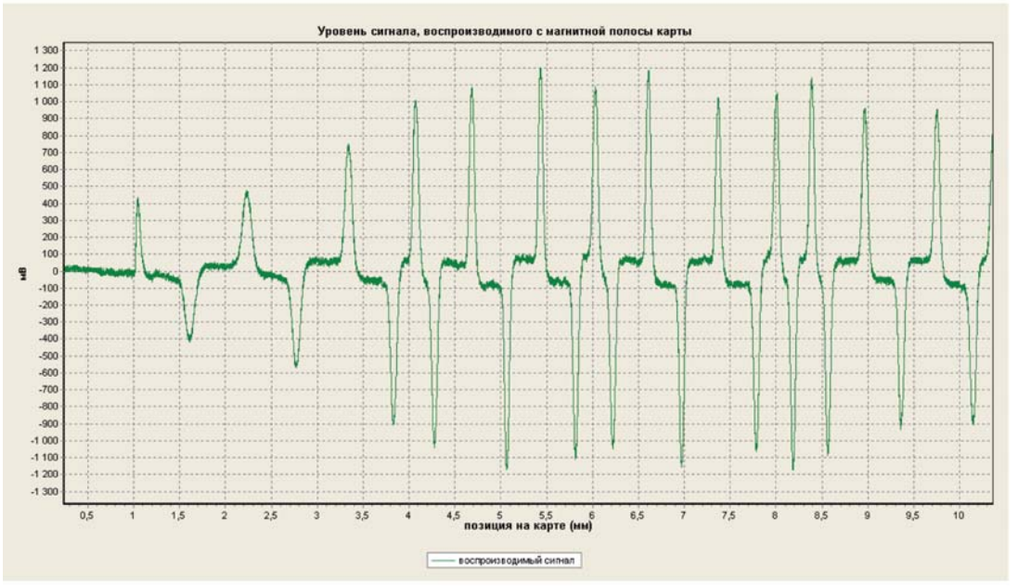


Рис. 2. Фрагмент сигнала, представленного на рисунке 1, считанный в интервале 0,5...10 мм расположенного на второй дорожке МК

контрольной карт. Узел записи-воспроизведения должен быть оснащен механизмом транспортирования карт, обеспечивающим возможность многократного провода магнитной полосы карты под блоком магнитных головок. Параметры стенда должны быть согласованы с аналогичными характеристиками оборудования для банковских операций с пластиковыми картами, такими как скорость транспортирования карт относительно блока магнитных головок, сила прижима карты к головке и т.д.

В общем случае последовательность операций, выполняемая аппаратом контроля в автоматическом режиме, следующая:

— определение вольтамперной характеристики эталонной МК при плотности записи 8 ипн/мм путем последовательной записи сигнала в виде "меандра" при разных токах записи, определение из полученных данных эталонных токов записи и эталонных амплитуд воспроизводимого сигнала, калибровку стенда путем установки найденных расчетным путем токов записи;

— контроль насыщения магнитного материала испытуемой МК путем записи сигналов контрольными токами и их последующего воспроизведения с сопоставлением амплитуд сигнала при контрольных токах записи [2, 3];

— контроль амплитуды сигнала воспроизводимого с магнитной полосы испытуемой карты путем сопоставления амплитуд воспроизводимого сигнала с эталонной и испытуемой карт при эталонных токах записи [2, 3];

— контроль разрешающей способности испытуемой МК путем сопоставления амплитуд воспроизводимого сигнала при плотностях записи 8 ипн/мм и 20 ипн/мм;

— контроль стираемости записи путем записи эталонными токами и стирания постоянным током с последующим определением амплитуды остаточного сигнала;

— контроль дефектности магнитной полосы путем записи заданной последовательности логических символов и анализа воспроизведенных сигналов;

— автоматическая отбраковка МК при выявлении отклонения ее характеристик от установленных техническими условиями;

Таким образом, АКП представляет собой сложную электронно-механическую систему, которая при массовом контроле МК должна быть полностью автоматизированной.

В работе проведены экспериментальные исследования, позволяющие определять влияние характеристик канала записи-воспроизведения, включая износ магнитной полосы МК, на параметры воспроизводимых сигналов, и как следствие, на точность восстановления записанных данных. В ходе экспериментов осуществлялась запись измерительной кодовой последовательности, и анализ сигналов, полученных на выходе усилителя воспроизведения. Сигнал, воспроизведенный со второй дорожки магнитной полосы, выведенной из обращения банковской МК, представлен на рис. 1, на котором построена его огибающая. Рассмотрение представленной сигналограммы говорит о значительной степени износа магнитной полосы МК, что объясняется ее длительным использованием. Для наглядности на рис. 2 представлен фрагмент воспроизведенного сигнала.

Разработана программа, с использованием языка С, позволяющая определять характеристики сигналов, воспроизводимых с МК, включая джиттер. Кроме того, при установлении различных порогов принятия решений при восстановлении воспроизведенных сигналов, имеется возможность осуществлять сравнение записываемой и считанной информационной последовательности.

В результате проведенной работы реализован аппаратно-программный комплекс, позволяющий проводить сравнительные исследования МК различных типов, инфраструктура обеспечивающая функционирование которых широко развита и не сдает позиции по сравнению с новым поколением идентификационных документов пользователя, функционирующем на основе радиочастотных технологий [5-8].

Литература

1. **Зелевич Е.П.** Пластиковые карты в связи. — М.: Радио и Связь. —2004. —288 с.

2. ГОСТ Р ИСО/МЭК 7811-2-2002 Карты идентификационные. Способ записи. Часть 2. Магнитная полоса малой коэрцитивной силы.

3. ГОСТ Р ИСО/МЭК 7811-6-2003 Карты идентификационные. Способ записи. Часть 6. Магнитная полоса большой коэрцитивной силы.

4. ГОСТ Р ИСО/МЭК 7810-2006 Карты идентификационные. Физические характеристики.

5. **Зелевич Е.П.** Проблема организации доступа к информационным ресурсам с помощью бесконтактных идентификационных документов пользователя// T-Comm, 2008. — спецвыпуск "Информационная безопасность". — С.28-33.

6. **Дшхунян В.Л., Шаньгин В.Ф.** Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты. — М.: НТ Пресс, 2004. — 695 с.

7. **Зелевич Е.П.** Основные подходы к формированию единого идентификационного пространства// T-Comm, 2009. — спецвыпуск "Информационная безопасность". — С.36-37.

8. **Зелевич Е.П.** Идентификационные технологии для управления процессами в инфокоммуникационной среде// Электросвязь, 2006. — № 2. — С.34-37.

Анализ влияния свойств объектов на функционирование систем радиочастотной идентификации

Технология радиочастотной идентификации (РЧИД) является универсальным инструментом отслеживания продукции в глобальной цепи поставок. Однако эффективность работы системы РЧИД зачастую зависит от условий эксплуатации. Сиситемы РЧИД критичны к материалам объектов, на которых расположены метки. Проведен анализ влияния свойств различных объектов на функционирование систем РЧИД.

Ключевые слова:
радиочастотная идентификация, специализированные радиометки, логистика

Зелевич Е.П.,
Профессор МТУСИ,
oiris.mtusi@gmail.com
Черников К.В.,
Студент дипломник МТУСИ

Радиочастотная идентификация обладает рядом преимуществ по сравнению с другими технологиями идентификации. Расстояние, на которых происходит получение идентификационной информации, варьируется от нескольких миллиметров до нескольких десятков метров. Технология РЧИД позволяет получать информацию о предмете без необходимости обеспечения его прямой видимости. Радиочастотные метки могут быть весьма различны по оформлению. Они могут иметь вид пластиковых карт формата ИД-1 или могут быть выполнены в виде стеклянных капсул, вживляемых в животных, для отслеживания их перемещения и т.п. Частота, на которой работают метки и считывающие устройства также различна и находится в пределах от 125 кГц до 5,8 ГГц [1].

Используя технологию РЧИД, которая обладает рядом преимуществ по сравнению со штриховым кодированием, можно ожидать высокой точности идентификации объектов. В реальных условиях, при решении задач логистики, довольно часто возникает необходимость идентифицировать объекты, содержащие металл или контейнеры с жидкостью. Устройства считывания не всегда способны взаимодействовать с меткой через такие объекты (радиоволны отражаются от металлических поверхностей и сильно поглощаются жидкостями). Специалистам приходится экспериментировать с расположением устройств считывания, чтобы добиться увеличения точности идентификации данных с метки. Кроме того системы РЧИД подвержены воздействию других систем радиосвязи, работающих на той же частоте.

К иным существующим ограничениям применения систем РЧИД относятся:

— возможность отказа систем при наличие радионепрозрачных и радиопоглощающих объектов.

— условия окружающей среды также могут оказывать негативное влияние на РЧИД системы;

— на функционирование РЧИД системы может отрицательно влиять неправильная установка оборудования (например, неточное расположение и ориентация антенны);

— несмотря на то, что нет необходимости в обеспечении прямой видимости между меткой и считывателем, существует предел проникновения энергии радиоволн, даже через радиопрозрачные объекты [2].

При взаимодействии считывающего устройства с меткой, на параметры радиотракта влияют следующие факторы: поглощение, ослабление, диэлектрические эффекты, дифракция, потери в свободном пространстве, интерференция, отражение, преломление, а также рассеивание.

Влияние различных материалов на параметры радиотракта. На качество идентификации существенно влияют свойства материала, через который проходят радиоволны. Как известно, материал является радиопрозрачным для определенных частот, если радиоволны проходят через него без существенных потерь энергии. Соответственно — радионепрозрачным, если он блокирует, отражает или рассеивает радиоволны. Радиопоглощающий материал пропускает через себя радиоволны, но с существенными потерями энергии. Уровень радиопоглощения и радионепрозрачности зависят от частоты, используемой конкретной системой. Так, например, материал может быть радиопоглощающим на определенной частоте и радиопрозрачным на другой частоте [3].

Влияние емкостей с жидкостями и металлических конструкций на функционирование системы РЧИД. Вода или влажные поверхности неблагоприятным способом влияют на эффективность взаимодействия считывающего устройства и радиометки. Высокочастотные сигналы

Таблица 1

Внешние воздействия на системы РЧИД

Электромагнитные поля	Механические нагрузки	Химические Материалы	Температурный режим	Природные факторы
Отражающие или электропроводящие поверхности, материал, поглощающий радиоволны, электростатический заряд ...	Удары, вибрации давление, трение, деформация, физические нагрузки ...	Масло, чистящие средства, смазочный материал, кислота, щелочь, растворитель …	Рабочая температура и температура хранения оборудования	Дождь, туман, влажность, мороз, лёд, солнечное излучение, солёный морской воздух ...

Таблица 2

Свойства некоторых типов материалов

Материалы	НЧ	ВЧ	УВЧ	Микроволны
Одежда	-	-	-	-
Древесина	-	-	-	O
Графит	-	-	X	X
Металлы	-	-	X	X
Бумажные изделия	-	-	-	-
Вода	-	-	O	O

Радиопрозрачный — "–" ; Радиопоглощающий — "O"; Радионепрозрачный — "X".

(ВЧ) лучше проникают сквозь объекты, содержащие воду, чем УВЧ и микроволновые сигналы, которые имеют большее поглощение. Таким образом метки, работающие в ВЧ-диапазоне, являются наиболее подходящими для контейнеров, содержащих жидкости.

Металлические конструкции препятствуют распространению радиоволн затрудняют коммуникацию между меткой и считывателем не только, в случае если они будут помещены между ними, но и если будут расположены в непосредственной близости от них. Когда металлический объект помещен около антенны, характеристики этой антенны изменятся, и может возникнуть эффект расстройки частоты. Системы, работающие в высокочастотном диапазоне сильнее подвержены влиянию металлических объектов, чем системы, использующие более низкий частотный диапазон.

Наличие некоторых материалов между считывателем и меткой, не только может затруднить работу системы, но и полностью блокировать радиоволны. Эффективность функционирования РЧИД систем будет снижена, если метка помещена на поверхность из такого материала, что приведёт к уменьшению дальности считывания. Также может произойти смещение рабочей частоты метки. Если рабочую частоту метки сдвинуть, так что она выйдет из полосы частот считывателя, то считыватель не будет в состоянии идентифицировать данную метку.

Для идентификации объектов, выполненных из металла, контейнеров, содержащих жидкость, а также материалы с высокой диэлектрической постоянной, нужно прибегнуть к специальным мерам [6].

Например, некоторые материалы, такие как жидкости или металлы, оказывают сильное влияние на функционирование УВЧ меток, которые имеют рабочую частоту 915 МГц (США). Антенны таких меток принимают сигнал с частотой от 900 МГц (на 15 МГц ниже) и до 930 МГц (на 15 МГц выше. Если метка помещена на металлическую поверхность, рабочая частота может сместиться до 800 МГц, и тогда диапазон, в котором она сможет принять сигнал считывателя, будет лежать в пределах от 785 МГц (–15 МГц) до 815 МГц (+15 МГц).

Если известно, что метка прикрепляется к металлическому объекту, который изменит рабочую частоту метки с 915 МГц до 800 МГц, то можно спроектировать метку, у которой в идеальном состоянии была бы рабочая частота 1030 МГц (+115 МГц). При размещении метки на металлическом объекте, ее частота снизится до стандартной частоты 915 МГц и будет функционировать в диапазоне 900-930 МГц.

Для повышения эффективности работы систем РЧИД в неблагоприятных условиях, изготовители разработали метки, предназначенные для использования с определенными материалами. Такие метки имеют специальные оболочки. Например, существуют метки для размещения на металлической, стеклянной поверхности, на контейнерах с жидкостью, и т.д. Как правило, нежелательно использовать метки, предназначенные для работы с объектами, сделанными из одного материала, для объектов, сделанных из иных материалов, т.к. это может привести к нарушению функционирования системы.

Несмотря на то, что металлы являются отражателями, однако, они также могут поглотить часть радио энергии и рассеять ее через металлическую поверхность.

Размещение метки на металлической поверхности. Если метку в стеклянном корпусе поместить горизонтально в небольшое углубление на металлической поверхности, то она сможет эффективно взаимодействовать с устройством считывания. Существует возможность защитить метку металлической крышкой. Однако, необходимо оставить узкий промежуток из диэлектрического материала (краска, пластик, воздух и т.д.) между двумя металлическими поверхностями для эффективной работы метки. Помещение метки в металлическую основу позволяет использование ее в жестких условиях (они могут выдерживать нагрузку в несколько тонн) [5].

Особенности радиочастотных меток, работающих в различных диапазонах. Системы РЧИД в диапазоне низких частот (30-300 кГЦ) имеют малую дальность считывания — дальность идентификации у систем РЧИД, работающих в НЧ-диапазоне, меньше полуметра, а также низкую скорость передачи данных. Из-за более высокой длины волны, НЧ-сигналы меньше подвержены поглощению атмосферой и материалом, через который они проходят. Поэтому системы РЧИД, работающие в НЧ-диапазоне, эффективно работают рядом с металлическими конструкциями и контейнерами с жидкостью. Имея малую дальность считывания и хорошую проникающую способность, НЧ-системы являются более устойчивыми к внешним воздействиям, по сравнению с системами, работающими на более высоких частотах.

Системы РЧИД, работающие в высокочастотном диапазоне (3 МГц — 30 МГц) используют частоту 13,56 МГц, которая является глобально принятой частотой для систем РЧИД. Сигналы ВЧ-диапазона не могут проникать сквозь материалы, так же как хорошо, как НЧ-сигналы. Использование этого частотного диапазона, обеспечит большие скорости передачи данных, в сравнении с НЧ-диапазоном.

Высокую скорость считывания и передачи данных имеют системы РЧИД, работающие на ультра высокой частоте (300 МГц — 3 ГГц). Однако системы в этом диапазоне относительно новы и сталкиваются с некоторыми проблемами. Из-за меньшей длины волны, радио энергия может быть легко поглощена жидкостями, что может значительно сократить дальность считывания. Страны распределили различные частоты для РЧИД-систем в этом диапазоне, поэтому система УВЧ, которая работает в одной стране, не могла бы работать в другой. Много потребительских устройств также функционируют в этом частотном диапазоне, что может привести к помехам от них.

Системы РЧИД в микроволновом диапазоне (1 ГГц — 300 ГГц) обычно работают на частотах 2,44 и 5,80 ГГц, которые предлагают высокую скорость передачи данных и большую

Таблица 3

Характеристики систем РЧИД, работающих в различных радиочастотных диапазонах

Частота	Достоинства	Недостатки	Использование
НЧ	Эффективная работа вблизи металла и воды. Общеприняты во всём мире.	Маленькая дальность считывания и низкая скорость передачи данных.	Идентификация животных, продуктов, меток на объектах, содержащих воду.
ВЧ	Высокая точность идентификации и скорость считывания. Большой объём информации.	Требуют большую мощность передатчика считывателя	Контроль доступа, авиабагаж, библиотеки.
УВЧ	Большая скорость считывания. Большой объём информации.	Мало эффективно работают вблизи воды и металла.	Доступ на автостоянки, автоматический сбор пошлины, канал поставок
Микроволны	Большая скорость считывания.	Мало эффективно работают вблизи воды и металла.	Идентификация транспорта, автоматический сбор пошлины, канал поставок

дальность считывания. Однако они имеют низкую эффективность работы рядом с металлическими конструкциями и продуктами, содержащих воду [4].

Выводы

При внедрении систем РЧИД необходимо учитывать некоторые ограничения, а именно: невозможность размещения меток под экранирующими поверхностями, подверженность влиянию помех от радиосредств, функционирующих в том же частотном диапазоне и т.п.

Системы РЧИД критичны к материалам объектов, на которых расположены метки. Это затрудняет их применение на металлических поверхностях и контейнерах, содержащих жидкости.

Необходимо принимать специальные меры для минимизации негативного влияния объектов, содержащих металлические элементы и воду, на функционирование систем РЧИД.

Целесообразно создание специализированных радиометок, предназначенных для установки на объекты, свойства которых влияют на процесс их идентификации.

Литература

1. **Дшхунян В.Л.** Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты / В.Л. Дшхунян. В.Ф. Шаньгин. — М: Издательство "НТ Пресс". 2004. — 695 с.
2. RFID for the Optimization of Business Processes. Carl Hanser Verlag GmbH & Co. KG. 2007.-286 с.
3. **Sandip Lahiri.** RFID Sourcebook. Издательство Prentice Hall PTR. 2005. — 304 с.
4. Paul Sanghera. RFID + Exam Study Guide. Syngress Publishing. 2007. — 354 с.
5. **Klaus Finkenzeller.** RFID Handbook, 2nd ed. John Wiley & Sons Ltd. 2003. — 446 с.

WiMAX Forum региональное видение: Россия и СНГ

С 18 по 19 ноября 2009 г. в Москве прошла очередная международная конференция Ассоциации WiMAX Forum "WiMAX Forum региональное видение: Россия и СНГ", проводимая компанией INFORMA Telecoms & media (Великобритания).

В работе международной конференции "WiMAX Forum региональное видение: Россия и СНГ" приняло участие более 80 участников из 20 стран мира, представляющих регулятора (Минкомсвязь РФ, Роскомнадзор РФ), разработчиков и системных интеграторов, инвесторов, консалтинговых и научных центров и Ассоциаций операторов связи.

Международная конференция "WiMAX Forum региональное видение: Россия и СНГ" была посвящена следующим вопросам: на каких рынках в пределах России и СНГ сегодня наиболее благоприятные условия для WIMAX; тенденции регионального широкополосного рынка и перспективы прироста абонентов; какие сервисы определяют революцию 4G; какое воздействие на пропускную способность оказывает совместное использование новых устройств и программного обеспечения; индустрия WiMAX: Вызовы и возможности WiMAX; позиционирование WiMAX услуг на местном конкурентном рынке: когда мобильность имеет смысл; ценовая стратегия и стратегия пакетирования услуг для стимулирования спроса и привлечения новых абонентов; когда в России состоится аукцион по выделению спектра для WiMAX и в каком частотном диапазоне; какие ограничения в настоящее время существуют в диапазонах 2,5/3,5 ГГц и каковы последствия этого для WiMAX.

Конференцию открыли Зам. министра связи и массовых коммуникаций д.т.н. проф. Н.С. Мардер и Директор WiMAX Forum по России и СНГ, член отделения "Информационных и телекоммуникационных технологий" РАЕН — д.т.н., академик РАЕН С.Л.Портной. Н.С. Мардер доложил о задачах инновационного развития широкополосных беспроводных технологий связи и роли регулятора в стимулировании и поддержке этого развития на территории России. В ходе конференции было заслушано более 20 докладов и сообщений. Отделение "Информационные и телекоммуникационные технологии" РАЕН приняло участие в работе международной конференции.

В рамках конференции компанией DETECON и ее московским представительством был проведен семинар по актуальным вопросам строительства сетей и развития бизнеса WiMAX на котором с докладами выступили Иностранный член ИТТ РАЕН, руководитель группы управления жизненным циклом продукта, компании DETECON International, д-р Юлиус Головачев (Германия), а также Региональный директор по России и СНГ Rainer Seelig и Глава московского представительства DETECON А.Плотников.

Доклады Председателя ИТТ РАЕН, д.э.н, академика РАЕН. Тихвинского В.О "WiMAX в период экономического спада: определение влияния воздействия мирового экономического кризиса на амбиции операторов и ожидания инвесторов в России и странах СНГ", Руководителя РГ 11 ИТТ РАЕН, д.т.н., академика РАЕН С.Л.Портного "Обзор рынка и новинок: как WiMAX изменяет динамичность конкуренции в России и СНГ" и Иностранного члена ИТТ РАЕН, д-ра Юлиуса Головачева доступны по запросу.

В ходе конференции Директор WiMAX Forum по России и СНГ, член отделения ИТТ РАЕН - д.т.н., академик РАЕН С.Л.Портной представил свою новую книгу "Энциклопедия WiMAX: путь к 4G", написанную в соавторстве с В.М. Вишневским и И.В. Шахновичем.

Анализ перспектив применения технологии RFID для задач управления поставками и складскими ресурсами

Ключевые слова:
Идентификационные технологии, штрихкодовое кодирование, управление поставками, ERC Network

Рассматриваются перспективы применения технологии RFID для решения задач применения управления поставками и управления складскими ресурсами. Проанализировано использование RFID в цепочке поставок, обоснованы преимущества технологии RFID по сравнению с штрихкодовым кодированием.

Русаков Д.А.,
аспирант МТУСИ

Введение. Технология RFID существует с 1940-х гг. XX в., но только в последние годы развитие технологий позволило рассматривать ее практическое применение в цепочке поставок. Несмотря на огромные перспективы, RFID все еще находится в стадии становления. Стоимость компонентов и систем RFID значительно снизится через несколько лет, пока предоставляя потребителям время, для принятий решения об использовании этой технологии. Это объясняет, почему многие крупные поставщики, дистрибьюторы и ритейлеры запускают пилотные программы или планируют их в скором времени. До сегодняшнего времени, применение RFID было в большинстве случаев правом собственности одной компании и не выходило за границы ее деятельности.Wal-Mart является наиболее показательной компанией, не просто использующей RFID, но и активно продвигающей данную технологию среди других компаний, в частности своих поставщиков. В 2003 г. руководство компании обратилось к своим поставщикам с историческим заявлением, которое произвело резонанс как в рядах самих поставщиков, так и среди многочисленных производителей средств безопасности и цепочек поставки сетей во всем мире. Компания объявила, что 100 самых крупных поставщиков потребительских товаров и производителей фармацевтической продукции обязаны начиная с января 2005 г. все свои товары, которые будут направляться в адрес Wal-Mart в коробках, ящиках и на поддонах, снабжать RFID-метками. Для остальных поставщиков такой срок установлен на январь 2006 г. В 2004 г. в компании начался пилотный проект внедрения системы RFID и к 1 января 2007 г. обязала всех своих поставщиков производить товары только с радиометками. За последние три года наблюдалось десятикратное увеличение количества магазинов Wal-Mart, использующих RFID, со 100 супермаркетов в 2004 г. до 1000 — в 2007. Согласно исследованию Cap Gemini Ernst & Young, 100 наиболее крупных поставщиков компании составляют 3 млрд. долл. рынка RFID, при этом одна треть приходится на радиометки, треть на архитектуру и ридеры,и еще одна треть на сервисы .

Раньше технология RFID в основном использовалась для идентификации людей и применялась в транспорте, для контроля доступа, платежах и паспортах. Однако уже сейчас есть тенденция к тому, что данная технология используется для идентификации товаров для управления активами, цепочкой поставок и в розничной торговле.

Опираясь на прогнозы исследователей, можно предположить, что управление цепочкой поставок становится областью номер один в применении RFID. Происходит это из-за того, что уже сейчас видны преимущества, которые дает эта технология, опережая уже известные и широко используемые инструменты, такие как, например, штрих-коды.

Еще десятилетие назад продажи RFID-систем в областях безопасности и общественного транспорта занимали около 80-90%, в 2003 г., по данным журнала Reseller, в Европе для обеспечения контроля доступа было продано только 33% всех RFID-систем. Сегодня на первый план выходит применение RFID в логистике (складской и транспортной), а также стремительно растет доля в производстве и торговле как оптовой, так и розничной.

Управление цепочкой поставок является на сегодняшний день одним из наиболее сложных технологических процессов в компании. Для повышения конкурентноспособности бизнеса необходимо решать целый комплекс задач, связанных с управлением цепочкой поставок: снижать затраты на транспортировку и дистрибуцию, оптимизировать цены, минимизировать запасы плохо реализуемых товаров и сокращать издержки на их хранение. В этой связи все больше предприятий розничной торговли обращаются к SCM-решениям, чтобы перестроить свои логистические цепочки в соответствии с меняющимися требованиями рынка. Все более актуальной становится такая SCM-система, которая была бы ориентирована на оптимизацию взаимодействия с дистрибуторами и конечными потребителями.

Сегодня технология RFID (Radio Frequency Identification, радиочастотной идентификации) формирует один из многообещающих сегментов рынка информационных технологий. Популярность RFID обусловлена возможностями, которые открывает данная технология для управления цепочками поставок — прежде всего, это более эффективное управление бизнес-процессами и сокращение издержек контроля грузопотоков.

Использование RFID в цепочке поставок. Товар отслеживается RFID-системами на каждом из этапов цепочки поставок: на производстве, при перевозке, в момент складской обработки и в момент продажи. Аналогично, под радиочастотным контролем находятся вся техника и персонал, обеспечивающий процесс товародвижения. Полученная информация сохраняется в информационной системе текущего звена цепи распределения. К отдельным отчетам, строящимся на основе данной информации, открывается доступ для авторизированных пользователей, в том числе и внешних (для предприятий-партнеров). Их анализ позволяет каждому участнику процесса принимать свои управленческие решения. На рис. 1 показано использование RFID на различных этапах цепочки поставок.

Рассмотрим основные этапы цепи управления поставками, на которых используется RFID. На этапе производства происходит экономия времени при сборке и отслеживание деталей, а

Таблица 1

Применение RFID-систем по областям использования

	2004, %	2008, %	Разница, %
Контроль доступа	33,4	18,1	- 15,3
Оплаты	20,4	8,3	- 12,2
Контроль за имуществом	17,8	22,3	+ 4,5
Иммобилайзеры для а/м	6,7	2,8	- 3,9
Транспорт/билеты	4,4	4,6	+ 0,3
Цепочки поставок	4,0	25,7	+ 21,7
Идентификация животных	2,9	3,2	+ 0,3
Авиатранспорт	2,3	2,4	+ 0,1
POS-терминалы (кассовые аппараты)	1,5	2,4	+ 0,9
Другое (аренда, багаж) и т.д.	6,5	10,2	+ 3,7

также автоматизируются нижние уровни. Наибольшее распространение RFID-технология получила при конвейерной сборке таких товаров, как, например, автомобили и бытовая техника. Поскольку с одного конвейера могут сходить разные модели, радиометки позволяют идентифицировать каждую деталь, предназначенную для конкретной модели. На деталь наносится радиометка, которая считывается в зоне действия ридера и, в зависимости от полученных данных, направляется на свой участок сборки. Это позволяет исключить ошибки при сборке и, соответственно, повысить ее качество и сократить общее время выхода изделия с конвейера. Радиометки могут прикрепляться в процессе производства непосредственно к самому изделию или к его упаковке с целью их последующего информационного наполнения в каналах распределения.

На этапе розничной продажи позволяет решить проблемы естественной убыли продуктов, т.е. воровства, а также недостатка запасов на полках. В настоящее время для розничных торговых сетей радиоидентификационная технология приобретает все большее значение. Благодаря тому, что RFID-метка может содержать много различной информации, магазин способен контролировать наличие товара в продаже, вести учет популярности различных продуктов и оперативно реагировать на поступающие данные, регулируя вопросы спроса-предложения. Также можно легко отслеживать соблюдение сроков хранения продуктов питания, как это делает английская розничная сеть Sainsbury, контролируя срок годности 225 тысяч упаковок с готовой едой еженедельно. Помимо Wal-Mart и Sainsbury показательный супермаркет Future Store с товарами, помеченными RFID-метками, открыла в Германии торговая сеть Metro. Внедрение RFID-систем в розничных торговых сетях позволяет не только решать проблему мониторинга поставок, но и осуществлять автоматический заказ продукции и контроль даты реализации скоропортящейся продукции, как в дистрибьюторском центре, так и в магазинах сети.

Кроме того, применение RFID-технологии позволит значительно ускорить процесс обслуживания покупателей, поскольку вместо считывания штрих-кодов с каждой товарной единицы на расчетном узле, покупателю достаточно пронести корзину с товарами через специальную рамку, и кассир получит полную информацию о его покупках. Товар со встроенной меткой, совершенно незаметной для покупателя, невозможно будет вынести из магазина, не оплатив его, следовательно, случаи воровства можно будет свести к минимуму.

Рис. 1. Использование RFID в цепочке поставок

EPCglobal Network. История использования RFID для управления цепочкой поставок началась в 1997 г., когда сотрудник компании Procter & Gamble Кевину Эштону начал использовать тэги RFID для управления движением товаров. Кевин Эштон посчитал, что использование тэгов RFID поможет ускорить реакцию ритейлеров и их поставщиков на изменение спроса и предложения. Ему удалось убедить свою компанию, а также крупные компании-ритейлеры такие как Wal-Mart, Coca-Cola, Johnson & Johnson, Unilever, Home Depot, PepsiCo, что идея имеет будущее.

При поддержке этих компаний на базе Массачусетского технологического института была создана лаборатория, которую назвали Auto-ID Center и руководителем которой стал Кевин Эштон, по исследованию вопросов применения и выработке стандартов RFID для управления цепочкой поставок. В конце октября 2003 г. эта лаборатория закрылась, посчитав свою миссию выполненной. Разработанная технология была передана EPCglobal — организации, которая в настоящее время управляет и развивает стандарты для технологии RFID.

Лаборатория Auto-ID Center разработала сеть EPCglobal Network, которая должна стать основой глобальной цепи управления поставок будущего. Цель создания сети EPCglobal Network заключается в том, чтобы обеспечить немедленную, автоматическую идентификацию товаров и обмен информацией о них в цепи поставок. В сентябре 2003 г. была выпущена первая версия спецификаций, которые описывают каждый компонент сети EPCglobal Network. Некоторые из этих спецификаций уже приняты к одобрению, другие находятся в стадии обсуждения и доработки.

Сеть EPCglobal Network состоит из 5 элементов:

• **Электронный код товара** (EPC, Electronic Product Code) — это уникальный номер, который идентифицирует отдельную единицу товара. Электронный код товара состоит из нескольких блоков, которые определяют производителя (например, Gillette), тип продукции (например, батарейки Duracell AAA) и саму отдельную единицу товара (конкретную упаковку с парой батареек).

Используя этот код, любое звено в цепочке поставки может идентифицировать отдельную единицу товара и найти о ней информацию. Код EPC имеет длину 96 бит, он позволяет задать более 268 млн. производителей, каждый из которых может выпускать более 16 млн. типов товаров. Объем производства каждого типа товара может составлять почти 69 млрд. единиц.

• **Тэги RFID** представляют собой устройство, объединяющее кремниевый чип и антенну,

используемую для передачи информации в диапазоне радиоволн. Тэг хранит в себе электронный код товара. Для чтения информации с тэгов используются специальные устройства чтения (ридеры), которые затем передают полученную информацию в различные программные приложения для ее обработки. Устройства чтения могут читать до 1000 тэгов в секунду. Стандарты EPCglobal предполагают, что на тэге хранится электронный код товара и только.

В настоящее время существуют три спецификации EPCglobal на следующие типы тэгов: 900 МГц Class 0, 863-930 МГц Class 1 и 13,56 МГц ISM Band Class 1. Все они описывают так называемый пассивный тэг, т.е. тэг, не имеющий батарейки, и для своей работы использующий энергию приходящих от устройства чтения радиоволн. Class 1 и Class 0 отличаются друг от друга структурой хранимых данных и способом функционирования: тэги типа Class 0 работают только на чтение информации (их программируют на фабрике), в тэги типа Class 1 можно записать информацию один раз.

Предполагается, что тэги типа Class 2 будут перезаписываемыми много раз. В настоящее время группой компаний передана на рассмотрение EPCglobal спецификация на т.н. "протокол второго поколения", описывающая взаимодействие с пассивным тэгом, который функционирует в диапазоне 868-956 МГц (UHF Generation 2 Protocol), в который информация может быть записана много раз и который поддерживает шифрованное общение с устройством чтения.

Существует также группа стандартов ISO 18000, которые описывают протоколы взаимодействия устройства чтения и тэга в различных диапазонах частот, в частности, предложенный, но еще не одобренный стандарт ISO 18000-6 делает это для диапазона 860-930 МГц. Стандарты ISO конкурируют со стандартами EPCglobal, что ведет к проблемам несовместимости оборудования и т.д. Поэтому сейчас ведется работа по тому, чтобы требования спецификаций "протокола второго поколения" EPCglobal и ISO 18000-6 совпадали для создания единого глобального стандарта.

• **Служба ONS (Object Naming Service)** — каталог источников информации, из которых можно получить данные об отдельной единице товаре по ее электронному коду. Она представляет собой иерархическую систему, напоминающую систему Domain Name System (DNS) сети интернет: от расположенной на самом верхнем уровне корневой службы ONS до локальных служб ONS производителей на самом нижнем уровне. Служба ONS получает электронный код товара и выдает адрес того места, где хранится информация о товаре.

• **Язык описания физических объектов (PML, Physical Markup Language).** Данный язык используется для описания товара, которое помогает найти служба ONS по электронному коду товара. В его основе лежит язык XML.

• **Программная технология Savant —** предназначена для сбора, хранения и обработки информации, получаемой от устройств чтения. Она имеет распределенную архитектуру и построена на иерархической основе. Технология Savant сглаживает поток данных, фильтрует его, устраняет сдвоенные чтения и передает информацию дальше либо в режиме online, либо в режиме с буферизацией.

Если необходимо получить какую-нибудь информацию о товаре по полученному от устройства чтения коду, Savant может послать запрос в службу ONS.

Как уже было отмечено выше, цель создания сети EPCglobal Network заключается в том, чтобы обеспечить немедленную, автоматическую идентификацию товаров и обмен информацией о них в цепи поставок. Для этого необходимо, во-первых, чтобы существовал единый и универсальный метод идентификации каждой единицы товара; во-вторых, наличие стандартного механизма, благодаря которому информация о каждой единице может быть доступна каждому участнику цепи поставки. Первая задача решается с помощью электронного кода товара EPC. Вторая задача решается собственно самой сетью EPCglobal Network, которая использует интернет для создания механизма нахождения и обмена информацией о товаре для торговых партнеров.

Принципы работы сети EPC Network

Производитель товаров на фабрике помещает тэг на каждую единицу товара. Товар укладывается в ящики, на каждый из которых также устанавливается тэг. Ящики ставятся на паллеты. Каждый паллет также несет на себе тэг. Когда грузовик с паллетами покидает фабрику, устройство чтения, расположенное на воротах зоны погрузки, "будит" тэги. Тэги используют энергию радиоволн, приходящих от устройства чтения, для передачи ему электронного кода, который они содержат в себе.

Устройства чтения передают прочитанные коды в компьютерную сеть, в которой работает программное обеспечение, реализующее технологию Savant. Система Savant посылает через веб запрос службе ONS, которая по электронному коду находит адрес сервера, содержащего исчерпывающую информацию о товаре. Данный сервер называется сервер EPC Information Services. Он использует язык PML для хранения информации о товарах. Он определяет, что пришедший электронный код принадлежит данному товару данного производителя. Поскольку сервер также знает, какое устройство чтения прочло пришедший код, то становится известным, на какой из фабрик был произведен этот товар. Если вдруг в товаре обнаружится какой-нибудь дефект изготовления, то будет легко определить виновную фабрику, а так же отозвать товар из торговой сети.

Система Savant может вносить изменения в информацию о товаре. Поэтому всякий раз, как товар проходит через какую-нибудь точку в цепи поставки (например, склад оптовика), в которой установлено устройство чтения, подключенное к системе Savant, информация о товаре обновляется. Поскольку устройство чтения посылает свои координаты вместе с прочитанным содержимым тэга, то таким образом формируется история движения товара по цепи поставки. Этим обеспечивается полная прозрачность цепи поставки.

Когда товар поступает в распределительный центр ритейлера, то благодаря устройствам чтения, установленным там, не надо будет вскрывать груз на паллете, чтобы посмотреть его содержимое. Система Savant предоставит описание груза, и а также обеспечит, чтобы груз был погружен на соответствующий грузовик.

Товар поступает в магазин, который отслеживал поставку благодаря системе Savant. Поскольку на приемке тоже установлены устройства чтения, то информационная система магазина получает информацию о каждой поступившей единице товара быстро и эффективно, без привлечения для этого ручного труда.

На полке магазина, куда попадает товар, также стоят устройства чтения. Когда покупатель снимает с полки товар, об этом становится известно информационной системе магазина, которая при достижении определенного количества снятых единиц товара может автоматически отдать распоряжение о том, чтобы товар вывезли со склада в зал. Как только запас товара на складе снизился до определенного порога, информационная система сформирует заказ на данный товар. При наличии такой системы отпадает необходимость иметь на складе резервный запас данного товара. Кроме того, теперь нет потерь продаж из-за того, что товар отсутствует на полке или на складе.

Технология RFID также облегчает жизнь покупателю. Вместо того чтобы теперь стоять в очереди у кассы, ожидая того, как кассир отсканирует или введет с клавиатуры штрих-коды товаров покупателей, стоящих впереди, покупатель катит тележку с покупками мимо устройства чтения, установленного на кассе, и касса остается только просуммировать результат.

Следует отметить, что глобальная сеть EPC Network еще не создана, и приведенное выше описание является лишь видением того, как она должна работать. Для создания сети придется

решить много организационных (в частности, вопросы глобальной синхронизации данных) и технических проблем. В качестве первого шага на пути построения сети организация EPCglobal выбрала компанию VeriSign, которая управляет корневой системой DNS для домена .com, для управления корневой службой ONS.

Существуют коммерческие реализации технологий Savant, EPC Information Services, используемые в проектах по созданию локальных (на уровне "ритейлер и его поставщики") цепей поставки на основе RFID.

Преимущества технологии RFID в цепочке поставок

Популярность RFID во многом обусловлена возможностями, которые открывает данная технология для управления логистическими процессами. Далее необходимо выделить те преимущества, которые RFID дает при использовании в цепочке поставок.

• ***Повышение степени прозрачности глобальной цепочки поставок.***

Снабдив товар радиометкой в процессе производства и записав на нее основные характеристики товара (например, наименование товара и компании производителя, массу товара, срок реализации), каждый последующий участник логистической цепи может дополнять данные необходимой ему информацией. Так, поставщик может записать на радиометку пункт назначения; на складе будет отмечено местонахождение товара; в розничной торговой сети данные занесут в соответствии с принятой системой идентификации товара. В процессе транспортировки радиоидентификационная технология используется в целях контроля движения транспортных средств. По маршруту движения автофургонов в контрольных точках устанавливаются ридеры, которые регистрируют прохождение автомобиля и пересылают информацию на автотранспортное предприятие в режиме реального времени, что дает возможность отслеживать нахождение груза в логистической цепи и координировать действия в случае задержки его прибытия в пункт назначения. Также радиометка позволяет получать информацию о номерах накладных перевозимых грузов, путевых листах и другие сведения.

• ***Снижение затрат и увеличение скорости оборота.***

По оценке специалистов нью-йоркской консалтинговой фирмы Accenture, Министерство обороны США, Wal-Mart и другие организации розничной торговли и должностные лица, которые используют RFID, в качестве преимуществ могут рассчитывать на повышение производительности и эффективности сбытовой сети. Поставщики, которые внедрят средства сбора данных RFID, могут ожидать сокращения издержек. По прогнозам, использование радиоидентификаторов позволит увеличить спрос на 10-20%, сократить товарные запасы на 10-30% и увеличить товарооборот на 1-2%.

• ***Усовершенствованный процесс сбора данных.***

Основой эффективного взаимодействия фирм, составляющих цепь поставок, является отнюдь не RFID-технологии, а интеграция комплексных систем автоматизации. Но после построения надежных информационных связей следующим важным этапом становится обеспечение стабильного, полноценного потока данных. И в достижении этой задачи радиочастотная идентификация не имеет себе равных по эффективности. А еще и принимая во внимание тот факт, что информация о передвижениях товара поступает в режиме реального времени, то можно говорить о почти 100% точности.

Схематично процесс обмена информацией в рамках цепи поставок описан на рис. 2.

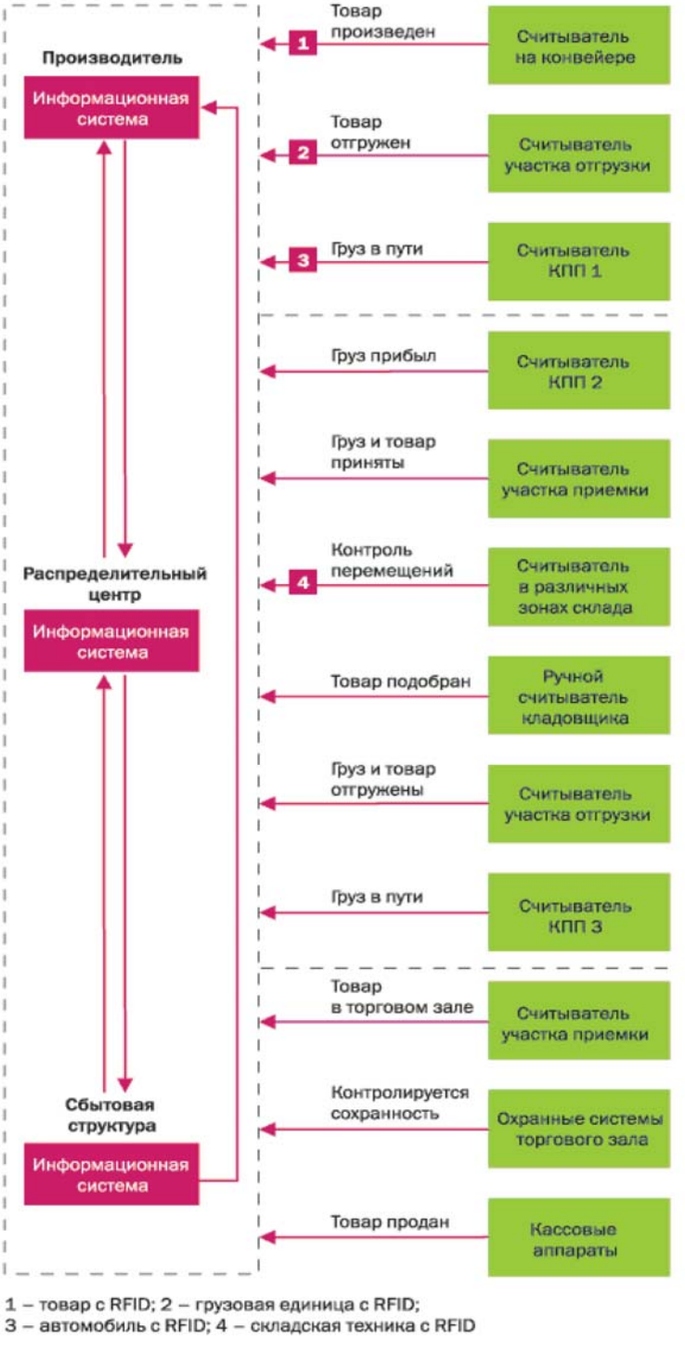


Рис. 2. Схема взаимодействия предприятий в рамках цепи поставок с использованием RFID

• ***Усовершенствованная цепочка поставок.***

Однако на предприятии, инвестирующем средства в RFID-системы, должны понимать, что усилия по совершенствованию своей собственной информационной системы и обеспечению полноты данных на уровне цепи поставок не ведут напрямую к сокращению издержек. Речь может идти лишь о предоставлении дополнительных информационных услуг своим партнерам. Однако поскольку такие услуги взаимны, достигается синергетический эффект, результатом которого становится увеличение эффективности деятельности всех взаимодействующих сторон.

Сотрудники распределительного центра, получая от поставщиков информацию о точном моменте выхода транспортного средства с товаром на маршрут и имея возможность отлеживать его продвижение, способны четко рассчитать ресурсы для оперативного приема и размещения товара на складе. В свою очередь, предоставляя доступ производителям и поставщикам к данным по остаткам товара на своих собственных складах, дистрибьютор может рассчитывать, что они грамотно спланируют свои производственные и закупочные процессы, что поможет избежать дефицита даже в самые напряженные дни работы.

Поставщики, имея с конечного этапа дистрибуции (из розничной торговой сети) информацию о динамике спроса и товарных остатках, могут эффективно планировать маркетинговую деятельность, закупочную политику и график поставок. Производители, получая оперативные данные от сбытовых подразделений, способны отслеживать текущие тенденции и принимать обоснованные решения по ассортименту той или иной продукции, запуску нового продукта или снятию с производства старого. Тем самым повышается адаптивность процесса, увеличивается вероятность успешного сбыта и сокращаются издержки по обработке неликвидов на всех этапах товародвижения.

Розничная сеть, являясь конечным (и наиболее важным) звеном в данной цепочке, генерирует параметры для работы всех остальных участков процесса товародвижения. Чем лучше производители и посредники анализируют данную информацию и следуют сделанным выводам, тем лучше предприятия розничной торговли реагируют на рыночные изменения и тем больше объемы сбыта, что соответственно повышает прибыльность всех участников процесса. Таким образом, можно утверждать, что цепочка поставок начинает функционировать с меньшими расходами, быстрее, лучше и с меньшим риском. Следует перечислить еще несколько преимуществ, которых можно достичь с помощью RFID:

• отслеживание срока годности продуктов;

• новые возможности продвижения продуктов;

• повышение уровня безопасности;

• удержание клиентов за счет соответствия их требованиям.

В настоящее время уже несложно представить, как применение концепции RFID на всех участках цепочки поставок сократит количество ошибок, потребности в запасах для достижения большей эффективности, лучшего управления активами и движения денежной наличности. По подсчетам аналитиков Wal-Mart, сокращение непрофильных издержек торговых предприятий может составлять 30-50%, а с учетом синергии процессов, экономический эффект может достигать по величине суммарной прибыли организации за период. Очень распространенной на сегодняшний момент идеей является, что RFID вскоре полностью заменит штрих-коды. Однако это совсем не так. Чтобы это произошло, RFID должна преодолеть "вскоре" значительные препятствия. В таблице 3 представлены основные преимущества RFID по сравнению со штрих-кодами, в цепочках поставок, а также проблемы, которые еще предстоит решить.

Даже сейчас, когда широкое использование RFID стало технологически возможным, все равно имеется довольно широкий круг проблем. Их нужно знать для того, чтобы сгладить путь использования RFID в будущем. Далее указан ряд ключевых сложностей, с которыми сталкивается RFID, которые также являются важными факторами успеха при ее внедрении.

• ***Высокая стоимость системы.***

В настоящий момент стоимость пассивной радиочастотной метки составляет от 0,15 долл. (при приобретении свыше 1 млн. шт.) до 3 долл. (при приобретении 1 шт.). В случае с метками защищенного исполнения (или на металл) эта цена может достигать 7 и более долл. А базовый ридер может стоить от 1000 до 4000 долл. каждый. Учитывая появляющиеся новые стандарты, прогресс в производстве микроизделий и конкурентные объемы экономики, отрасль RFID должна достичь своей целевой цены менее чем за десятилетие. Тем временем, однако, пока применение RFID относительно дороже других автоматически-идентификационных инструментов. Исходя из этого, использование радиочастотных меток целесообразно для защиты дорогих товаров от краж или для обеспечения сохранности изделий, переданных на гарантийное обслуживание. В сфере логистики и транспортировки грузов стоимость радиочастотной оказывается совершенно незначительной по сравнению со стоимостью содержимого контейнера, поэтому совершенно оправдано использование радиочастотных меток на упаковочных ящиках, паллетах и контейнерах.

• ***Возможное экранирование при размещении на металлических поверхностях.***

Радиочастотные метки подвержены влиянию металла (это касается упаковок определенного вида — металлических контейнеров, иногда даже некоторых типов упаковки жидких пищевых продуктов, запечатанных фольгой). Это вовсе не исключает применение RFID, но приводит или к необходимости использования более дорогих меток, разработанных специально для установки на металлические поверхности или к нестандартным способам закрепления меток на объекте.

• ***Подверженность систем радиочастотной идентификации помехам в виде электромагнитных полей.***

Включенное оборудование, излучающее радиопомехи в диапазоне частот, используемом для работы RFID-системой, может привести к помехам в ее работе. Необходимо тщательно проанализировать условия, в которых система RFID будет эксплуатироваться. Конечно, можно ут-

Таблица 2

Преимущества RFID

По отношению к штрих-коду	В цепи поставок
• Отсутствие необходимости в прямой видимости • Больший объем хранения данных • Возможность перезаписи • Большее расстояние чтения • Поддержка чтения нескольких меток • Устойчивость к воздействию окружающей среды • Считывание данных метки при любом ее расположении • Интеллектуальное поведение	• Повышение степени прозрачности глобальной цепочки поставок • Снижение затрат и увеличение скорости оборота • Усовершенствованный процесс сбора данных • Усовершенствованная цепочка поставок
Проблемы использования RFID	
• Высокая стоимость системы • Возможное экранирование при размещении на металлических поверхностях. • Подверженность систем радиочастотной идентификации помехам в виде электромагнитных полей	

верждать, что RFID имеет множество преимуществ перед штрих-кодами, но, исходя из всего вышесказанного, говорить о полной замене одной технологии другой просто невозможно. На основании проведенного в этой главе анализа можно понять, что обе технологии имеют как преимущества, так и недостатки и, по-видимому, будут сосуществовать как взаимодополняющие технологии в предстоящие годы.

RFID — это новый инструмент, который выводит управление цепочками поставок на новый уровень, способный решить многие проблемы, которые не в состоянии решить технология штрихового кодирования. Прикладные системы со штрих-кодами — это лишь некоторые из возможных направлений применения RFID. В действительности RFID может применяться в областях, которые находятся за пределами досягаемости штрих-кодов. Следовательно, эти две технологии имеют четко различающиеся функциональные возможности и диапазоны применения, в которых они работают лучше. По мере развития RFID эта технология может вызвать развитие прикладных систем, создание которых сегодня считается трудным или даже невозможным.

Анализ использования различных технологий в логистической сфере. Текущее состояние конкуренции в логистической сфере сейчас таково, что компаниям уже чрезвычайно сложно соперничать по ценовому фактору. Поэтому на первый план выходят те компании, способные предоставить наилучший сервис при минимальных издержках. В связи с этим возникает вопрос об оптимизации управления товарными запасами и цепочками поставок. Также существует множество проблем, связанных с продвижением товара от производителя к потребителю по цепи поставок. И здесь основным инструментом повышения эффективности управления цепочкой поставок являются информационные технологии. В работе были рассмотрены наиболее проблемные области SCM и проанализированы пути решения этих проблем с помощью информационных технологий. Отдельно была рассмотрена технология RFID. Очевидно, что технология радиочастотной идентификации только в начале пути своего развития, но, судя по достигнутым успехам и приведенной в работе статистике, имеет хороший потенциал. Существует ряд логистических процессов, в которых альтернатив данной технологии нет, например: текущий контроль над персоналом, управление автопарками или отслеживание транспортировки грузов, а главное достижение прозрачности информационных потоков. При перемещениях по разным звеньям цепочки поставок товар сопровождается информационными потоками, в которых содержится информация о том, где товар произведен, куда направлен, каковы его потребительские свойства, каким видом транспорта перевозится и т.п. Сейчас бумажные потоки во многом заменены компьютерными сетями, и это существенно снижает издержки, связанные с перемещением информации. Но чтобы ввести информацию в компьютер, требуется ручной труд и время. Сейчас наиболее распространенным инструментом является штриховой код, который в свое время решил проблему товародвижения.

На первый взгляд надежная и дешевая система штрихового кодирования по сочетанию параметров цена/качество выглядит привлекательней, однако она не способна предложить оптимальное решение перечисленных задач. Для того, чтобы доказать это, был проведен сравнительный анализ средств штрихового кодирования и радиочастотной идентификации.

Штрих-кодирование имеет множество проблем, которые способствуют развитию новых технологий, в частности RFID. В числе основных проблем стоит необходимость временных затрат на поиск штрих-кода на упаковке и размещение его перед сканером, последовательное считывание штрих-кодов на всех товарах, и невозможность считывания поврежденного штрих-кода. В результате эта технология не очень быстрая, не всегда удобная и надежная.

Комплексный контроль над всеми логистическими операциями, хотя и достигается при помощи больших первоначальных инвестиций, позволяет впоследствии достичь значительно больших стратегических преимуществ. Даже если рассматривать преимущества, получаемые только на уровне одного предприятия, их список вдохновит любого начальника логистического подразделения: сокращение ручного труда, уменьшение количества ошибок, сокращение бумажного документооборота, повышение уровня контроля всех процессов, совершенствование системы учета и т. д. Однако современная экономика все быстрее стремится к глобализации и интеграции. Таким образом, для успешного функционирования предприятия наиболее важным становится эффективное информационное взаимодействие с партнерами по цепи поставок. И на этом уровне возможности радиочастотной идентификации раскрываются максимально полно. Использование единых стандартов формирования информационных массивов позволяет построить гармоничную систему взаимовыгодного обмена данными и успешно интегрироваться в бизнес-сообщество наравне с крупнейшими транснациональными корпорациями.

Итак, существует решение, которое способно радикально решить многие проблемы, возникающие на пути движения товара по логистической цепи. Но на пути RFID-технологий возникает немало проблем. Пока и сами метки, и оборудование слишком дороги для того, чтобы рядовые компании могли использовать метки для оптимизации товародвижения. Во всем мире в области ритейла RFID-технология делает первые шаги. Для широкого распространения технологии радиочастотной идентификации необходимо создать условия — организационные и технические, и в первую очередь создать единую международную систему электронного кодирования, в рамках которой каждому товару будет присвоен свой уникальный номер. Прежде чем начать массовое производство и продажу идентификационных меток и оборудования, необходимо провести стандартизацию частот и протоколов обмена идентификационных меток и оборудования. Лишь выход на единые технические стандарты во всем мире позволит существенно увеличить объемы производства меток и понизить цены. В проекты по созданию RFID-технологий сейчас активно включились торговые сети Metro и Wal-Mart.

В настоящее время на первый план выходит применение RFID в логистике (складской и транспортной), а также стремительно возрастает роль RFID в сфере оптовой и розничной торговли.

Литература

1. **Базаров Р.** Опознавательные знаки. — Инфобизнес [Электронный ресурс], 2004. — 28 сентября. — Режим доступа: http://www.ibusiness.ru/marcet/tele/35732/, свободный.

2. Безопасность интермодальных контейнерных перевозок//Европейская конференция министров транспорта. [Электронный ресурс], 2005. — Режим доступа: http://www.cemt.org/pub/pubpdf/05ContainerRu.pdf, свободный.

3. **Беспалов Р.** Применение RFID в цепи поставок. — Логистика и управление, 2007. — №2. — С.15-19.

4. **Винокуров А.** Метки для вещей и людей. — Бизнес [Электронный ресурс]. — Режим доступа: http://www.sostav.ru/news/2006/08/ 08/62/#, свободный.

5. **Горев А.** Значение управления информационными потоками для повышения эффективности логистических систем. — ИД Гребенникова. Логистика сегодня, 2004. — №2. — С.8-15.

6. **Граванова Ю.** RFID в торговле: возможности и угрозы. — CNews Analytics. — Режим доступа: http://www.cnews.ru/reviews/free/trade2006/articles/rfidtrade/?print, свободный.

7. Десятка перспективных технологий. — PC Week Russian Edition [Электронный ресурс], 2007. — 16 февраля. — Режим доступа: http://www.pcweek.ru/ ?ID=623975&4Print=1, свободный.

Две задачи по сетям UMTS-900

Рассмотрены две практические задачи, решение которых может быть полезным для планирования сетей UMTS-900. Первая задача касается условий сохранения энергетики сети UMTS, эквивалентной по помеховому воздействию на систему РСБН со стороны заменяемого фрагмента сети GSM. Предложенная методика решения этой задачи носит общий характер и может быть использована и по отношению к другим РЭС в диапазонах частот 900/1800 МГц. Решение второй задачи имеет целью определить размер разделительной зоны между фрагментом локальной сети UMTS-900 и общей сетью GSM-900, в которых используется общий частотный ресурс.

Ключевые слова:
UMTS-900, GSM-900, электромагнитная совместимость, частотное планирование

Скрынников В.Г.,
к.т.н., независимый эксперт,
руководитель Рабочей группы по ЭМС
отделения ИТТ РАЕН

Ранее были опубликованы результаты исследований по совмещению сетей UMTS и GSM в диапазоне частот 900 МГц [1,2]. На этапе создания совмещенных сетей GSM/UMTS возникла необходимость решить две задачи прикладного характера:

1. Оценить условия энергетической эквивалентности создаваемой сети UMTS-900 и заменяемого ею фрагмента сети GSM в полосе частот шириной 5 МГц. Решение этой задачи позволит сохранить и не превысить энергетику реально функционировавшего фрагмента сети GSM в полосе частот, выделенной для сети UMTS. Это в свою очередь обеспечит условия ЭМС сети UMTS с системой РСБН, которые ранее были определены для сети GSM.

Актуальность такой задачи обусловлена несколькими факторами. Во-первых, условия ЭМС сети GSM с РЭС другого применения уже определены и апробированы в действующей сети. Во-вторых, применяемые методики оценки ЭМС для сетей GSM в настоящее время доведены до некоторого совершенства в результате уточнения их в ходе летных испытаний. Аналогичные методики для UMTS довольно сложны и сегодня практически отсутствуют [5].

Базовой основой для постановки такой задачи является следующий очевидный факт. Если частотный канал GSM являлся помеховым для РСБН, то мощность помехи, которая будет создаваться передатчиком UMTS в полосе этого канала, будет меньше примерно в 25 раз (на 14 дБ), и следовательно, количество помеховых передатчиков UMTS на этой частоте может быть во столько же раз больше.

2. Определить условия, при которых можно "развязать" по ЭМС построенный фрагмент сети UMTS (в составе совмещенной сети UMTS/GSM) и действующую сеть GSM, которая функционирует территориально за пределами совмещенной сети GSM/UMTS в общей полосе частот. Решение такой задачи позволит определить некоторую разделительную зону между указанными сетями и исключить их взаимное влияние.

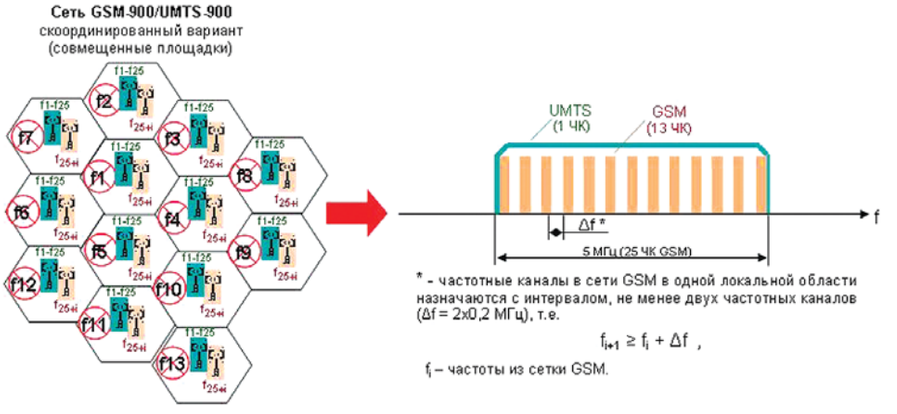


Рис..1. Общий сценарий к задаче 1

В статье рассмотрены подходы к решению отмеченных задач и приведены результаты их решения.

Задача 1

Исходные условия. Как было отмечено в [1], для UMTS достаточно выделить частотный ресурс сети GSM в виде непрерывной полосы шириной 5,4 МГц с учетом защитных частотных интервалов. При этом в активную полосу шириной 5 МГц попадает максимально 13 активных частотных каналов GSM, поскольку в одной локальной области частотные каналы в сети GSM назначаются с интервалом Df, равным 0,4 МГц. На рис. 1 эти каналы обозначены f1, f2,...,f13 и составляют часть общей полосы (f1-f25), выделенной для UMTS на скоординированных (совмещенных) площадках.

В табл. 1 приведены технические характеристики РЭС, которые были использованы при решении задачи.

Таблица 1

Технические характеристики РЭС

Параметры	UMTS	GSM
Ширина канала	5 МГц	0,2 МГц
Эффективная полоса	3,84 МГц	0,2 МГц
Мощность излучения	20 Вт 13 дБ Вт (БС)	20 Вт 13 дБ Вт (БС)
Эквивалентная мощность излучения в полосе 5 МГц	20 Вт 13 дБ Вт (БС)	13x20 Вт 24 дБ Вт (БС)

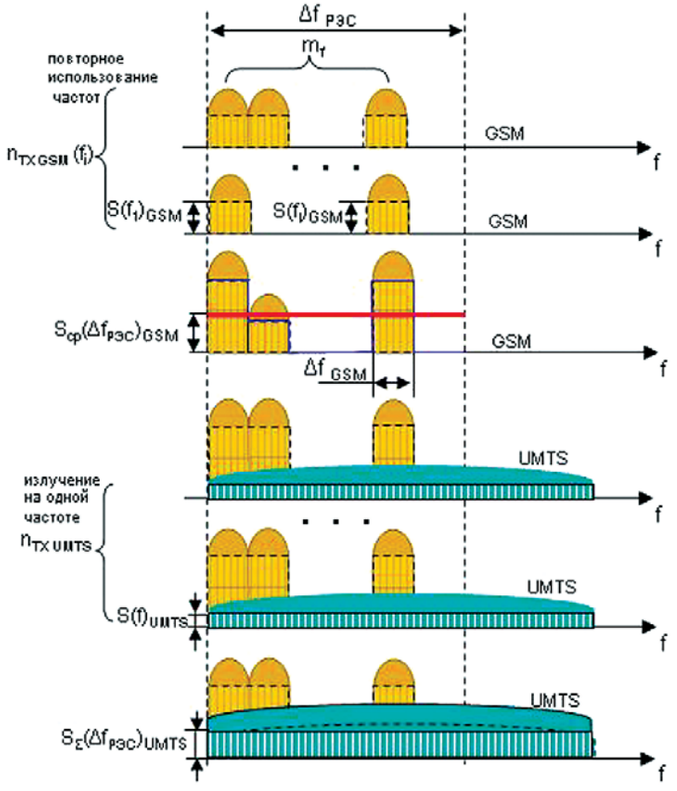


Рис. 2. Спектральные плотности мощности излучения БС GSM и UMTS

Поскольку характер энергетических спектров сигнала у рассматриваемых систем различен, целесообразно сравнивать энергетику на уровне спектральных плотностей мощности излучения базовых станций (БС) GSM и UMTS. Соотношение этих плотностей показано на рис. 2, где $\Delta f_{РЭС}$ — полоса пропускания приемника РЭС — потенциального рецептора помех, т.е. ширина частотного канала РЭС. Для диапазона частот 900 МГц в качестве такого РЭС может рассматриваться система воздушной радионавигации и посадки (РСБН).

Решение задачи. Аналитические выражения, описывающие указанные спектральные плотности, приведены ниже:

— средняя суммарная спектральная плотность мощности излучения передатчиков БС GSM в полосе частот $\Delta f_{РЭС}$

$$S_{ср}(\Delta f_{РЭС})_{GSM} = \frac{1}{m_f} \sum_{i=1}^{m_f} S(f_i)_{GSM}, \quad mf = \left\lfloor \frac{\Delta f_{РЭС}}{\Delta f_{GSM}} \right\rfloor$$

[x] — целая часть числа;

$$S(f_i)_{GSM} = \frac{P_{TX\,GSM}}{\Delta f_{GSM}} = \frac{P_{TX\,GSM}(1 - b_{iGSM})\ n_{TX\,GSM}(f_i)}{\Delta f_{GSM}};$$

$$S_{ср}(\Delta f_{РЭС})_{GSM} = \frac{1}{m_f} \sum_{i=1}^{m_f} \frac{P_{TX\,GSM}(1 - b_{iGSM})\ n_{TX\,GSM}(f_i)}{\Delta f_{GSM}}; \qquad (1)$$

— суммарная спектральная плотность мощности излучения передатчиков БС UMTS равномерна по всей полосе $\Delta f_{РЭС}$ ввиду псевдошумового характера сигнала и равна

$$S_{\Sigma}(\Delta f_{РЭС})_{UMTS} = \frac{P_{TxS\,UMTS}}{\Delta f_{UMTS}} = \frac{P_{TxUMTS}\ (1 - b_{UMTS})}{\Delta f_{UMTS}} \cdot n_{TxUMTS}\ N_{UMTS},\ \Delta f_{UMTS} \neq \Delta f_{РЭС}, \qquad (2)$$

где $P_{TxS\,GSM}$, $P_{TxS\,UMTS}$ — суммарные мощности передатчиков БС GSM и UMTS соответственно; N_{UMTS} — количество площадок, на которых планируется установка передатчиков UMTS; $n_{Tx\,UMTS}$ — количество передатчиков на площадке UMTS; $n_{Tx\,GSM}(f_i)$ — количество передатчиков GSM, создававших помехи РСБН на одной повторяемой частоте f_i, $i = 1...m_f$; m_f — количество частот в полосе $\Delta f_{РЭС}$, на которых создавались помехи РСБН от передатчиков GSM; $b_{iGSM} = \Delta P_{TxGSM}/P_{TxGSM}$, $0 \le b_{iGSM} < 1$, — степень ранее введенного ограничения мощности передатчиков GSM на частоте f_i по условиям ЭМС с РСБН; $b_{UMTS} = \Delta P_{TxUMTS}/P_{TxUMTS}$, $0 \le b_{UMTS} < 1$, — степень возможного ограничения мощности передатчиков UMTS по условиям ЭМС с РСБН.

Оценим степень увеличения мощности потенциальной помехи от сети UMTS в полосе частот, равной $\Delta f_{РЭС} = \Delta f_{GSM} \times m_f$, в виде следующего отношения

$$h = \frac{P_{S\ пом\ UMTS}(\Delta f_{РЭС})}{P_{S\ пом\ GSM}(\Delta f_{РЭС})} = \frac{S_{\Sigma}(\Delta f_{РЭС})_{UMTS}\ \Delta f_{РЭС}}{S_{ср}(\Delta f_{РЭС})_{GSM}\ \Delta f_{РЭС}} = \frac{\frac{P_{TxUMTS}}{\Delta f_{UMTS}}(1 - b_{UMTS})\ n_{TxUMTS}\ N_{UMTS}}{\frac{1}{m_f}\sum_{i=1}^{m_f}\frac{P_{TX\,GSM}}{\Delta f_{GSM}}(1 - b_{iGSM})\ n_{TxGSM}(f_i)} =$$

$$= \frac{P_{TxUMTS}}{P_{TxGSM}}(1 - b_{UMTS})\frac{\Delta f_{GSM}}{\Delta f_{UMTS}} \cdot \frac{n_{TxUMTS}\ N_{UMTS}}{\frac{1}{m_f}\sum_{i=1}^{m_f}(1 - b_{iGSM})\ n_{TxGSM}(f_i)} \qquad (3)$$

где $P_{S\ пом\ GSM}(\Delta f_{РЭС})$, $P_{S\ пом\ UMTS}(\Delta f_{РЭС})$ — суммарная мощность помех от сетей GSM и UMTS в полосе $\Delta f_{РЭС}$ соответственно.

Очевидно, что условием сохранения ЭМС по критерию энергетической эквивалентности является соотношение вида $h \le 1$, в соответствии с которым суммарная мощность помехи от сети UMTS в полосе частот $\Delta f_{РЭС}$ не превышает эквивалентную мощность помехи, ранее создаваемой для РСБН сетью GSM в этой полосе, т.е.

$$\frac{P_{TX\,UMTS}}{P_{TX\,GSM}}(1 - b_{UMTS})\frac{\Delta f_{GSM}}{\Delta f_{UMTS}} \cdot \frac{n_{TX\,UMTS}\ N_{UMTS}}{\frac{1}{m_f}\sum_{i=1}^{m_f}(1 - b_{iGSM})\ n_{TX\,GSM}(f_i)} \le 1. \qquad (4)$$

Причем, если помеховое влияние сети GSM оказывалось по нескольким частотно-кодовым каналам (ЧКК) РСБН, то достаточно оценить условие энергетической эквивалентности по одному ЧКК с наибольшим уровнем помехового воздействия.

Заметим, что входящий в (4) параметр $n_{TXGSM}(f_i)$ характеризует количество передатчиков GSM, излучающих на одной помеховой частоте f_i. По условиям повторного использования радиочастот в сети GSM каждый из этих передатчиков находится на одной из площадок, входящих в состав отдельного кластера. Следовательно, количество передатчиков GSM с повторяемой частотой f_i будет зависеть от общего количества площадок GSM (N_{GSM}) и коэффициента повторного использования частот в сети (K). С учетом этого при совмещенных площадках, когда $N_{GSM} = N_{UMTS}$, имеем

$$n_{TxGSM}(f_i) = \frac{N_{GSM}}{K_i} = \frac{N_{UMTS}}{K_i}. \qquad (5)$$

Однако, на практике могут встретиться ситуации, когда частота f_i может быть помеховой не во всех кластерах из-за того, что разные кластеры в сети по-разному удалены от РЭС — рецептора помех. В этом случае для каждой поме-

ховой частоты f_i могут быть разные значения коэффициента K, поэтому в выражении (5) использованы парциальные коэффициенты с индексом i (K_i).

Следовательно,

$$\frac{P_{TXUMTS}}{P_{TX\,GSM}}\,(1-b_{UMTS})\,\frac{\Delta f_{GSM}}{\Delta f_{UMTS}}\,\frac{n_{TXUMTS}}{\frac{1}{m_f}\sum_{i=1}^{m_f}(1-b_{iGSM})/K_i}\le 1. \qquad (6)$$

Полученное условие (6) позволяет оценить допустимое количество передатчиков UMTS (n_{TxUMTS}) на одной площадке, при котором не будет нарушена энергетическая эквивалентность

$$n_{TxUMTS}\le\frac{P_{Tx\,GSM}}{P_{TxUMTS}}\,\frac{1}{(1-b_{UMTS})}\,\frac{\Delta f_{UMTS}}{\Delta f_{GSM}}\,\frac{m_f}{\sum_{i=0}^{m_f}(1-b_{iGSM})/K_i}=$$
$$=\frac{P_{TxGSM}}{P_{TxUMTS}}\,\frac{1}{(1-b_{UMTS})}\,\frac{\Delta f_{UMTS}}{\Delta f_{PЭС}}\,\frac{m_f}{\sum_{i=1}^{m_f}(1-b_{iGSM})/K_i}. \qquad (7)$$

Соотношение (7) позволяет определить условие, при котором сохраняется энергетическая эквивалентность сети GSM в полосе частот шириной 5 МГц, выделенной для создания фрагмента сети UMTS. Это соотношение является универсальным и может быть использовано по отношению к другим РЭС при выборе соответствующего значения $\Delta f_{РЭС}$. Например, его можно использовать при оценке условий энергетической эквивалентности по отношении к РЭС фиксированной службы в диапазоне частот 1800 МГц.

Следует заметить, что при расчетах в соответствии с (7) в качестве исходных параметров могут быть использованы не только мощности передатчиков (P_{TxGSM} и P_{TxUMTS}), но и значения ЭИИМ при разных коэффициентах усиления и диаграммах направленности используемых и планируемых типов антенн.

Соотношение (7) можно привести к частному виду, соответствующему реальному случаю, когда

— полные мощности передатчиков БС UMTS и GSM равны ($P_{TX\,UMTS} = P_{TX\,GSM}$);

— ширина частотного канала UMTS равна 5 МГц (Δf_{UMTS} = 5 МГц);

— ширина частотно-кодового канала РСБН равна 0,7 МГц ($\Delta f_{РЭС}$ = 0,7 МГц);

— все передатчики на каждой помеховой частоте f_i имеют одинаковые ограничения по мощности ($K_i = K$, $b_{i\,GSM} = b_{GSM}$).

Проведя несложные преобразования (7), получим

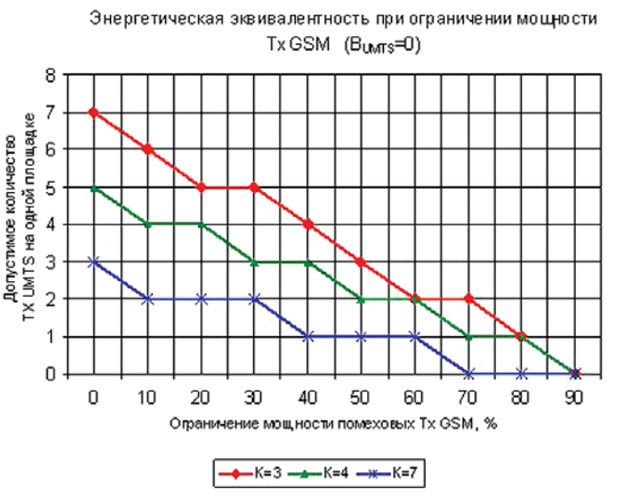


Рис. 3. Результаты оценки допустимого количества передатчиков UMTS на одной площадке

$$n_{Tx\ \ UMTS}\le 7{,}17\,\frac{m_f\,(1-b_{GSM})}{K\quad(1-b_{UMTS})}= \qquad (8)$$
$$=21{,}42\,\frac{(1-b_{GSM})}{K\ \ (1-b_{UMTS})}.$$

На рис. 3 приведены результаты расчета по формуле (8) для различных сценариев.

Эти результаты позволяют оценить и гибко спланировать для конкретных условий возможную архитектуру создаваемой радиосети UMTS. К примеру, если для каких-то условий допустимое количество передатчиков на площадке UMTS окажется недостаточным, то увеличить это количество можно за счет некоторого уменьшения мощности излучения этих передатчиков, сохраняя таким образом энергетическую эквивалентность. При этом необходимо предварительно оценить эквивалентность пропускной способности ячейки UMTS [3]. Для примера на рис. 4 приведена зависимость требуемого ограничения мощности передатчиков UMTS от степени ранее введенного ограничения мощности передатчиков GSM. Эта зависимость получена для K = 7, как наиболее худшего случая, и для минимально необходимого количества передатчиков UMTS в 3-секторной соте, т.е. для $n_{TX\,UMTS}$ = 3.

В заключение следует заметить, что зачастую логика подходов к решению подобных задач на инженерном, а тем более на менеджерском (административном) уровне, не всегда позволяет найти решения, полученные на основе теории. Так, полученное в статье решение,

Рис. 4. Выполнение условия энергетической эквивалентности за счет ограничения мощности передатчиков UMTS

на первый взгляд, может вызвать ряд сомнений. К примеру, почему не следует оценивать энергетическую эквивалентность на других помеховых частотах f_j, отличных от f_i ($j \neq i$), почему для частного случая (8), когда все передатчики на каждой помеховой частоте GSM f_i ($i=1...m_f$) имеют одинаковые ограничения, энергетическая эквивалентность определяется лишь значением этого ограничения и количество помеховых передатчиков в явном виде не учитывается, и наконец, почему энергетическая эквивалентность (6) не зависит в явном виде от большого количества передатчиков UMTS в сети. Поэтому для понимания (7) рассмотрим на примере решение задачи для наиболее общего случая.

Пусть наибольшему помеховому воздействию со стороны сети GSM подвергается k-й частотно-кодовый канал РСБН, количество помеховых частотных каналов GSM равно $m_f = Df_{РЭС}/Df_{GSM} = 0,7/0,2 = 3$. При этом на частоте f_1 ограничения мощности излучения передатчиков GSM составляет 25% ($b_{1GSM} = 0,25$), на f_2 — 60% ($b_{2GSM} = 0,6$), на f_3 — 95% ($b_{3GSM} = 0,95$). Коэффициенты повторения частот f1 и f2 равны $K_1 = K_2 = 3$. Количество передатчиков GSM с частотой f_3 и большими ограничениями мощности равно 10 при общем количестве площадок (БС) в сети, равном 300, т.е. парциальный коэффициент повтора равен $K_3 = 300/10 = 30$.

Найти в соответствии с (7) допустимое количество передатчиков UMTS на каждой площадке. Мощности передатчиков GSM и UMTS равны, антенны по типу и азимуту излучения идентичны.

$$n_{TxUMTS} \leq \frac{1}{(1 - b_{UMTS})} \cdot 7,14 \cdot [(1 - 0,25)/3 + (1 - 0,6)/3 + (1 - 0,9)/30] = \frac{7,14}{(1 - b_{UMTS})} \cdot \left(\frac{0,75}{3} + \frac{0,4}{3} + \frac{0,05}{30}\right) = \frac{2,73}{(1 - b_{UMTS})} . \quad (9)$$

Полученный результат свидетельствует о том, что без введения ограничений по мощности передатчиков UMTS ($b_{UMTS} = 0$) допустимое их количество на каждой площадке равно двум.

При необходимости увеличения количества передатчиков UMTS на площадке необходимо ввести ограничения по мощности их излучения для сохранения энергетической эквивалентности.

Оценим эти ограничения (b_{UMTS}) для количества передатчиков UMTS, равного трем. Нетрудно рассчитать значение параметра b_{UMTS} в выражении (9) при $n_{TxUMTS} = 3$. Результат такого расчета равен 9%, т.е. при размещении 3 передатчиков на каждой площадке необходимо ограничить мощность излучения каждого из них, как минимум, на 9%.

При этих условиях мощность излучения передатчиков должна составлять не более 18,2 Вт (при полной мощности 20 Вт).

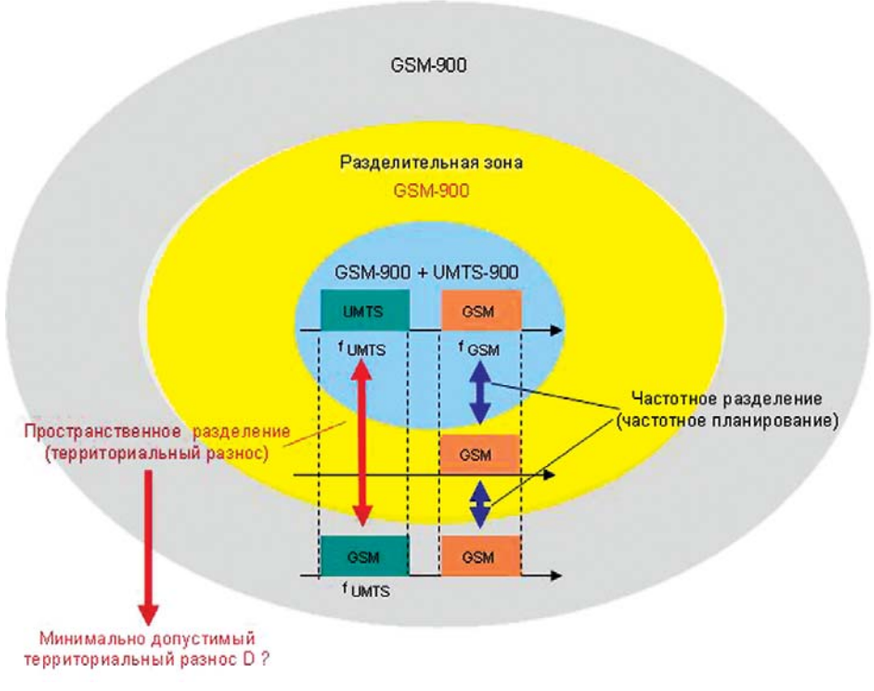


Рис. 5. Общий сценарий к задаче 2

Задача 2

Исходные условия. Суть задачи проиллюстрирована на рис. 5 и состоит в следующем. При наличии локальной совмещенной сети GSM-900/UMTS-900 существуют 3 фрагмента с разным частотным ресурсом:

— сеть UMTS с частотным ресурсом f_{UMTS};

— сеть GSM в составе совмещенной сети с частотным ресурсом f_{GSM};

— общая сеть GSM за пределами совмещенной сети (ранее существовавшая) с общим частотным ресурсом $f = f_{UMTS} + f_{GSM}$.

При строительстве такой гибридной сети необходимо исключить взаимное влияние совмещенной и общей сетей в полосе совместно используемого частотного ресурса. При этом взаимное влияние сетей GSM может быть устранено традиционным методом частотного планирования с повторным использованием частот и, следовательно, территориальный разнос радиосредств указанных сетей не требуется. Взаимное влияние сети UMTS и обшей сети GSM может быть устранено лишь за счет территориального разноса их радиосредств. Величина такого разноса и будет соответствовать размеру разделительной зоны.

Как было показано в [1], в условиях совместного функционирования сетей GSM и UMTS наибольшее помеховое влияние оказывает сеть UMTS, а именно, существенное влияние на базовую станцию GSM оказывает большое количество абонентских терминалов UMTS.

Таким образом, необходимо найти взаимное удаление ближайших друг к другу сот в сети UMTS-900 и в общей сети GSM-900, в которых совместно используется частотный ресурс f_{UMTS}. При этом важно отметить два обстоятельства. Во-первых, под удалением сот понимается расстояние D между их центрами, т.е. местами расположения базовых станций (рис. 6). Такое определение удобно использовать при планировании сетей. Во-вторых, для оценки же степени влияния сетей используется удаление d ближайших базовых станций на границе общей сети GSM-900 от абонентских терминалов на границе сети UMTS-900, которые находятся на краю зоны обслуживания сот с радиусом r.

Решение задачи. С учетом отмеченного, запишем

$$D = d + r. \quad (10)$$

В табл. 2 приведены результаты статистического моделирования с учетом соотношения (10).

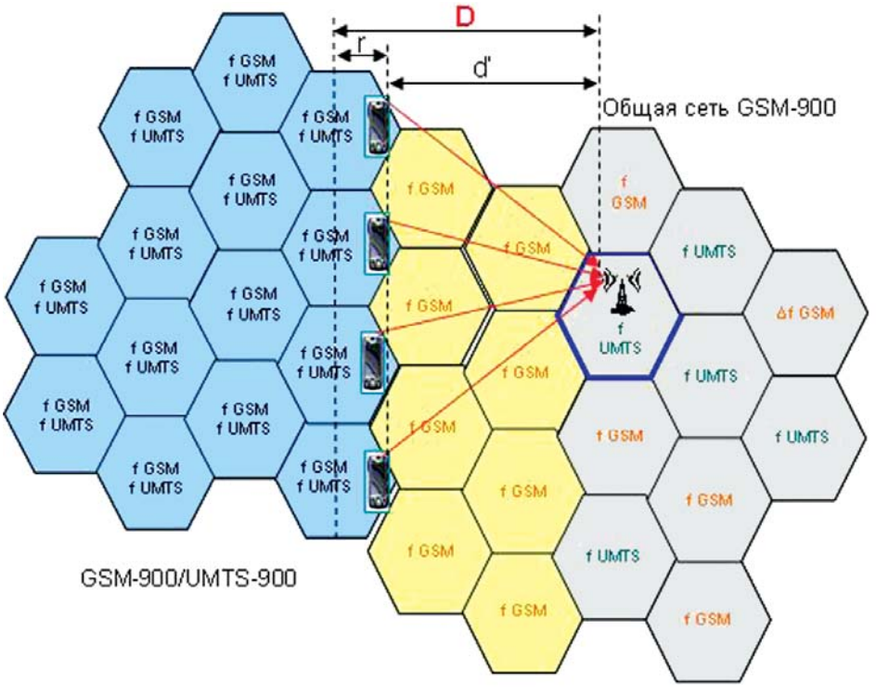


Рис. 6. Разделительная зона

Таблица 2

Размер разделительной зоны

Кол-во АТ UMTS	r, км	d', км	Вероятность влияния	Ď, км
3	2,5	5	$6\cdot10^{-2}$	7,5
	2,5	7,5	$4,5\cdot10^{-2}$	10
10	2,5	7,5	$6\cdot10^{-2}$	10
	2,5	10	$5,3\cdot10^{-2}$	12,5
30	2,5	7,5	$8,4\cdot10^{-2}$	10
	2,5	10	$6,4\cdot10^{-2}$	12,5
50	2,5	7,5	$1\cdot10^{-1}$	10
	2,5	10	$7,4\cdot10^{-2}$	12,5

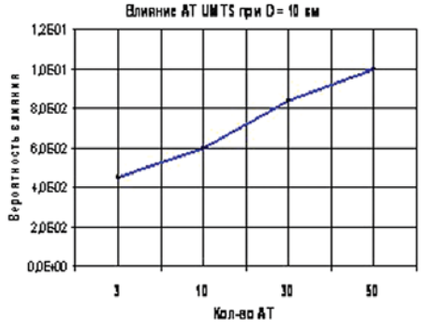


Рис. 7. Зависимость вероятности помехового влияния от количества АТ в сети UMTS

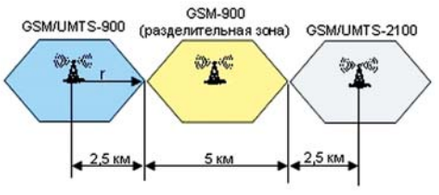


Рис. 8. Структура сети с разделяемой зоной

Как видно из таблицы, вероятность помехового влияния в значительной степени зависит от количества активных абонентских терминалов (АТ) в сети UMTS. Такая зависимость для территориального разноса сот D = 10 км приведена на рис. 7.

Далее из таблицы следует, что для реальной сети UMTS с 30...50 активными абонентскими терминалами допустимая вероятность помехового влияния на уровне 10^{-2} может быть обеспечена при территориальном разносе ближайших друг к другу сот разделяемых сетей, равном 10...12,5 км. На рис. 8 в качестве примера приведен фрагмент сети с разделительной зоной размером 10 км.

Заключение

Решение поставленных в статье задач дает методологию и позволяет оценить при планировании сетей UMTS-900 допустимое количество передатчиков в сети на одной площадке, а также определить размер разделительной зоны, которая необходима для исключения помехового влияния сети UMTS на общую сеть GSM в совместной полосе частот.

Литература

1. **В.Г. Скрынников.** Оценка условий ЭМС в совмещенных сетях GSM/UMTS. — Мобильные Телекоммуникации, 2008. — № 10.

2. **В.Г. Скрынников.** Повышение эффективности использования радиочастотного ресурса в сетях GSM/UMTS в диапазонах частот 900 МГц и 1800 МГц. — Мобильные Телекоммуникации, 2009. — №1.

3. **В.Г. Скрынников.** Предварительная оценка параметров сети UMTS/HSDPA. — Электросвязь, 2009. — №3

4. **В.Г. Скрынников.** Предварительная оценка параметров сети UMTS/HSDPA при статическом распределении мощности базовой станции. — Мобильные Телекоммуникации, 2008. — №8.

5. **В.Г. Скрынников.** Оценка условий ЭМС при учете особенностей радиоинтерфейса системы UMTS. — T-Comm, 2008. — №2.

Целевая функция структурно-параметрического синтеза конструктивной системы модулей радиоэлектронных средств

Ключевые слова:
Структурно-параметрический синтез, радиоэлектронные средства

Кондрашов А.С.,
к.т.н.

Для современных многоуровневых несущих конструкций (НК) радиоэлектронных средств (РЭС) характерна иерархическая структура построения, в которой модули нижестоящих уровней размещаются в модулях вышестоящих уровней [1]. Выбор варианта реализации проектируемой системы конструктивных модулей на ранних стадиях проектирования удобно проводить на основании сравнения стоимости изготовления того или иного варианта системы и коэффициента использования объема синтезированной совокупности конструктивных модулей различных уровней конструктивной иерархии. Именно стоимость изготовления позволяет комплексно учесть уровень техники и технологии производства и объективно выбрать тот вариант системы НК, который обеспечит наименьшие затраты и большую конкурентоспособность изделия в целом. А коэффициент использования объема конструктивного модуля позволяет достаточно объективно судить о достигнутом уровне функциональной плотности РЭС, размещаемых в проектируемых НК.

Предлагаемая в настоящей статье практически целесообразная целевая функция, пригодная для структурного и параметрического синтеза системы НК, имеет следующий вид.

$$F(\vec{X},\vec{Z}) = a_1 K^V + a_2 K^C \to \min, \quad (1)$$

где

$$K^V = \sum_{k=1}^{K} \sum_{q=1}^{Q(k)} \left(1 - \frac{\sum_{q'=1}^{Q'(k-1)} N_{q'}^{k-1} L_{q'}^{k-1} B_{q'}^{k-1} H_{q'}^{k-1}}{L_q^k B_q^k H_q^k} \right) \quad (2)$$

$$K^C = \sum_{k=1}^{K} \sum_{q}^{Q(k)} \left(C_q^k + \sum_{q'=1}^{Q'(k-1)} N_{q'}^{k-1} C_{q'}^{k-1} \right) \Big/ C_{q\,(max)}^k \quad (3)$$

Целевая функция $F(\vec{X},\vec{Z})$ с весовыми коэффициентами $a_1, a_2 \in [0,1]$, выбираемыми пользователем в зависимости от конкретных условий синтеза, объединяет два показателя качества: K^V и K^C представляющими из себя суммированные по всем уровням конструктивной иерархии и видам типоразмеров модулей НК коэффициенты использования объема конструктивных модулей и нормализованных затрат на их изготовление для всего синтезированного ряда модулей НК. Таким образом, K^V определяется как сумма разностей единицы и отношений суммарного объема совокупности конструктивных модулей различных типоразмеров k-1 уровня конструктивной иерархии, размещаемых в проектируемом модуле НК k-го уровня конструктивной иерархии к общему объему этого модуля НК. При этом уровень конструктивной иерархии обозначен через $k \in [1,K]$, а индекс типоразмера конструктивного модуля k-го уровня конструктивной иерархии через $q \in [1,Q(k)]$. Через $q' \in [1,Q'(k)]$ обозначен индекс типоразмера совокупности конструктивных модулей k-1 уровня конструктивной иерархии, а через N_q^{k-1} число этих модулей НК, размещаемых в проектируемом модуле k-го уровня конструктивной иерархии. При этом объем конструктивного модуля определяется исходя из его габаритных размеров, обозначенных через L_q^{k-1}, H_q^{k-1}, B_q^{k-1} для конструктивного модуля q'-го типоразмера k-1 уровня конструктивной иерархии и L_q^k, H_q^k, B_q^k для конструктивного модуля q-го типоразмера k-го уровня конструктивной иерархии.

Показатель качества K^C обозначает затраты на разработку и производство синтезируемой системы конструктивных модулей. Затраты представлены в виде дроби где в числителе суммируются затраты на разработку и производство конструктивного модуля q-го типоразмера k-го уровня конструктивной иерархии (C_q^k) и суммарные затраты на разработку и производство совокупности размещаемых в нем конструктивных модулей q'-го типоразмера k-1 уровня конструктивной иерархии (C_q^{k-1}). При этом суммирование затрат для размещаемых модулей проводится по всей номенклатуре их типоразмеров $q' \in [1,Q'(k-1)]$, с учетом числа конструктивных модулей q'-го типоразмера (N_q^{k-1}). В знаменателе, исходя из условий проектирования и производства, задается максимальный уровень затрат на разработку и производство конструктивного модуля q-го типоразмера k-го уровня конструктивной иерархии ($C_{q(max)}^k$). Выбор в качестве одного из показателей качества целевой функции стоимостной зависимости обусловлен актуальным требованием обеспечения уменьшения затрат и повышения конкурентоспособности РЭС в целом.

Анализируя приведенную целевую функцию (1), можно сделать вывод, что результат, выдаваемый целевой функцией, является безразмерным. И, кроме этого, значения K^V и K^C для каждого из конструктивных модулей q-го типоразмера k-го уровня конструктивной иерархии, без учета величин весовых коэффициентов, лежат в диапазоне от 0 до 1. Критерии K^V и K^C наиболее эффективны при одновременном синтезе совокупности структурных модулей НК в условиях существования ограничений на параметры конструктивного модуля высшего уровня конструктивной иерархии (например, на габаритные размеры стойки, устанавливаемые стандартами МЭК). При отсутствии подобных ограничений синтез НК предпочтительно осуществлять, начиная с оптимизации модуля НК первого (блок, ТЭЗ) или нулевого (КП) уровня конструктивной иерархии. Для случая КП, в качестве размещаемых конструк-

тивных модулей, выступают входящие в ее состав ИЭТ. Площадь КП и максимальная высота, располагаемых на ней ИЭТ, определяют объем этого модуля.

Данная целевая функция приведена для случая синтеза перспективной конструктивной системы НК. В случае (для производителя РЭС, а не НК) если требуется с ее помощью оценить целесообразность применения той или иной покупаемой конструктивной системы в качестве затрат должны фигурировать затраты на закупку соответствующих конструктивных модулей и максимально допустимый уровень этих затрат.

Весовые коэффициенты, присутствующие в целевой функции, необходимы для достижения желаемого баланса между стоимостью изготовления и компоновочной емкостью проектируемых НК. С точки зрения затрат на производство, для производителя изготовляющего НК серийно на специализированном производстве, выгодно иметь ограниченный ряд типоразмеров [2,3]. При этом, чем меньшее количество типоразмеров модулей НК различных уровней конструктивной иерархии будет иметь синтезируемая конструктивная система, тем выше серийность изготовления входящих в ее состав модулей, а значит и себестоимость их изготовления. Однако при этом, из-за несовпадения требуемых типоразмеров и имеющихся в наличии, неизбежно снижение коэффициента использования объема конструктивных модулей при размещении в них функциональных устройств РЭС. И наоборот, чем больше типоразмеров модулей НК имеет конструктивная система, тем выше вероятность подобрать типоразмер адекватный объему, необходимому для размещения функционального устройства РЭС. Однако, при этом происходит рост стоимости изготовления такой конструктивной системы НК.

Таким образом, в предлагаемая целевая функция позволяет комплексно учесть наиболее общие и емкие показатели качества принимаемого технического решения по синтезу конструктивной системы многоуровневых НК. В частности, комплексный коэффициент использования объема всего ряда конструктивных модулей перспективных НК, определяет качество принятого решения по размещению в них планируемой техническим заданием совокупности функциональных устройств РЭС. А коэффициент приведенной стоимости позволяет в существенной мере напрямую учитывать конкурентоспособность и рентабельность производства системы НК еще на ранних стадиях проектирования. Проведение автоматизированного структурно-параметрического системного синтеза многоуровневых НК РЭС, на основе предлагаемой целевой функции отвечает постоянной тенденции постоянного повышения функциональной емкости размещаемых в НК РЭС при одновременном обеспечении надежности работы и минимизации затрат на разработку и производство.

Литература

1. **Ненашев А.П.** Конструирование радиоэлектронных средств: Учеб. для радиотехнич. спец. вузов. — М.: Высш. шк., 1990. — 432 с.

2. **Кондрашов А.С.** Алгоритм выбора оптимальных типоразмеров коммутационных плат при разработке несущих конструкций для аппаратуры связи // Синтез и анализ алгоритмов оптимальной обработки сигналов: Сб. науч. тр. учеб. завед. связи / СПб. ГУТ. — СПб, 1993. — №158. — С.94-99.

3. **Кондрашов А.С.** Математическая постановка задачи выбора оптимальных габаритов типовых элементов замены стоечной аппаратуры связи // Синтез и анализ алгоритмов оптимальной обработки сигналов: Сб. науч. тр. учеб. завед. связи / СПб. ГУТ. — СПб, 1993. — №159. — С.94-99.

25 прогнозов главного футуролога Cisco

В связи с 25-летием Cisco главный футуролог консалтингового подразделения Cisco IBSG Дэйв Эванс обнародовал свой прогноз дальнейшего развития технологий. Дэйв — частый гость телевизионных каналов и радиостанций США, его прогнозы охотно публикуют такие издания, как газета "Файненшл таймс" и журнал "Форбс".

По его мнению:

• К 2029 г. за 100 долл. можно будет купить систему хранения емкостью в 11 петабайт. Такого объема электронной памяти будет достаточно, чтобы круглосуточно проигрывать видео DVD-качества в течение 600 с лишним лет.

• В предстоящие 10 лет скорость передачи данных в домашних сетях увеличится в 20 раз.

• К 2013 г. ежемесячный объем трафика в беспроводных сетях составит 400 петабайт (сегодня весь мировой сетевой трафик составляет 9 экзабайт в месяц).

• К концу 2010 г. на каждого жителя планеты будет приходиться по миллиарду транзисторов стоимостью одна миллионная американского цента каждый.

• Интернет эволюционирует до такой степени, что сможет поддерживать мгновенные коммуникации независимо от расстояния.

• Первый коммерческий квантовый компьютер появится к середине 2020 г.

• К 2020 г. персональный компьютер стоимостью в 1 тыс. долл. по своей вычислительной мощности сравняется с человеческим мозгом.

• К 2030 г. вычислительная мощность персонального компьютера стоимостью в 1 тыс. долл. будет равна мыслительной способности населения целого поселка.

• К 2050 г., если к тому времени население нашей планеты составит 9 млрд людей, мощность вычислительного устройства стоимостью в 1 тыс. долл. будет равна вычислительной мощности всего человечества.

• Сегодня мы знаем 5% того, что нам станет известно через 50 лет. Другими словами, 95% знаний, которые будут доступны людям к 2060 г., станут результатом открытий, сделанных в предстоящие 50 лет.

• В ближайшие 2 года объем информации в нашем мире будет ежегодно увеличиваться в шесть раз, а объем корпоративных данных в тот же период будет ежегодно возрастать в 50 раз.

• К 2015 г. Google проиндексирует примерно 775 млрд. страниц контента.

• К 2015 г. человечество будет ежегодно создавать контент, объем которого в 92,5 млн. раз превышает объем информации, хранящейся в библиотеке Конгресса США .

• К 2020 г. каждый житель нашей планеты будет в среднем хранить 130 терабайт персональных данных (сегодня этот объем равен 128 гигабайтам).

• К 2015 г. объем скачиваемых кинофильмов и файлов, которыми обмениваются между собой пользователи, возрастет до 100 экзабайт, что в 5 млн. раз превышает объем информации, хранящейся в библиотеке Конгресса США.

• К 2015 г. повсеместно распространится видеосвязь, и она будет генерировать 400 экзабайт трафика, что в 20 млн. раз превышает объем информации, хранящейся в библиотеке Конгресса США.

• К 2015 г. объем данных, которые будут генерировать телефонная связь, Интернет, электронная почта, фото- и музыкальные файлы, составит 50 экзабайт.

• В течение двух следующих лет объем информации во Всемирной сети будет удваиваться каждые 11 часов.

• К началу 2010 г. к Сети окажутся подключены 35 млрд. различных устройств, т.е. почти по 6 устройств на каждого жителя нашей планеты.

• К 2020 г. в Интернете будет работать больше устройств, чем людей.

• С внедрением протокола IPv6 в Интернете появится такое количество электронных адресов, что каждую из известных человечеству звезд во вселенной можно будет снабдить 4,8 триллионами адресов.

• К 2020 г. каждое электронное устройство будет иметь универсальное приложение для перевода с других языков.

• Через 5 лет любая поверхность сможет выполнять функции дисплея.

• К 2025 г. появятся первые случаи телепортации на уровне частиц.

• К 2030 г. станет возможным вживление искусственной ткани в человеческий мозг.

Исследование эффективности управления мощностью подвижной станции системы стандарта IS-2000 в многолучевом канале

Исследуется возможность использования многобитовых команд управления мощностью в обратной линии. Предлагается способ передачи таких команд по прямой линии. Исследуется эффективности такой системы управление мощностью. Получены графики зависимости BER и FER от CIR для условий связи, предусматриваемых стандартом IS-2000 для 1xRTT. Сделан анализ.

Ключевые слова:
Стандарт IS-2000, технология кодового разделения каналов, CDMA

Шинаков Ю.С.,
Заведующий кафедрой радиотехнических систем МТУСИ, д.т.н., профессор, академик МАС

Ахмат М.С.,
аспират МТУСИ
ahmat01@mail.ru

Введение

Полноценная эксплуатация систем с технологией кодового разделения каналов (CDMA) ставит перед разработчиками ряд проблем, одна из которых — необходимость быстрой прецизионной автоматической регулировки мощности (АРМ) передатчиков подвижных станций (ПС). Поскольку рабочие каналы в системе CDMA используют единый частотный ресурс, для успешного разделения и обработки сигналов ПС на базовой станции (БС) мощности сигналов рабочих каналов необходимо привести к единому уровню. В противном случае сильные сигналы одних каналов будут подавлять слабые сигналы других, что резко ограничит пропускную способность обратного канала (ПС-БС) и системы связи в целом. Задача управления мощностью передатчика ПС имеет целью обеспечение номинального (минимально допустимого) уровня сигнала на входе приемника БС от каждой абонентской станции из числа одновременно работающих в данной соте. При идеальном управлении сигнал каждой ПС будет принят приемником БС с одним и тем же уровнем независимо от местоположения ПС и потерь распространения. Если передатчики всех абонентских станций в пределах соты управляются таким образом, то суммарная мощность сигнала, принимаемого приемником БС, будет равна номинальной мощности принимаемого сигнала, умноженной на количество подвижных станций [1].

Если сигнал ПС имеет уровень, меньший номинального, то вероятность ошибки при выделении информации данного абонента оказывается слишком высокой и качество связи недопустимо низкой. Если сигнал ПС имеет слишком высокий уровень, то прием сигнала данной ПС выполняется нормально, однако при этом увеличиваются помехи для приема сигналов всех остальных подвижных станций, также работающих в данной полосе частот. Это может привести к неудовлетворительной работе других абонентов и, следовательно, к снижению емкости системы. Таким образом, качество работы АРМ ПС в значительной мере влияет на пропускную способность сети сотовой связи с кодовым разделением каналов.

Система управления мощностью систем подвижной станции в сети стандарта IS-2000

В соответствии с рекомендацией стандарта IS-2000 [2] управление мощностью ПС осуществляется открытой, замкнутой и внешней петлями. Управление мощностью открытой петлей устанавливает излучаемую мощность на основе значения мощности сигнала БС, принимаемого мобильной станцией, т.е. управление мощностью открытой петлей компенсирует медленно меняющиеся потери распространения на трассе от БС до ПС. Управление мощностью замкнутой петлей компенсирует изменение уровня сигнала из-за наличия быстрых замираний, а также из-за точности управления мощностью открытой петлей. Управление мощностью внешней петлей реализуется обычно с целью сохранения требуемого значения частости приема ошибочных кадров и устанавливает пороговое значение для управления замкнутой петлей.

Мощность передатчика ПС физически может устанавливаться двумя способами:

а) изменением коэффициента передачи усилителя мощности радиосигнала;

б) изменением уровня модулирующего сигнала соответствующего кодового канала.

При управлении мощностью с помощью открытой петли излучаемая мощность мобильного терминала устанавливается в соответствии с мощностью принимаемого сигнала БС. Как отмечается в патенте фирмы Qualcomm управление мощностью открытой петлей и автоматическая регулировка усиления приемника ПС реализуются аналоговой цепью БС. При этом измеряется мощность сигнала на входе приемника ПС. Результат измерения используется для установки как коэффициента усиления УПЧ приемника, так и для установки коэффициента

усилителя мощности передатчика ПС. Таким образом, роль управления мощностью ПС с помощью открытой петли состоит в том, чтобы установить грубо уровень мощности, излучаемой передатчиком ПС. Отмечается, что значение ошибки управления мощностью открытой петлей должно находится в диапазоне от 0 до 8 дБ.

Управление мощностью открытой петлей является в основном функцией ПС. Однако БС обеспечивает реализацию этой функции при номинальном значении эффективно излучаемой мощности (ЭИМ). Если же БС ведет передачу с ЭИМ, отличной от номинального значения, то эта БС должна информировать своих абонентов так, чтобы ПС не вели передачу с уровнем излучаемой мощности, ниже или выше требуемого.

При управлении мощностью замкнутой петлей для измерения качества обратной линии в приемнике БС используется пилот-канал [1]. Излучаемая мощность ПС может устанавливаться в соответствии со значениями следующих оценок, формируемых в приемнике БС:

а) мощности принимаемого сигнала;

б) отношения CIR мощности сигнала к мощности интерференции и шума;

в) вероятности ошибки при приеме одного бита.

Подход "а" был использован на раннем этапе в экспериментальной широкополосной системе CDMA Японии. Позднее этот подход к установке излучаемой ПС мощности заменен подходом "б". Фирма Qualcomm использует одновременно подходы "б" и "в". Для канала с аддитивным гауссовским белым шумом вероятность ошибки может быть вычислена при известном значении отношения сигнал/шум. Однако для канала с внутрисистемной интерференцией соотношение между вероятностью ошибки и отношением CIR не является столь определенным.

Хорошо известен комбинированный подход, состоящий в следующем: формируется оценка вероятности ошибки при приеме одного символа (BER), которая используется для установки порогового значения $(C/I)_{пор}$ отношения C/I; измеряется текущее значение отношения $(CIR)_{est}$, которое сравнивается с его установленным пороговым значением $(CIR)_{target}$; на основе результата этого сравнения формируется решение о необходимости увеличения или уменьшения мощности ПС, т.е. о значении бита управления мощностью [2].

На рис.1 представлена возможная структурная схема системы управления мощностью в обратной линии с помощью открытой и замкнутой петель, в которой команды управления мощностью ПС формируются с частотой 800 Гц (блок 9) на основе сравнения текущего значения оценки отношения C/I (блок 7) с порогом, значение которого устанавливается блоком 8 на основе измерения BER (блок 6).

В дальнейшем будем предполагать, что оценка текущего значения BER формируется на основе данных декодера (блок 5) и является относительно инерционной. Рекомендуемое значение BER устанавливается в блоке 8 и в данной статье принимается равным 10%. Предположим, что оценка текущего значения отношения C/I формируется на основе данных демодулятора 4, в котором осуществлено сложение всех обнаруженных и используемых лучей.

В приемнике ПС команды управления мощностью выделяются из потока принимаемых данных (блок 11) и используются для изменения коэффициента радиочастотного усилителя мощности (блок 12), или для установки нового уровня модулирующего сигнала (блок 13).

В соответствии с рекомендациями [2] управление мощностью, излучаемой ПС, с помощью замкнутой петли устанавливается так, чтобы сохранить на входе приемника БС требуемое значение параметра CIR. БС должна оценивать текущее значение мощности сигнала канала DPCH(Dedicated Pilot Control Channel) конкретного пользователя на выходе Rake-приемника. Одновременно БС должна оценивать в текущей полосе частот мощность общего принимаемого в обратном канале сигнала интерференции. На основе этих оценок БС должна формировать команды управления мощностью (TPC-команды) в соответствии со следующим правилом:

$$CIR_{est} > CIR_{target} \text{ fi } TPCcommand = уменьшить,$$
$$CIR_{est} < CIR_{target} \text{ fi } TPCcommand = увеличить.$$

Бит управления мощностью должен бить установлен равным '0', когда значение $(CIR)_{est}$, получаемое внутренней петлей управления мощности, меньше, чем соответствующее установленное значение CIR_{target}. Бит управления мощностью должен быть установлен равным '1', когда $(CIR)_{est}$ больше или равно соответствующему уставленному значению.

Приемник БС должен сравнивать значение $(CIR)_{est}$, получаемое внутренней петлей управления мощностью, с соответствующим значением $(CIR)_{target}$ внешней петли, для определения значения бита управления мощностью ('0' или '1'), который должен быть передан по прямому подканалу управления мощности на ПС.

После приема этой команды ПС должна изменить излучаемую мощность во всех кодовых каналах в указанном направлении на заданную величину, которая является параметром системы управления, значение которого может быть различным для разных сот.

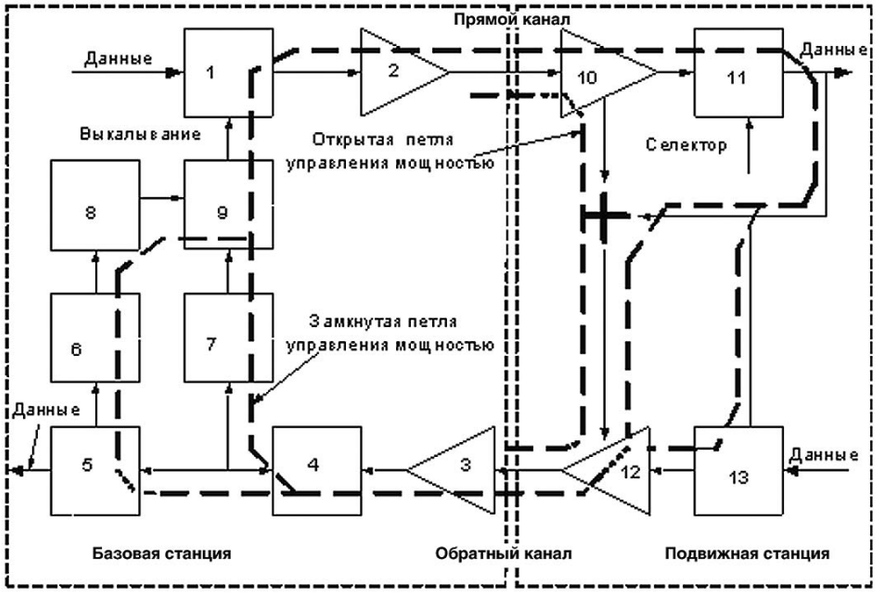


Рис. 1. Управление мощностью в обратной линии открытой и замкнутой петлями:
1 — мультиплексор; 2 — усилитель мощности; 3 — усилитель радиочастотного сигнала; 4 — цифровой демодулятор; 5 — деперемежитель и декодер; 6 — оценка BER; 7 — оценка C/I; 8 — устройство формирования порогового значения отношения C/I; 9 — устройство формирования команды управления мощностью; 10 — усилитель радиочастотного сигнала с АРУ; 11 — цифровой демодулятор; 12 — управляемый усилитель мощности; 13 — установка уровня модулирующего сигнала.

Требуемое значение CIR устанавливается независимо для каждого пользователя соты на основе оценки качества связи в его обратной линии. Дополнительно может быть установлена разница между мощностями различных кодовых каналов обратной линии. Оценка качества связи может быть различной для разных услуг. Обычно она основывается на комбинации оценок BER и FER.

Открытая петля управления мощностью используется также для установки излучаемой мощности физического канала случайного доступа. До передачи окна случайного доступа ПС должна измерить мощность принимаемого сигнала PCCPCH (Primary Common Control Physical Channel) прямой линии на достаточно большом временном интервале для устранения влияния многолучевого фединга. На основе полученной оценки мощности и известного значения излучаемой мощности канала PCCPCH (передается по BCCH) могут быть определены потери распространения в прямой линии, включая затенения. Эта оценка потерь распространения и знание уровня интерференции в обратном канале и требуемого значения CIR затем используются для установки излучаемой мощности канала случайного доступа. Уровень интерференции в обратной линии и требуемое значение CIR на входе приемника БС сообщаются ПС по BCCH.

Замкнутая петля производит оценку текущего значения сигнал/интерференция для каждого из кодовых каналов, для которых предусмотрено управление мощностью в прямом канале. Механизм этого оценивания стандартом не регламентируется. В настоящее время не существует однозначной рекомендации по этому поводу, и данный вопрос может являться предметом дальнейшего рассмотрения.

Способы формирования и передачи команд управления

В данном разделе поясняется предлагаемая методика борьбы с быстрыми замираниями в обратной линии, отличающаяся от рекомендаций стандарта IS-2000 двумя более важными моментами.

Во-первых, предлагается использовать двухбитовую команду управления мощностью вместо однобитовой и новый способ ее передачи. Во-вторых, с целью повышения скорости реакции системы управления мощностью ПС на изменения уровня сигнала на входе приемника БС предлагается вместо оценивания текущего значения CIR прогнозированию его будущие значения.

На рис. 2 представлена схема передачи однобитовой команды управления мощностью ПС по основному каналу прямой линии методом выкалывания. Пунктирной линией обведены элементы системы управления мощностью ПС, предусмотренные стандартом IS-2000. Обратим внимание на тот факт, что в оба квадратурных канала при такой схеме выкалывания подаются один и тот же символ +1 либо -1. При квадратурной схеме модуляции, используемой в прямой линии IS-2000 и представленной на рис. 3(a), это соответствует способу модуляции ФМ-2. Интервал времени T_s, используемый для передачи такой однобитовой команды управления равен длительности симво-

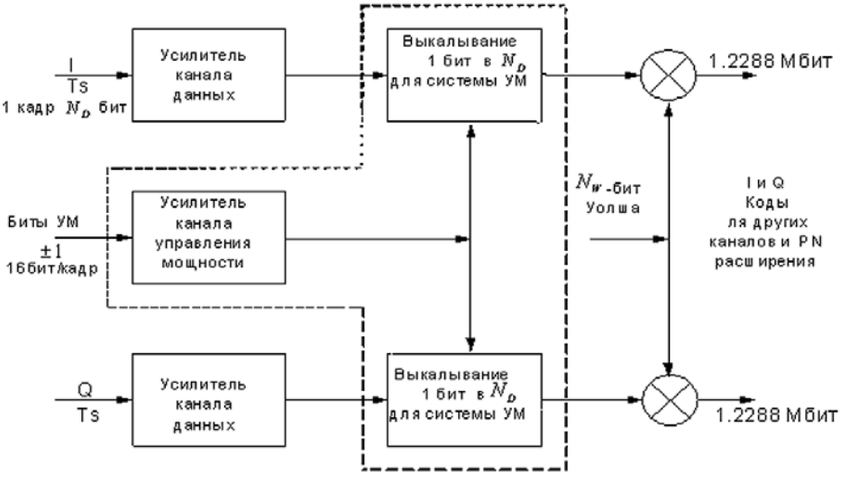


Рис. 2. Передача однобитовой команды управления мощностью по основному каналу методом выкалывания (N = 1,1.25 МГц, Ts- длительность символа, N_w — число символов Уолша)

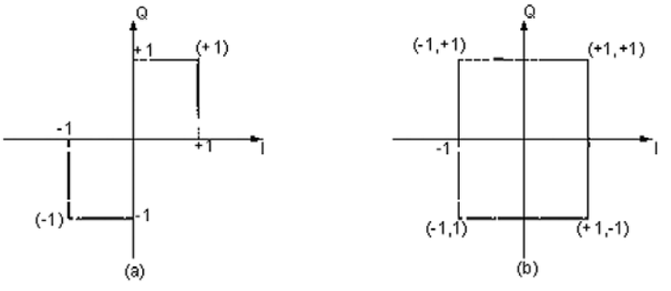


Рис. 3. Сигнальные созвездия:(a)-при однобитовой команде управления мощность ПС; (b) — при двубитовой команды управления

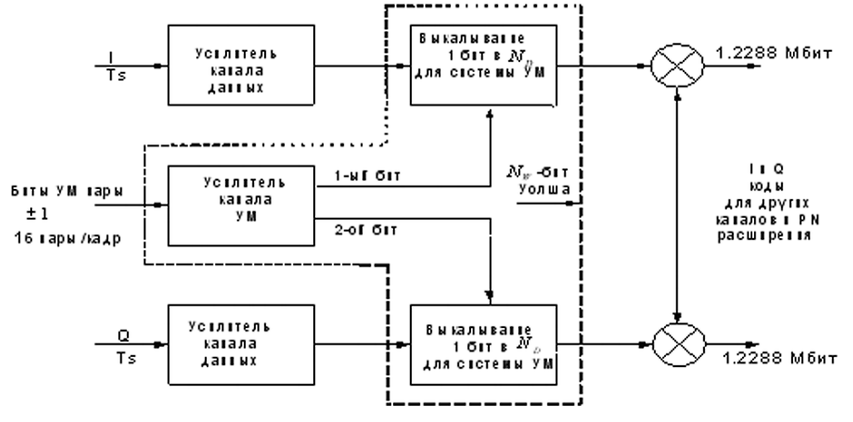


Рис. 4. Передача двухбитовой команды управления мощностью по основному каналу методом выкалывания (N =1,1.25 МГц, Ts — длительность символа, N_w — число символов Уолша)

ла модуляции и зависит от установленной скорости передачи данных, как и значения остальных параметров N_D, N_W.

На этом же интервале времени T_s можно передать двухбитовую команду управления мощностью, если вместо ФМ-2 использовать на этом же интервале ФМ-4 (рис. 3,b), для чего достаточно лишь незначительно изменить функциональную схему рис. 2, как это показано на рис. 4. При таком способе модуляции можно передать четыре разные команды, если использовать все возможные фазовые переходы.

Можно предложить следующие варианты кодирования команд управления мощностью.

1. (+1, -1) или (-1, +1) — уровень мощности не изменять;
2. (+1, +1) — уровень мощности увеличить на величину DP дБ;
3. (-1, -1) — уровень мощности уменьшить на величину DP дБ.

Можно ожидать, что при таком способе управления мощностью ПС флуктуации мощности сигнала ПС при малых скоростях ее движения уменьшатся, поскольку будет устранен режим "bang-bang", (пинг-понг) типичный для замкнутой петли регулирования уровня сигнала в обратном канале связи системы CDMA стандарта IS-2000. Можно ожидать, что характеристики замкнутой петли управления системы с предсказанием, при средних и больших скоростях движения ПС при этом останутся неизменными.

Недостатком данного способа передачи двухбитовой команды управления является использование модуляции ФМ-4 вместо ФМ-2, что сопровождается понижением помехоустойчивости передачи этой команды. Однако этот энергетический проигрыш можно компенсировать путем увеличения "PC Channel Gain" на соответствующую величину, что легко реализуемо в системе IS-2000.

Дополнительные аппаратные затраты, необходимые для реализации этого способа передачи, невелики: необходимо в оборудование БС добавить один демультиплексор, который должен разделять первый и второй биты двухбитовой команды управления, а в оборудование ПС — логический дешифратор на двух вентилях типа "И".

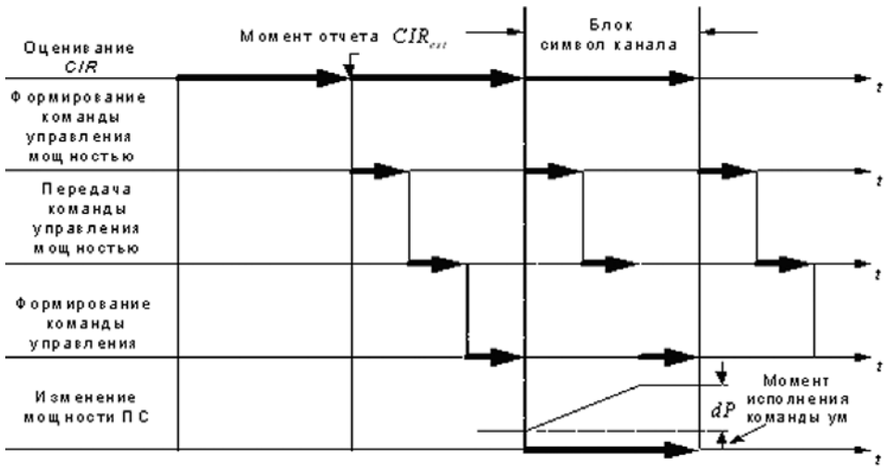


Рис. 5. Возможный режим работы системы управления мощностью с замкнутой петлей

Пусть CIR_{target} является номинальным значением отношения CIR в обратной линии. Тогда при любом уровне интерференции I требуемое номинальное значение мощности сигнала ПС на входе приемника БС можно определить равенством:

$$C_{target} = CIR_{target} \quad I.$$

Это равенство мы будем использовать для формирования двухбитовых команд управления мощностью в соответствии со следующим правилом:

увеличить мощность ПС на DP дБ, если,

$$\hat{D}_k(p) \pounds k_d \quad CIR_{targ\,et} \quad \hat{I}_k(p),$$

уменьшить мощность ПС на DP дБ, если,

$$\hat{D}_k(p) \ddagger k_u \quad CIR_{targ\,et} \quad \hat{I}_k(p), \qquad (1)$$

не изменять мощность ПС, в противном случае,

где лв $k_d \le 1$, $k_u \ge 1$, являются параметрами системы быстрого управления мощностью ПС. Здесь также приняты следующие обозначения: $\hat{D}_k(p)$ — оценка уровня сигнала пилот-канала k-го пользователя, вычисленная на p-м шаге, $\hat{I}_k(p)$ — оценка среднеквадратического значения суммарной помехи в обратной линии k-ого пользователя, полученная на этом же шаге.

Правило (1) является двухпороговым. Это представляется целесообразным, поскольку формируемые оценки уровней сигнала и помехи обладают конечной точностью, которая зависит от текущего значения параметра CIR. Даже в том случае, когда значение параметра CIR не изменяется, из-за случайных ошибок в формировании оценок $\hat{D}_k(p)$ и $\hat{I}_k(p)$ при $k_d = k_u$ с вероятностью 1 принимаются неверные решения в формировании команд управления мощностью. Можно указать оптимальные значения этих порогов, когда вероятность формирования ошибочной команды управления мощностью оказывается минимальной.

В таблице указан возможный способ кодирования данных трех команд управления мощностью ПС.

В правиле (1) осталось только определить номинальное значение CIR_{target} для отношения сигнал/интерференция в обратной линии, которое обычно определяется стандартом.

Важно подчеркнуть, что в реальной петле обратной связи имеется задержка, обусловленная как необходимостью измерения текущего значения $(CIR)_{est}$ отношения CIR, так и особенностями протокола организации работы этой системы управления во времени. Временные задержки могут иметь место во всех указанных элементах петли обратной связи. Временные диаграммы, представленные на рис. 5, иллюстрируют возможное распределение задержек вдоль петли обратной связи. На данном рисунке временная задержка между моментом окончания измерения $(CIR)_{est}$ и моментом завершения изменения мощности ПС оказывается равной двум длительностям блока канальных символов, используемых для измерения CIR. Все перечисленные этапы управления мощностью должны иметь, возможно, меньшую длительность, с тем, чтобы уменьшить задержку в

Кодирование двухбитовой команды быстрого управления мощностью

Номер команды	Команды управление мощностью	Кодовое слово
1	увеличить мощность на ΔP (дБ)	1 1
2	без изменений	1-1
3	без изменений	-1 1
4	уменьшить мощность на ΔP (дБ)	-1-1

петле обратной связи.

В данной статье нет возможности привести сведения о способах формирования оценок $\widehat{D}_k(p)$ и $\widehat{I}_k(p)$ в приемнике БС стандарта IS-2000, которые не являются предметом исследования этой работы. Поэтому здесь в дальнейшем будем полагать, что выборочные значения этих статистик сформированы и могут быть использованы при исследовании эффективности предлагаемой системы управления мощности ПС.

План и результаты статистического эксперимента

Эффективность системы управления мощностью с замкнутой петлей в обратной линии в данной статье будем характеризовать среднеквадратическим значением отклонения CIR от установленного номинального значения CIR_{target}. Очевидно, что это отклонение существенно зависит от скорости замираний, поэтому оценки эффективности системы управления должны быть получены для разных значений допплеровского расширения спектра. Для данного эксперимента примем рекомендации стандарта: частота Доплера не более 500 Гц [2].

Количественные оценки эффективности системы управления мощностью получим с помощью статистического моделирования на ПЭВМ. Для этого была подготовлена программа для имитационного моделирования, которая в одном эксперименте позволяла исследовать следующие варианты построения обратной линии:

- система управления мощностью выключена, на БС осуществляется непрерывный режим когерентного приема Q лучей (NxRTT Rake-приемник), межсимвольная интерференция создается M предшествующими и M последующими элементарными символами;
- система управления мощностью стандарта IS-2000 включена, непрерывный режим передачи в обратном канале, когерентное сложение и демодуляция Q лучей (NxRTT Rake-приемник), межсимвольная интерференция от M символов, используется однобитовая команда управления мощностью, частота следования команд управления мощностью F_{PCC} = 800, 1600, 3200 Гц, CIR_{nom} = 7 дБ;
- модифицированная система управления мощностью стандарта CDMA2000 включена, когерентное сложение и демодуляция Q лучей (NxRTT Rake-приемник), межсимвольная интерференция от M канальных символов, двухбитовая команда управления мощностью, частота следования команд уп-

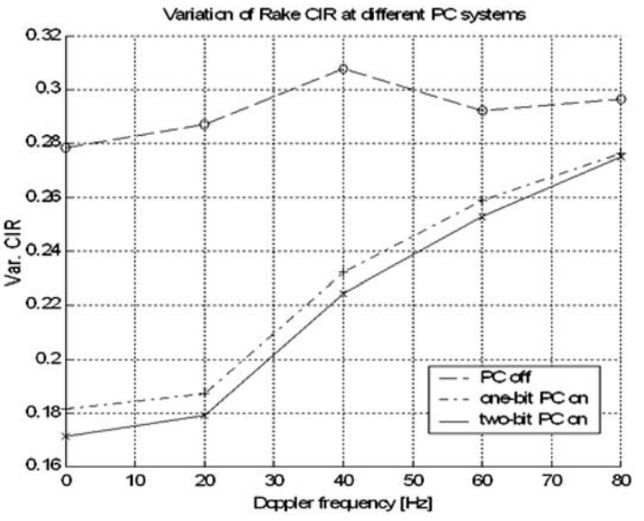


Рис. 6. Зависимость среднеквадратического значения отклонения CIR от номинального значения

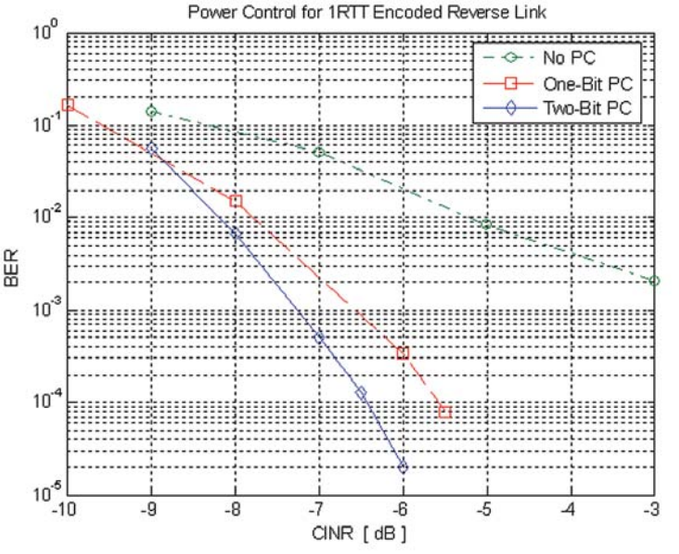


Рис. 7. Эффективности двухбитовой системы управления мощностью с замкнутой петлей

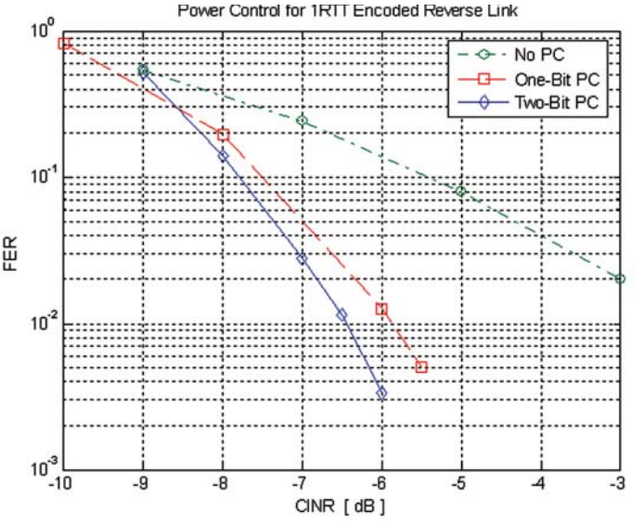


Рис. 8. Эффективности двухбитовой системы управления мощностью с замкнутой петлей

равления мощностью F_{PCC} = 800, 1600, 3200 Гц, CIR_{nom} = 7дБ.

Вычисление среднеквадратического значения отклонения CIR от его номинального значения осуществлялось на выходе Rake-приемника (на выходе устройства выделения сигнала пилот канала) путем усреднения получаемых оценок CIR_{est} на интервалах времени длительностью $N_{окон}$ x 20 мс по $N_{реализаций}$ реализациям. Вычисления выполнялись для $N_{частоты}$ значений частоты Доплера.

Результаты статистического моделирования представляются тремя графиками зависимости среднеквадратического значения отклонения CIP_{est} от его номинального (установленного) значения.

При планировании статистического эксперимента было принято решение о целесообразности вычисления оценок BER и FER путем обработки нескольких реализаций процесса, каждая из которых содержит заданное число окон. Число реализаций будем обозначать символом $N_{реализаций}$, а число окон в одной реализации — $N_{окон}$. При такой организации эксперимента имеется возможность осуществлять усреднение получаемых результатов как по времени при достаточно длинной реализации, так и по множеству моделируемых сравнительно коротких реализаций. Усреднение по времени является эффективной операцией при относительно больших значениях допплеровского расширения спектра (более 50 Гц), в то время как усреднение по множеству эффективно при малых значениях этого параметра (менее 10 Гц). Моделирование и обработка одной реализации любой длины выполняются блоками, объем которых одинаков и равен числу канальных символов в одном окне; результаты статистической обработки одной реализации затем усредняются по совокупности всех моделируемых реализаций.

Следует подчеркнуть, что для исследования статистических характеристик системы управления мощностью возможность обработки достаточно длинных реализаций процессов принципиально необходима. Это обусловлено тем, что система управления мощностью является нелинейной инерционной системой и, следовательно, качество ее функционирования необходимо характеризовать флуктуационной и динамической ошибками. Приведены результаты статистического моделирования для установившегося режима, который имеет место только после завершения переходных процессов, в момент включения системы управления. Для обеспечения таких условий при моделировании предусмотрено, что подсчет числа ошибок в системе начинается только со второго передаваемого окна. Время установления стационарного режима при указанных ниже значениях параметров системы составляет менее половины длительности окна (около 5 мс). Поэтому минимальное количество окон, передаваемых последовательно во времени, не может быть менее двух. Кроме того, в силу многолучевости используемой модели канала при демодуляции символов очередного окна необходимо учитывать около 20 символов предыдущего и 20 символов последующего окна, поэтому приходится моделировать на одно окно больше, чем число окон, запланированное для статистической обработки.

На рис. 6 представлена зависимость среднеквадратического значения отклонения оценки $V_{ar}CIR_{est}$ от номинального значения как функция от допплеровского спектра при следующих численных значениях параметров эксперимента: когерентный Rake приемник; число лучей Q = 4; межсимвольные искажение M = 5; CIR_{nom} = 7 дБ; шаг изменение DP =1дБ; нижний порог CIR_{low} = CIR-0,5*DP; верхний порог CIR_{upper} = CIR + 0,5*DP; частота команд управления мощностью 800 Гц; число окон в одном испытании $N_{окон}$ = 4; число реализаций $N_{реализаций}$ = 20; задержка в петле управления 0,625 мкс.

При отсутствии управления мощностью Var CIR фактически определяет глубину замираний и не зависит от допплеровского расширения спектра, изменяется лишь скорость замираний. При включении новой системы управления мощностью отклонения CIR_{est} от заданного значения CIR_{nom} существенно уменьшаются. При этом система с двухбитовой командой управления обеспечивает большую устойчивость отношения CIR_{est}. С ростом допплеровского расширения спектра эффективность системы управления мощностью подает, но система с двухбитовой командой всегда обладает большей эффективностью. При любом значении допплеровского расширения спектра параметры эксперимента выбраны таким образом, что среднее значение CIR всегда равно CIR_{nom}.

На рис. 7, 8 представлены результаты моделирования в аналогичных условиях (допплеровская частота расширения равна 10 Гц). Однако в качестве эффективности систем управления мощности здесь выбрана оценка доли неверно принятых кадров и кодовых битов. Предполагалось, что команды управления мощностью в прямой линии передаются без ошибок.

Заключение

Исследование проблемы управления мощностью в прямой и обратной линиях в рамках стандарта IS-2000 позволяет сделать вывод о том, что в рамках предлагаемого в данной статье подхода возможно построение более эффективных алгоритмов управления, чем алгоритм предусматриваемый стандартом. Основные идеи этого направления — уменьшение времени задержки в петлях регулирования путем управления на основе предсказанных значений отношения сигнал/интерференция и использование многобитовых команд управления мощности.

Основные выводы, которые можно сделать на основе анализа представленных результатов статистического эксперимента, можно сформулировать следующим образом:

- переход от однобитовой команды управления к двубитовой позволяет получить энергетический выигрыш около 0,7 дБ для значения $BER = 10^{-3}$;
- при значении $FER = 2 \cdot 10^{-2}$ система управления мощностью с двухбитовой командой управления обеспечивает энергетически выигрыш примерно на 0,5 дБ по сравнению с системой, использующей однобитовую команду управления.

Отметим здесь, что в эксперименте была исследована двухбитовая система управления мощностью, которая не использует алгоритм предсказания и имеет задержку в замкнутой петле такую же, как и однобитовая система управления (1,25 мс).

Приведенные данные экспериментальных исследований свидетельствуют о том, что разработанная в рамках данной статьи двух-битовая система управления мощностью имеет определенное преимущество перед однобитовой, рекомендуемой стандартом IS-2000. Однако в пространстве параметров систем управления мощностью рассмотренные условия представляют собой всего лишь одну точку (допплеровское расширение спектра равно 10 Гц).

Представляется очень важным продолжение исследований для других условий работы систем управления. В первую очередь следует указать на необходимость проведения аналогичных исследований для других значений допплеровского расширения спектра.

Литература

1. CDMA: прошлое, настоящее, будущее/ Под ред. проф.Л.Е Варакина и проф. Ю.С. Шинакова — Москва МАС, 2003. — 608 с.

2. Physical Layer Standard for cdma2000 Spread Spectrum Systems (PN-4428, to be published as IS-2000-2).

9-я международная конференция

СТАНДАРТИЗАЦИЯ, ВНЕДРЕНИЕ И ОЦЕНКА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ИКТ

30-31 марта 2010 г.
Москва, Марриотт Гранд Отель

Конференция проводится общественно-государственным объединением «Ассоциация документальной электросвязи» при поддержке Министерства связи и массовых коммуникаций Российской Федерации.

Отличительной особенностью конференций АДЭ является высокий уровень представительства органов государственной власти и бизнеса, а также методологическая стройность, профессионализм, актуальность и практическая направленность программ, в реализации которых участвуют ведущие российские и зарубежные специалисты.

ОСНОВНЫЕ ТЕМЫ КОНФЕРЕНЦИИ:

- безопасность применения ИКТ в критически важных инфраструктурах
- информационная безопасность оказания государственных услуг
- управление сетью связи общего пользования в чрезвычайных ситуациях
- оценка соответствия и совместимости систем безопасности
- управление идентификацией пользователей и оборудования
- защита персональных данных в информационных системах операторов связи
- противодействие мошенничеству на сетях связи
- внедрение шифровальных (криптографических) средств на сети связи общего пользования
- обеспечение базового уровня безопасности и возмездное оказание дополнительных услуг

Приглашаем Вас на международный форум 2010 года по обеспечению информационной безопасности инфокоммуникационных сетей и систем!

АССОЦИАЦИЯ ДОКУМЕНТАЛЬНОЙ ЭЛЕКТРОСВЯЗИ

Оргкомитет:
тел.: (495) 673-34-28, 673-32-46, 673-48-83, 956-26-12, 995-20-11
факс (495) 673-30-29 • e-mail: info@rans.ru • http://www.rans.ru

Форум "Интерком-2009: Инфокоммуникации будущего"

INTER•COM
ФОРУМ ИНФОКОММУНИКАЦИИ БУДУЩЕГО

Форум "Интерком — 2009: Инфокоммуникации будущего" является продолжением цикла мероприятий под брендом "Интерком", которые традиционно проходят в Санкт-Петербурге. Тематика Форума охватывает наиболее актуальные вопросы современного состояния отрасли и перспектив ее дальнейшего развития:

• Кого выбирает потребитель в условиях кризиса — мобильных или фиксированных операторов? Причины и следствия.

• Эпоха реальной конвергенции проводной и беспроводной связи в России. Результаты крупнейшего конвергентного проекта в России.

• Переход на технологии NGN и введение в эксплуатацию новейшей сетевой инфраструктуры связи.

• Перспективы развития MVNO в условиях кризиса. Результаты действующих проектов и перспективные стартапы.

• За счет чего операторам дальше увеличивать ARPU в условиях исчерпавшегося потенциала роста голосовых услуг.

• Будущее региональных проектов по строительству сетей ШПД. Начало острой конкуренции фиксированных операторов с мобильными на региональных рынках.

• Новые подходы к лицензированию услуг связи. Государственные инициативы по регулированию рынка.

• Перспективы реформы "Связьинвеста". Ожидаемые изменения позиций ведущих игроков отрасли.

• Какие услуги сейчас приносят операторам наибольшую прибыль? Кто выигрывает на фоне общего спада?

• Где искать деньги в условиях кризиса? Новые кредитные и инвестиционные ресурсы. Успешные финансовые и маркетинговые решения.

• Что кроме кризиса мешает инвестированию в российский телеком? Каких действий ждут инвесторы от государства?

• Наиболее устойчивые островки российского телекома. Какие сегменты имеют наибольший инвестиционный потенциал?

Топ-менеджеры крупнейших компаний отрасли в течение двух дней обсуждали основные вопросы в области телекоммуникаций и новейших технологий. В числе компаний-участников Форума — "Ростелеком", "МТС", "Вымпелком", "Скай Линк", "Комстар", "МегаФон", "РТКомм", "Северо-Западный Телеком" и др.

"Проводящийся уже в третий раз форум "Интерком-2009" доказал, что является весьма значимым событием отрасли информационно-телекоммуникационных технологий и связи", — отметил заместитель министра связи и массовых коммуникаций РФ Алексей Солдатов. Он убежден, что регулярное проведение таких мероприятий способствует развитию телекоммуникационного рынка России.

Целью III Международного форума "Интерком-2009" стало развитие телекоммуникационного рынка России через внедрение технологических и маркетинговых разработок ведущих российских и зарубежных компаний в области телекоммуникаций и высоких технологий.

С приветственным словом на открытии Форума "Интекрком-2009" выступил представитель Генерального спонсора Форума — компании "Ростелеком" — Иван Маковкин, заместитель коммерческого директора Северо-Западного филиала компании. Для национального оператора связи "Ростелеком" ежегодное участие в Форуме стало доброй традицией: компания приветствует развитие профессиональных связей, обмен опытом, взаимовыгодное межоператорское партнерство, доверительные отношения между коллегами по отрасли.

Программа первого дня Форума была насыщена выступлениями по самым актуальным вопросам отрасли. Секцию "Современные тенденции и перспективы рынков фиксированной и мобильной связи; потребительская востребованность в сегодняшних условиях" модерировал Денис Кусков, генеральный директор информационного агентства "Неделя сотовых технологий".

Ключевыми докладами стали выступления Андрея Ковтонюка, директора Северо-Западного региона "Вымпелком", тема: "Уникальный интеграционный опыт "Билайн"", Алексея Никитина, директора департамента технического развития "Северо-Западный Телеком", тема: "Переход на технологии NGN и введение в эксплуатацию новейшей сетевой инфраструктуры связи", и Алексея Ефимова, начальника отдела продаж операторам связи Северо-Западного филиала "Ростелеком", тема: "IP-телевидение "Ростелекома" как инструмент увеличения дохода оператора связи".

Первый день Форума завершил круглый стол на тему: "Возможности операторов связи в сфере обеспечения безопасности детей в сети Интернет: взаимодействие с государственными органами и собственные инициативы", который проходил под эгидой Года Безопасного Интернета и при поддержке Партнера Форума "Интерком-2009" — Российского клуба связистов.

Во второй день форума прошла панельная дискуссия "Проекты по строительству ШПД: движение в регионы", основными темами которой стали:

• Примеры стартапов по строительству ШПД в 2009 г.

• Новые условия для основных игроков телекоммуникационной отрасли.

• Проблемы, с которыми операторы могут столкнуться в 2010 г.

• Снижение прибыли и увеличение расходов вследствие обострения конкуренции.

• Доступность услуг ШПД для пользователя в регионах.

Организатор Форума:
ICF-Международные конференции.
Генеральный спонсор:
национальный оператор связи "Ростелеком"