MOBILE & WIRELESS

INTERNATIONAL CONFERENCE & EXHIBITION

3-я МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ И ВЫСТАВКА

БЕСПРОВОДНЫЕ И МОБИЛЬНЫЕ ТЕХНОЛОГИИ

27-29 ноября 2007

ЦЕНТР МЕЖДУНАРОДНОЙ ТОРГОВЛИ
МОСКВА, РОССИЯ

технологии, которые меняют мир...

Организатор:
INCONEX
International Conferences & Exhibitions

ООО "ИНКОНЭКС"
Тел.: (495) 739 55 09, факс: (495) 641 22 38
E-mail: electronica@inconex.ru

www.inconex.ru

Now in its 8th year

BILLING OSS

TELECOM FORUM RUSSIA

17th - 19th December 2007, World Trade Center, Moscow

Организатор

exposystems
part of Expomedia Group Plc.

Платиновые спонсоры

EASTWIND

TTI Telecom
Your Network Management Partner

Золотые спонсоры

Alcatel·Lucent

amdocs

INTEC

COMPTEL
INTELLIGENT LINK

HUAWEI

Генеральный спонсор конференции

ТехноСерв А/С

Спонсор конференции

hp invent

Спонсор

NVisionGroup

BSS сектор • Биллинг и поддержка клиента

Биллинговые системы (Billing systems)
- конвергенция post/prepaid;
- расчеты с партнерами (interconnect);
- тарификация и биллинг новых сервисов;
- противодействие мошенничеству (fraud management)
- конвергентный предбиллинг (mediation)

Поддержка клиентов (Customer care)
- Help & service desk;
- самообслуживание;
- повышение лояльности и сокращение оттока;
- CRM.

OSS сектор • Поддержка сети

Инвентаризация (Inventory)
- инвентаризация и учет ресурсов;
- планирование сети.

Управление ошибками (Fault Management)
- регистрация неисправностей в сети;
- управление неисправностями в сети.

Управление производительностью (Performance management)
- производительность сети
- производительность IT систем

Управление и сетевой мониторинг (Network monitoring)
- сбор информации
- GPRS мониторинг
- SS7 мониторинг

OSS сектор • Поддержка услуг

Управление заказами (Order Management)
- заказ услуг;
- активация услуг.

Управление уровнем сервиса (SLA management)

Мониторинг услуг (Services monitoring)
- мониторинг сервисов и контента (end-to-end мониторинг)
- управление качеством голосовых услуг

www.exposystems.ru/boss • +7 495 995 80 80

T•Comm
Телекоммуникации и транспорт
№ 7-8(2007)

"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 диссертаций и рекомендован УМО по образованию в области телекоммуникаций для студентов высших учебных заведений.

Учредитель
ООО "Издательский дом Медиа Паблишер"

Главный редактор
Тихвинский Вадим Олегович

Издатель
Дымкова Светлана Сергеевна
ds@media-publisher.ru

Предпечатная подготовка
ООО "ИД Медиа Паблишер"
Дизайн обложки
Владимир Горохов

www.media-publisher.ru

СОДЕРЖАНИЕ

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

exporail2007

27 – 29 ноября
ЦВК "ЭКСПОЦЕНТР", Москва

При поддержке:

Российские железные дороги

Генеральный партнер:
Финансово-Строительная компания «МостГеоЦентр»

Генеральный спонсор:
ВНИИЖТ

Официальный спонсор:
Ж·А·С·О Страховое общество с 1991 www.zhaso.ru

Генеральный информационный партнер:
Деловой журнал РЖД·партнер

ВСЕ ДЛЯ ЖЕЛЕЗНЫХ ДОРОГ:

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

www.exporail.ru

Одновременно с выставкой: V Международная конференция
"ОАО "Российские железные дороги" на рынке транспортных услуг: взаимодействие и партнерство"

Организатор:
РЕСТЭК·БРУКС

Россия, 197110, С.-Петербург,
ул. Петрозаводская, 12
Тел.: +7 (812) 320 80 94
Факс: +7 (812) 320 80 90
E-mail: exporail@restec.ru

Организатор конференции:
Компания "БизнесДиалог"
Тел./факс: +7 (495) 262 98 15, 624 59 32
E-mail: info@businessdialog.ru
www.businessdialog.ru

Международный конгресс "Менеджмент успешного бизнеса"

1 ноября 2007 г. в Москве прошел Международный конгресс в рамках Европейской недели качества в России и Глобального проекта "России — новое качество роста", в котором приняли участие представители министерств и ведомств, Совета Федерации Федерального Собрания РФ, Госдумы России, руководители и специалисты ведущих компаний.

Цель конгресса — содействие в проведении экономических реформ, обеспечивающих конкурентоспособность России на внутреннем и международном рынках.

Конгресс объединил представителей многих отраслей экономики, в том числе и отрасли "Связь", сделав важный шаг на пути к реализации стратегической задачи — содействие распространению современных методов управления качеством и конкурентоспособностью предприятий в условиях вступления России в ВТО.

Участники Конгресса обменялись мнениями по проблемам создания систем управления и сертификации систем качества предприятий нового поколения, государственного и общественного регулирования, определили задачи повышения эффективности и конкурентоспособности российской экономики, науки и образования.

Одной из центральных тем в программе Конгресса стало обсуждение роли государства в нормативно-правовом регулировании вопросов повышения качества бизнеса, продукции и услуг. Это весьма актуально, поскольку системные мероприятия по реформированию экономики России требуют поддержки высокообразованных специалистов и ученых.

В рамках конгресса состоялось вручение национальных премий "Олимп качества", "Лидер российской экономики" и высшей общественной награды "Золотой знак".

"Золотым знаком" отмечаются лучшие из лучших руководителей, получивших всеобщее признание за вклад в становление движения по совершенствованию бизнеса и активное применение современных технологий менеджмента.

В 2007 г. высшей общественной наградой "Золотой Знак" награждены:

За большой вклад в реализацию государственной политики в области телекоммуникаций

В.Б. Булгак, Министр связи РФ в период с 1990 по 1997 гг.

За большой вклад в реализацию государственной политики и совершенствование деятельности по надзору в сфере связи и информатизации в период с 2000 по 2007 гг.

В.Н. Бутаенко, Руководитель Федерального агентства связи

За большой вклад в организацию антимонопольной деятельности и поддержку предпринимательства

А.Н. Голомолзин, заместитель руководителя Федеральной Антимонопольной Службы

За большой вклад в совершенствование законодательной деятельности в сфере образование и науки

С.И. Колесников, заместитель Председателя Комитета Госдумы России по образованию и науке.

Адрес редакции
101990, Россия, Москва, Центр,
Хохловский пер., д. 7
Тел./факс: +7 (495) 625-43-05

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

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.

www.media-publisher.ru

Fitch Ratings повысило кредитный рейтинг ОАО "Северо-Западный Телеком"

19 октября 2007 г. международное рейтинговое агентство Fitch Ratings повысило международный долгосрочный кредитный рейтинг ОАО "Северо-Западный Телеком" с уровня "B+" до "BB-", национальный долгосрочный кредитный рейтинг ОАО "СЗТ" — с "A (rus) до "A+ (rus)", рейтингам присвоен прогноз "Стабильный". Краткосрочный рейтинг Компании в иностранной валюте подтвержден на уровне "B".

"Комстар-ОТС" запустил сеть WIFI в аэропорту Шереметьево

В ближайшем будущем компания планирует обеспечить работу сети на всей территории аэропорта и расширить спектр сервисов, предлагаемых пассажирам.

На данный момент развернутая на территории Терминала "С" сеть Wi-Fi подключена к магистральной сети "Комстар-ОТС" на скорости 10 Мбит/с. Это обеспечивает возможность выхода во "всемирную паутину" с мобильных устройств для более чем 120 одновременно работающих пользователей. Оплата доступа будет осуществляться с помощью предоплаченных карт Comstar-WiFi.

В основу сети беспроводного доступа легла инфраструктура ОАО "Международный аэропорт Шереметьево" ("МАШ") и 100% дочерней компании "Комстар-ОТС" — ЗАО "ПортТелеком", которое будет обеспечивать дистрибуцию карт Comstar-WiFi на территории аэропорта через дилерскую сеть и собственные точки продаж.

Избран новый состав правления МГТС

СОВЕТ ДИРЕКТОРОВ ОАО "МОСКОВСКАЯ ГОРОДСКАЯ ТЕЛЕФОННАЯ СЕТЬ" ИЗБРАЛ НОВЫЙ СОСТАВ ПРАВЛЕНИЯ, В КОТОРЫЙ ВОШЛИ ПЯТЬ ПРЕДСТАВИТЕЛЕЙ МГТС И ТРИ ПРЕДСТАВИТЕЛЯ "КОМСТАР-ОТС".

Ранее правление МГТС состояло из 12 членов, в числе которых был один представитель "КОМСТАР-ОТС".

"МГТС — оператор, входящий в "КОМСТАР-ОТС", и вся его операционная деятельность тесно связана с другими компаниями группы, — подчеркнул председатель совета директоров ОАО МГТС Владимир Лагутин. — Поэтому было принято решение усилить присутствие представителей основного акционера в правлении. Члены этого исполнительного органа — как от МГТС, так и от "КОМСТАР-ОТС" — будут совместно решать текущие операционные задачи и принимать тактические решения с учетом интересов всей группы. Не сомневаюсь, что данное решение окажет позитивное влияние на развитие Московской городской телефонной сети".

Новый состав правления ОАО МГТС:

- *Гольцов Алексей*, генеральный директор ОАО МГТС, председатель правления ОАО МГТС;
- *Гудзенко Елена*, директор Департамента управления услугами и тарифной политики ОАО "КОМСТАР-ОТС";
- *Дьяков Андрей*, технический директор ОАО "КОМСТАР-ОТС";
- *Лобанов Денис*, зам. генерального директора — коммерческий директор ОАО МГТС;
- *Матвеева Ирина*, зам. генерального директора — финансовый директор ОАО МГТС;
- *Олейникова Татьяна*, директор Департамента кадровой политики ОАО "КОМСТАР-ОТС";
- *Панов Виктор*, зам. генерального директора — начальник Управления технической эксплуатации телекоммуникаций ОАО МГТС;
- *Семушкин Сергей*, зам. генерального директора — начальник Управления безопасности ОАО МГТС.

МТС сообщает о выборе поставщиков оборудования для строительства сети 3G по России

ОАО "МОБИЛЬНЫЕ ТЕЛЕСИСТЕМЫ" ОБЪЯВЛЯЕТ О СОТРУДНИЧЕСТВЕ С КОМПАНИЯМИ ERICSSON И NOKIA SIEMENS NETWORKS В ОБЛАСТИ СТРОИТЕЛЬСТВА СЕТИ 3G ПО РОССИИ.

Выбор партнеров для строительства сети 3G в России обусловлен действующей технологической стратегией МТС. Разделение поставщиков по регионам будет проводиться по географическому принципу. При этом МТС планирует использовать преимущества синергии — поставщик будет работать в тех регионах, где уровень его текущего присутствия интегрально составляет не ниже 40%.

Выбранные компании поставят МТС базовые станции (nodeB), контроллеры (RNC), ПО и оборудование канальной и пакетной коммутации, ПО и оборудование управления сетью (OSS), проведут весь комплекс работ, связанных со строительством, запуском сети, организацией технической поддержки и обучения, а также обеспечат эксплуатацию сети 3G в течение времени, необходимого для передачи опыта специалистам МТС.

МТС планирует строить совмещенную сеть 2G/3G с использованием существующих площадок под базовые станции без остановки или существенной переконфигурации сети GSM. Абоненты UMTS смогут пользоваться всеми существующими на данный момент в сети 2/2,5G дополнительными услугами. Уже на первом этапе действия сети 3G все оборудование будет поддерживать технологию широкополосной передачи данных HSPA, кроме того, абонентам будут доступны такие услуги как видеозвонок и видеоконференция.

Компании Ericsson и Nokia Siemens Networks были выбраны на конкурсной основе. При выборе поставщика учитывались: позиция на рынке и финансовое положение компании, доказанный опыт в проектах аналогичного масштаба, качество технического предложения, возможности по реализации проекта в России и предложенные ценовые условия. Консультантом в процессе выбора поставщика выступила одна из ведущих консалтинговых компаний в индустрии — Booz Allen Hamilton.

"Выбранные вендоры предложили оптимальные с точки зрения МТС условия поставки. Дополнительным аргументом в их пользу также стал тот факт, что оборудование Nokia Siemens Networks в сети МТС 2-2,5G преобладает в Москве и Центральном федеральном округе, а оборудование Ericsson активно задействовано в большинстве других регионов страны. Этот фактор значительно упростит технологическую интеграцию и поможет нам развернуть сеть 3G в максимально оперативном режиме", — прокомментировал вице-президент ОАО "МТС" по технике и информационным технологиям Сергей Асланян.

МТС и ВГТРК продемонстрировали возможности трансляции телеканала "Вести" по сети 3G

ОАО "МОБИЛЬНЫЕ ТЕЛЕСИСТЕМЫ" И ВСЕРОССИЙСКАЯ ГОСУДАРСТВЕННАЯ ТЕЛЕРАДИОВЕЩАТЕЛЬНАЯ КОМПАНИЯ (ВГТРК) В РАМКАХ ВЫСТАВКИ ИНФОКОМ-2007 ОСУЩЕСТВИЛИ ТЕСТОВУЮ ТРАНСЛЯЦИЮ ПРЯМОГО ЭФИРА РОССИЙСКОГО ИНФОРМАЦИОННОГО ТЕЛЕКАНАЛА "ВЕСТИ" НА МОБИЛЬНЫЙ ТЕЛЕФОН ПО СЕТИ 3G.

В процессе демонстрации была показана возможность трансляции потокового видео с Интернет-сайта РИК "Вести" на мобильный аппарат, работающий в локальной сети 3G МТС, развернутой на выставке.

Техническое решение МТС позволяет демонстрировать потоковое видео со скоростью до 3,6 Мбит/с и с качеством, которое существенно превышает существующие возможности GPRS и EDGE. Воспроизведение и загрузка видеосюжетов прямого эфира происходит непрерывно и одновременно, в реальном масштабе времени.

Абоненты смогут получить доступ к сюжетам прямого эфира в любой точке, где действует сеть 3G, при этом дополнительная авторизация или регистрация не требуется.

Запуск сетей 3G позволит МТС предложить своим абонентам новые перспективные возможности. Совместный проект с телеканалом "Вести" продемонстрировал, что вскоре у абонентов МТС появится отличная возможность в любой момент получать самую оперативную информацию с Интернет-сайтов телеканалов, а благодаря высокой скорости сетей нового поколения качество трансляции будет сравнимо со стандартным телевизионным вещанием.

В церемонии запуска тестовой трансляции российского информационного канала "Вести" приняли участие Министр информационных технологий и связи РФ Леонид Рейман, генеральный директор РИК "Вести" Дмитрий Медников и президент ОАО "МТС" Леонид Меламед. Демонстрация транслировалась в прямом эфире новостного выпуска РИК "Вести".

Группа компаний "КОМСТАР-ОТС" внедряет программу модернизации инфраструктуры

В РАМКАХ ПРОГРАММЫ БУДЕТ ПОЭТАПНО ПРОВЕДЕНА ИНТЕГРАЦИЯ СУЩЕСТВУЮЩИХ NGN-СЕТЕЙ КОМПАНИЙ МГТС И "КОМСТАР-ОТС", УВЕЛИЧЕНА ПРОПУСКНАЯ СПОСОБНОСТЬ МАГИСТРАЛЬНОГО ЯДРА СЕТЕЙ МГТС И "КОМСТАР-ДИРЕКТ".

Проект интеграции сетей МГТС и "Комстар-ОТС" позволит группе устранить дублирование инвестиций в развитие обеих сетей, снизить капитальные вложения в модернизацию сети группы в ближайшие несколько лет.

С целью обеспечения высокого качества соединения, а также сокращения сроков подключения новых абонентов СТРИМ и МГТС в рамках группы компаний завершен проект по увеличению пропускной способности опорного кольца сети МГТС до 40 Гбит/с. Одновременно с этим такие же работы были проведены в отношении собственной магистральной сети "Комстар-Директ" в Москве, благодаря чему ее пропускная способность увеличена с 20 до 40 Гбит/с. Ранее "Комстар-Директ" расширил до 30 Гбит/с емкость магистральных каналов, соединяющих сеть компании с международным сегментом сети Интернет в четырех крупных узловых точках: Лондоне, Стокгольме, Амстердаме и Франкфурте.

С завершением интеграции обеих сетей и увеличения скорости опорных сетей МГТС и "Комстар-Директ" мы получаем дополнительные возможности для быстрого развития услуг широкополосного доступа в Интернет, снижения капитальных вложений и стоимости поддержки инфраструктуры. В планах группы переход на объединенную сеть с единым управлением и развитием и реализация программы модернизации "последней мили" МГТС".

Зарегистрирован пятый облигационный займ ОАО "Северо-Западный Телеком"

23 октября Федеральная служба по финансовым рынкам России осуществила регистрацию пятого выпуска процентных документарных облигаций на предъявителя ОАО "Северо-Западный Телеком". Займу присвоен государственный регистрационный номер 4-05-00119-А. Одновременно с регистрацией выпуска ценных бумаг осуществлена государственная регистрация Проспекта ценных бумаг.

Общий объем зарегистрированного выпуска ОАО "СЗТ" составляет 3 млрд руб. Период обращения облигаций — 5 лет, с возможностью досрочного погашения облигаций по желанию Общества в любую из дат выплаты купонного дохода по облигациям в период с 728-го по 1729-й день с даты начала размещения облигаций. Размер премии, выплачиваемой при досрочном погашении, составляет 2 руб. 50 коп. на одну облигацию.

Цена размещения одной облигации устанавливается равной номинальной стоимости и составляет 1 000 руб. за одну облигацию. Процентная ставка по первому купону будет определяться как сумма двух слагаемых:

— ставка MosPrime Rate на срок 3 месяца, установленная в последний рабочий день перед датой начала размещения выпуска;

— премия к ставке MosPrime Rate на срок 3 месяца.

"АМТ" подключает автопарк "Телеком Клуб" к Системе мониторинга и навигации

Проект предусматривает оборудование 120 автомобилей компании "Телеком Клуб" системами радиосвязи на базе сети профессиональной подвижной радиосвязи и создание системы мониторинга транспорта. Для приема и распределения заказов по автомобилям компания "АМТ" установила ПО на рабочих местах специалистов "Телеком Клуб". После авторизации диспетчер имеет возможность выбрать объекты, за которыми будет осуществляться мониторинг, из числа зарегистрированных. Также возможно осуществлять контроль над автомобилями используя только web-интерфейс. Диспетчер имеет возможность определять зоны транспортной доступности, рекомендовать оптимальный маршрут, получать оперативную информацию об автоматически выявленных нарушениях заданных режимов работы.

Внедрение системы мониторинга позволяет повысить эффективность функционирования диспетчерских служб, снизить затраты на транспортное обслуживание, повысить безопасность перевозок, исключить использование автотранспорта не по назначению, качественно улучшить систему информационного сопровождения перевозки людей и грузов, улучшить качество транспортного обслуживания клиентов.

Сетям кабельного телевидения теперь доступны скорости в 200 Мбит/с и выше

CISCO И UPC BROADBAND УСТАНОВИЛИ НОВЫЙ МИРОВОЙ РЕКОРД СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ ДЛЯДОМАШНИХ ПОЛЬЗОВАТЕЛЕЙ КАБЕЛЬНОГО ТВ.

В кабельной телевизионной сети UPS в Амстердаме была показана скорость в 120 Мбит/с. Скорости, характерные для оптического волокна, были достигнуты в коаксиальных кабелях в результате первого в Европе внедрения технологий EuroDocsis 3.0 (ED 3.0) и M-CMTS в существующей операторской сети. О новом рекорде было объявлено на проходившей 7-11 сентября в Амстердаме конференции IBC, которая считается самой крупной в Европе отраслевой выставкой для вещательных компаний и широкополосных операторов. Успех Cisco и UPC Broadband показывает, что сетям кабельного телевидения вполне доступны скорости в 200 Мбит/с и выше.

Cisco и UPC первыми внедрили технологии Eurodocsis 3.0 и M-CMTS в ходе пилотного проекта в одном из жилых пригородов Амстердама. Испытания новых технологий проходили в существующей гибридной волоконно-коаксиальной сети UPC с использованием самой современной модульной архитектуры модемной терминации M-CMTS и технологии пакетирования каналов ED 3.0.

Скорости, намного превышающие 120 Мбит/с, были показаны в самом начале испытательного проекта. Испытания только начинаются, и после полномасштабного развертывания технологии EuroDocsis 3.0 Cisco надеется получить скорость, превышающую 200 Мбит/с.

Архитектура M-CMTS, разработанная компанией CableLabs и включенная в спецификации стандарта DOCSIS 3.0, становится мощным средством поддержки широкополосных услуг нового поколения. Решение с архитектурой M-CMTS, установленное для полевых испытаний, включает устройства Cisco uBR10000 Series CMTS (считаются одними из лучших в отрасли).

В Стамбуле реализуется стратегия "цифрового города"

Мэр Стамбула Кадир Топбас и президент компании Cisco по работе на развивающихся рынках Пол Монтфорд открыли новый web-портал, разработанный специалистами Cisco и некоммерческой организацией One Economy Corporation. Новый портал, получивший название Turkey Beehive (букв. — турецкий улей), был создан подразделением Cisco по разработке решений для электронного бизнеса (IBSG) в рамках программы "цифрового города", реализуемой в Стамбуле. Портал был разработан с учетом серии опросов населения, позволивших определить, какая именно информация нужна гражданам в первую очередь.

Доступ к порталу предоставляется всем жителям Стамбула через подключенные общественные центры. Портал состоит из восьми разделов: "Деньги", "Физкультура и здоровье", "Образование", "Работа", "Как открыть свой бизнес", "Семья", "Дом", "Органы власти".

На портале Turkey Beehive публикуется полезная информация о том, как строить семейный бюджет, вести здоровый образ жизни, лечить наиболее распространенные болезни и готовить детей к школе. При этом жителям города предоставляется информация, адаптированная к особенностям того или иного района.

Официальное открытие портала Turkey Beehive состоялось в новом центре BelNet — одном из трех пилотных технологических центров, созданных компанией Cisco при поддержке Турецкого фонда информатизации. В центра установлены следующие технологические решения:

- централизованная система управления, повышающая безопасность и эффективность работы центра, и портал для аутентификации пользователей и сбора статистических и демографических данных;
- рекламно-информационные панели Cisco Digital Signage для демонстрации учебного и коммуникационного мультимедийного контента на экраны, вывешенные в городских центрах;
- решение Cisco для унифицированных коммуникаций.

Стамбульский проект "цифрового города" сфокусирован на трех факторах: повышении производительности труда и качества индивидуальных, корпоративных услуг, а также ускорении социально-экономического развития. Для решения этих задач в городе началось повсеместное развертывание широкополосных сетей.

TANDBERG и Hewlett-Packard открывают двери в мир телеприсутствия

ВИДЕОКОММУНИКАЦИОННЫЙ ШЛЮЗ HALO GATEWAY СВЯЗЫВАЕТ КОРПОРАТИВНЫЕ СТУДИИ ТЕЛЕПРИСУТСТВИЯ HP И ОБЫЧНЫЕ СИСТЕМЫ ВИДЕОКОНФЕРЕНЦСВЯЗИ, РАЗРАБОТАННЫЕ НА ОСНОВЕ ОТКРЫТЫХ СТАНДАРТОВ.

Данное решение обеспечивает "бесшовную" интеграцию систем телеприсутствия (HP) и решений по ВКС (TANDBERG).

В последнее время интерес к решениям по телеприсутствию заметно растет, а вместе с ним возрастает и потребность в более полном раскрытии потенциала таких решений. Halo Gateway призвана решить именно эту задачу.

Для компаний, выбирающих системы телеприсутствия, наилучшую защиту инвестиций гарантируют решения, максимально повышающие гибкость и производительность в масштабах всей организации. Halo Gateway — это первый результат серьезных совместных усилий, которые и дальше будут направлены на неуклонное расширение возможностей видеокоммуникационных решений HP и TANDBERG.

Решение Halo Gateway разработано в рамках программы партнерства компаний TANDBERG и HP, стартовавшего в январе 2007 г. Целью данного партнерства является достижение полной совместимости разработок и решений обеих компаний в области видеосвязи, видеоконференцсвязи и телеприсутствия. В итоге, заказчики получат возможность беспрепятственного видеообщения с использованием всего спектра видеорешений — от студий телеприсутствия HP Halo Collaboration до разнообразных систем ВКС компании TANDBERG для конференц-залов, переговорных комнат и персонального использования. При этом от заказчика не потребуются дальнейшие инвестиции во внутренние ИТ-ресурсы и развитие корпоративных сетей связи.

В состав Halo Gateway входят: кодек TANDBERG 6000 MXP, устройство подключения TANDBERG Video Switch, система Halo compositor, сервер HP ProLiant и ПО, разработанное компанией Hewlett-Packard.

TANDBERG последовательно расширяет поддержку видеосистем разных производителей

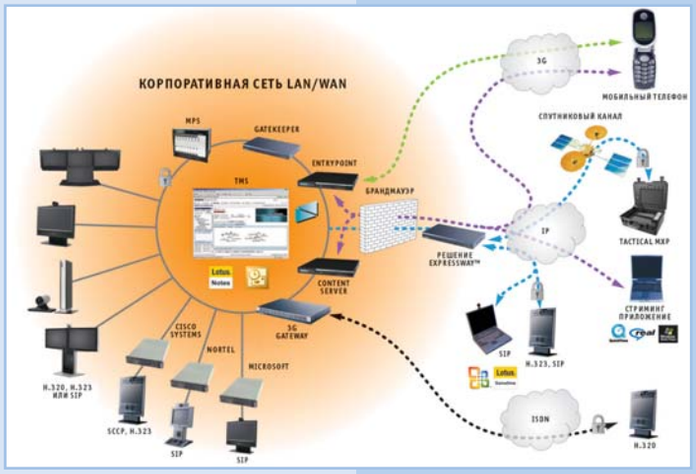
ПРОГРАММНЫЙ КОМПЛЕКС TANDBERG MANAGEMENT SUITE (TMS) ОБЕСПЕЧИВАЕТ УПРАВЛЕНИЕ СЕРВЕРАМИ МНОГОТОЧЕЧНОЙ ВИДЕОКОНФЕРЕНЦСВЯЗИ CODIAN (CODIAN MULTIPOINT CONTROL UNITS) И ТЕРМИНАЛЬНЫМ ВИДЕООБОРУДОВАНИЕМ SONY.

Компания TANDBERG объявила о поддержке продуктов Codian и Sony программным комплексом для управления видеосетями TANDBERG Management Suite (TMS). В первой половине 2008 г. будет добавлена поддержка систем Polycom HDX Благодаря этим усовершенствованиям заказчики, использующие оборудование разных поставщиков, смогут эффективнее управлять своими видеосетями.

Системы управления с реальной поддержкой оборудования разных производителей, такие как TMS, позволят системному администратору легко и эффективно конфигурировать системы и управлять большим количеством видео устройств независимо от того, кем они были изготовлены. Это ключ к дальнейшему расширению сферы использования видеосвязи.

TMS является самым совершенным программным комплексом для управления видеосетями и планирования использования их ресурсов. Этот комплекс позволяет предприятию получить максимальную отдачу от средств, вложенных в оборудование, вне зависимости от типа используемых устройств видеоконференцсвязи.

TANDBERG Management Suite (TMS), уже поддерживающий широкий набор оборудования разных производителей, с ноября 2007 г. поддерживает ряд продуктов Sony и Codian. Поддержка систем Polycom HDX запланирована на первую половину 2008 г.



Symantec делает очередной шаг навстречу конечным пользователям

Корпорация Symantec объявила об открытии интернет-магазина для конечных потребителей. В новом интернет-магазине каждый желающий сможет, не тратя на это дополнительного времени, приобрести самые популярные пользовательские решения от Symantec — Norton Internet Security, Norton 360 Norton AntiVirus и др. Посетители магазина смогут в режиме online сравнить функциональные возможности всех имеющихся в наличии продуктов и выбрать оптимальное средство защиты для своего компьютера.

Каждый покупатель интернет-магазина Symantec будет иметь возможность приобрести как коробочную, так и download-версию продукта и начать им пользоваться непосредственно в день оформления заказа. Пользователи предыдущих или OEM версий теперь смогут, используя удобный интерфейс, продлить лицензию, или приобрести последнюю версию продукта. При этом, если клиент магазина уже использует по крайней мере один продукт Symantec для дома или домашнего офиса, то при обновлении до последней версии или приобретении других продуктов, он сможет получить скидку до 40%.

Первый в мире приемник HDMI1.3 с четырьмя входами компании NXP

Новая интегральная микросхема позволяет обойтись без внешнего переключателя, ускорить проектирование телевизионных приемников и снизить их себестоимость.

Новый однокристальный приемник HDMI 1.3, TDA19978HL позволяет существенно повысить качество принимаемых аудио- и видеосигналов и снизить себестоимость аудио/телевизионных приемников high-definition, HD. TDA19978HL является первым в отрасли приемником HDMI 1.3 с четырьмя входами, позволяя обходиться без внешнего переключателя HDMI. Благодаря такой конструкции сокращается общая себестоимость систем и сроки их разработки, ускоряется выход новой продукции на рынок.

При разработке HDMI1.3 специально учитывалась необходимость повышения качества аудио- и видеопотоков высокой четкости. Глубина цвета составляет 12 разрядов, используется сочетание нового метода формирования изображения Deep Color и технологии Extended Gamut для воспроизведения натуральных цветов, поддерживаются аудиоформаты High Bit Rate (HBR) и Direct Stream Transport. Микросхема TDA19978 также позволяет снизить общую себестоимость телевизионных приемников высокой четкости благодаря наличию встроенной памяти EDID для каждого из четырех независимых входов HDMI.

HDMI1.3 TDA19978 поддерживает частоту сигнала до 2,3 ГГц, что обеспечивает воспроизведение всех форматов телевидения высокой четкости, в том числе телевизионное разрешение 1080 пикселов / 60 Гц и разрешение дисплея ПК UXGA (1600 на 1200 точек), 60 Гц. TDA19978 выпускается в компактном корпусе HLQFP144 с небольшим количеством разъемов.

ESET NOD32 получил награду лаборатории Virus Bulletin в тестировании на платформе Novell NetWare 6.5

ESET NOD32 ПО РЕЗУЛЬТАТАМ СРАВНИТЕЛЬНОГО ТЕСТИРОВАНИЯ АНТИВИРУСНЫХ СРЕДСТВ НА ПЛАТФОРМЕ NOVELL NETWARE, ПРОВЕДЕННОГО БРИТАНСКИМ ЖУРНАЛОМ VIRUS BULLETIN В ОКТЯБРЕ 2007 г., УЖЕ В 48 РАЗ УДОСТОИЛСЯ НАГРАДЫ "VB100".

Лаборатория Virus Bulletin является наиболее авторитетным журналом, посвященным проблемам борьбы с компьютерными вирусами и вредоносным ПО. Важнейшее направление работы журнала — сравнительное тестирование эффективности средств антивирусной защиты, разработанных для различных платформ. В ходе проводимых тестирований исследуется способность антивируса противостоять действию вирусов из собственной коллекции Virus Bulletin, а также из коллекции Wild List.

Для получения награды "VB100" тестируемый антивирус должен выявить абсолютно все вирусы из коллекции Wild List, продемонстрировать высокий уровень детектирования вирусов из коллекции Virus Bulletin, а также не показать ни одного ложного срабатывания.

В октябрьском тестировании 2007 г. испытывались антивирусные продукты, предназначенные для защиты серверов под управлением Novell NetWare с предустановленным пакетом обновлений 6.5. Тестирование проводилось в два этапа — "on-access" и "on-demand". На первом этапе оценивалась эффективность антивируса при попытке вторжения вируса в систему, а на втором — эффективность продукта при обезвреживании уже проникших в систему вирусов. В обоих этапах антивирус ESET NOD32 показал высокие результаты в детектировании вирусов из коллекций Wild List и Virus Bulletin, не допустив при этом ложных срабатываний. Аналогичный результат смогли продемонстрировать лишь трое из десяти участников тестирования. При этом, ESET NOD32 продемонстрировал наивысшую скорость сканирования архивных файлов, значительно опередив по этому показателю всех конкурентов.

Сегодня Novell NetWare широко применяется в качестве серверной платформы на предприятиях различного масштаба и сфер деятельности. Этим обусловлено появление большого числа вирусов, написанных специально для этой платформы. Поэтому вопрос защиты серверов под управлением Novell NetWare особо остро стоит перед пользователями антивирусных средств. И результаты независимых испытаний проводимые лабораторией Virus Bulletin, помогут пользователю выбрать наиболее эффективный продукт.

Защита конфиденциальных данных от утечки информации

ИССЛЕДОВАНИЕ ИСПОЛЬЗУЕТ ДАННЫЕ И ВЫВОДЫ ИЗ АНАЛИТИЧЕСКОГО ОТЧЕТА КОМПАНИИ LETA: "НАВСТРЕЧУ ПЕРЕМЕНАМ: РЫНОК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 2007".

Информация получена путем опроса потребителей услуг в области защиты конфиденциальной информации от утечек — методом экспертных интервью, а также анализа публикаций в СМИ и других открытых источниках. Большую помощь при подготовке обзора оказали данные компаний IDC, PWC, Gartner, Ponemon Institute, Forrester, мировых лидеров индустрии Vontu, WebSense, InfoWatch и др.

Использован также опыт компании LETA по созданию и поддержанию систем защиты от утечек, основанный на 14 проведенных только с середины 2006 г. проектах по построению комплексной защиты от внутренних угроз и более чем на 30 проектах по защите отдельных каналов утечек.

Ключевые выводы исследования: Объем рынка ILDP растет опережающими весь рынок ИБ темпами. На 2007 г. в России он составит 26 млн долл. на 2008 г. ожидается рост на 63%, объем рынка в 43 млн долл. На российском рынке доминируют отечественные разработки (это обусловлено тем, что они "понимают" русский язык). Но в течение трех-пяти лет существенную долю могут занять западные производители.

Стремительное развитие данного сегмента сохранится и в ближайшие годы, а импульсом к росту послужат инициативы государственных органов и "саморегулирующие" механизмы отрасли — стандарты безопасности, которые принимаются в добровольном порядке и в виде обязательных документов (стандарт ЦБ РФ).

Основой каждого проекта является его экономическая целесообразность, для оценки которой необходимо использовать подход ROSI. Например, более 70% компаний из списка Fortune 1000 увеличили в 2007 г. свои расходы на информационную безопасность. Не случайно рынок ИБ развивается под влиянием стандартов отраслевых регуляторов из государственных структур и ассоциаций, которые разрабатывают и внедряют единые подходы к построению системы управления информационной безопасности (СУИБ).

Система европейских и американских стандартов, затрагивающих ИБ, в достаточной степени сложилась и позволяет стандартизировано подходить к построению СУИБ. Подобная типизация позволяет добиваться существенного уровня защищенности и гарантировать качественные показатели СУИБ.

Первая годовщина успешной деятельности компании NXP на российском рынке

РОССИЯ СТАНЕТ СТРАТЕГИЧЕСКИ ВАЖНЫМ РЫНКОМ И БАЗОЙ ДЛЯ РАЗРАБОТКИ НОВОЙ ПРОДУКЦИИ NXP.

Компания NXP Semiconductors, независимая компания по производству полупроводниковых компонентов, основанная корпорацией Philips, объявила результаты первого года своей деятельности в России и странах СНГ и поделилась планами на следующий год.

За первый год работы NXP в России объем продаж превысил средние показатели рынка полупроводниковых компонентов, которые находятся на уровне 25%. Такие значительные результаты были достигнуты благодаря привлечению в компанию новых специалистов и установлению устойчивых взаимоотношений с крупнейшими дистрибуторами и с OEM-производителями.

NXP производит полупроводниковые компоненты и решения для пяти важнейших сегментов: ***мобильные и персональные устройства*** (сотовые телефоны и инфраструктура сотовой связи, портативные мультимедийные устройства, средства связи, аудио- и видеоустройства), ***потребительская электроника*** (аналоговые и цифровые телевизионные приемники, телевизионные абонентские приставки, видеоустройства для ПК, телевизионные модули и высокочастотные решения), ***автомобильное оборудование*** (автомобильные развлекательные системы, сетевое оборудование, решения для контроля доступа к транспортным средствам и противоугонные системы, а также системы контроля давления в шинах), ***средства идентификации*** (смарт-карты, электронное правительство, радиочастотная идентификация (RFID, Radio Frequency Identification), NFC (Near Field Communication)), а также ***полупроводниковые компоненты общего назначения*** (транзисторы и диоды, дискретные элементы, логические схемы, датчики, силовые компоненты, микроконтроллеры, интерфейсы и высокочастотная продукция). В настоящее время NXP выполняет или осуществляет поддержку более 1000 проектов в странах СНГ.

Уже сейчас десятки миллионов микросхем на основе технологии NXP MiFARE используются в бесконтактных картах для оплаты проезда в московском метрополитене. Компания NXP уже обладает существенной долей рынка микросхем для аналоговых телевизионных приемников, выпускаемых такими производителями, как "Горизонт", "Витязь" и "Полар", при этом она тесно сотрудничает с местными производителями, выпускающими кабельные и наземные телевизионные абонентские приставки.

Недавно NXP подтвердила соглашение о поставке полупроводниковых технологий компании "Интеркросс", с помощью которых эта компания сможет наладить массовый выпуск телевизионных абонентских приставок для приема видео в формате MPEG2.

NXP ведет успешное сотрудничество с несколькими университетами Москвы и Санкт-Петербурга, которые занимаются исследованиями и реализацией ее проектов.

ОАО "МРС" и Alcatel-Lucent развернут многофункциональную сеть передачи данных

Alcatel-Lucent и ОАО "Мультисервисная радиосеть" (ОАО "МРС") новый московский оператор связи, объявили о планах развертывания многофункциональной широкополосной сети передачи данных в Москве и Московской области.

Alcatel-Lucent будет работать с ОАО "МРС" по определению параметров сети доступа и опорной сети и предоставит инфраструктуру полнофункциональной беспроводной широкополосной сети, которая позволит заказчику поддерживать современные услуги передачи данных, такие как мгновенные сообщения, системы видеонаблюдения, экстренного предупреждения и многие другие услуги необходимые для городских структур и служб оперативного реагирования Москвы.

Alcatel-Lucent готова предоставить компании надежные проверенные технологии, которые позволят удовлетворить требования заказчиков, особенно тех, кто призван защищать безопасность жителей Москвы.

Решение NXP используется в первом в мире сотовом телефоне на солнечных батареях компании Hi-Tech Wealth

Компания Hi-Tech Wealth (HTW) выбрала системное решение Nexperia Cellular System Solution 5110 для использования в первом в мире мобильном телефоне на солнечных батареях — S116.

Используемое в конструкторской разработке компании Laucent Technology системное решение NXP обеспечивает исключительно низкий уровень энергопотребления, что позволяет оптимизировать процесс зарядки солнечных батарей. В результате, телефон S116, массовое производство которого было запущено в июле 2007 г., демонстрирует рекордные в отрасли показатели времени работы в режиме ожидания и разговора.

Новый телефон на солнечных батареях позволяет пользователям подзаряжать батарею, используя любой источник света, даже свет свечи. Это гарантирует более длительное время работы в режиме ожидания по сравнению с любыми другими телефонами на рынке.

Разработка телефона на солнечных батареях является революционным достижением в области производства беспроводных мультимедийных устройств.

Экологически безопасное конструкторское решение — это также важный шаг на пути к созданию все более востребованных на рынке "зеленых" товаров и сервисов, которые оказывают минимальное негативное воздействие на окружающую среду.

NXP повысит безопасность немецких электронных паспортов

Компания NXP поставит свои новейшие интеллектуальные микросхемы для Германии, которая первой в мире вводит электронные паспорта второго поколения с усовершенствованной защитой. На втором этапе подготовки спецификации ePassport страны Евросоюза примут решение о включении цифровой биометрической информации в форме отпечатков двух пальцев во все электронные паспорта. NXP уже поставила компании Bundesdruckerei GmbH, выпускающей паспорта для Германии, около 4,5 млн. решений (включающих микросхему, операционную систему и вкладыш) для электронных паспортов. Компания NXP — участник более чем 80% проектов внедрения электронных паспортов по всему миру — к настоящему моменту поставила 100 млн ИС. Электронные паспорта внедряются в 51 стране, 43 из них, в том числе США, Франция и Сингапур, используют технологию интеллектуальных микросхем NXP.

Евросоюз определил крайний срок выполнения требований и внедрения электронных паспортов нового поколения — 28 июня 2009 г. Германия первой в Европе начнет переход к новой системе в ноябре 2007 г. Чтобы добавить изображения двух отпечатков пальцев в электронные паспорта, требуется процедура с повышенным уровнем безопасности (EAC), определенная Европейской комиссией. Процедура EAC в обязательном порядке поддерживает более надежные средства шифрования, позволяющие защитить конфиденциальность секретных данных и предотвратить возможность их клонирования.

продолжение на стр. 13

Customer Management Congress

CRM КОНГРЕСС — ТРАДИЦИОННАЯ ЕЖЕГОДНАЯ ВСТРЕЧА БИЗНЕС-ЛИДЕРОВ, НА КОТОРОЙ ОБСУЖДАЮТСЧ СТРАТЕГИЧЕСКИЕ ВОПРОСЫ УПРАВЛЕНИЯ ВЗАИМООТНОШЕНИЯМИ С КЛИЕНТАМИ, РАССМАТРИВАЮТСЯ УСПЕШНЫЕ ПРИМЕРЫ РЕАЛИЗАЦИИ ПРОГРАММ ЛОЯЛЬНОСТИ И ПОСТРОЕНИЯ КЛИЕНТОРИЕНТИРОВАННОЙ МОДЕЛИ БИЗНЕСА.

В Москве прошел IV Международный Конгресс "Управление отношениями с клиентами", на котором были представлены успешные российские и зарубежные CRM-проекты в самых различных отраслях бизнеса.

Более 80 докладчиков и участников панельных дискуссий — это представители топ-менеджмента ведущих российских и зарубежных компаний. Форум предоставил уникальную возможность в режиме интерактивного общения с лидерами рынка перенять опыт, задать острые и интересные вопросы, услышать мнение экспертов, аналитиков и консультантов. Участники Конгресса в этом году представлены бизнес-лидерами от ведущих компаний: финансовых учреждений, в том числе банков, страховых и инвестиционных компаний, крупнейших операторов сотовой и фиксированной связи, риелтеров, транспортных компаний, аэропортов, предприятий сферы туризма и отдыха, гостиниц, магазинов розничной и оптовой торговли и др.

Конгресс собрал более 500 участников из 10 стран: России, Украины, Казахстана, Беларуси, Киргизии, Азербайджана, стран Европейского союза и других государств.

"Взлеты и падения CRM-индустрии последние несколько лет требуют решения множества задач, обхождения подводных камней, грамотного консультирования, обмена успешным опытом и экспертизы. Самое важное, что участники получают на форуме — это деловое общение и опыт лидеров", — считает Дмитрий Аристархов, главный продюсер Exposystems part of Expomedia Group Plc (компании-организатора Конгресса).

Ежегодная конференция Nortel Forum 2007

В ЦЕНТРЕ ВНИМАНИЯ ПОСЛЕДНИЕ ТЕНДЕНЦИИ ИКТ ИНДУСТРИИ — UNIFIED COMMUNICATIONS И HYPERCONNECTIVITY

Форум является одним из крупнейших корпоративных мероприятий компании и ежегодно предоставляет уникальную возможность всем, кто интересуется развитием глобального телекоммуникационного рынка, встретиться и обсудить последние тенденции развития мировой ИКТ-индустрии.

Nortel зарекомендовал себя как инновационная компания, предоставляющая новейшие телекоммуникационные технологии как операторам связи, так и корпоративным заказчикам в области передачи данных и телефонии. Форум объединяет все эти направления и технологии и позволяет обсудить как общие тенденции развития отрасли — гиперподключенность (Hyperconnectivity), так и технологии, объединяющие различные направления отрасли — унифицированные коммуникации (Unified Communications).

Помимо партнеров и заказчиков Nortel, в конференции ежегодно принимают участие представители государственных органов, финансовых организаций и консалтинговых агентств, крупнейших ИКТ-компаний и провайдеров телекоммуникационных услуг, СМИ.

Ключевые спикеры форума — топ-менеджеры Nortel, которые представили стратегию компании на 2008 г. Представители глобальных партнеров Nortel (Microsoft и IBM) выступили с докладами об унифицированных коммуникационных системах и сервис ориентированной архитектуре.

Особое внимание было уделено результатам деятельности стратегического альянса Nortel-Microsoft по созданию совместных решений в области унифицированных коммуникаций, а также обсуждению концепции гиперподключенности, которую в компании Nortel определяют как состояние среды, в которой число устройств, активных RFID-меток и приложений, подключенных к сети, намного превосходит число людей, использующих сеть для передачи данных.

Официальными партнерами Nortel Forum стали компании: BELTEL, IBS/Platformix, INLINE Technologies, KPOK, Golden Telecom, OCS, Soft-Tronik, Teleopti, а также тренинг-центры BELTEL, DIONA Master Lab и RedCenter.

"Склад. Транспорт. Логистика-2007"

В ЦВК "ЭКСПОЦЕНТР" (МОСКВА) ПРОШЛА 14-я МЕЖДУНАРОДНАЯ ВЫСТАВКА СИСТЕМ ЛОГИСТИКИ, ТРАНСПОРТНОГО ОБСЛУЖИВАНИЯ, СРЕДСТВ АВТОМАТИЗАЦИИ И МЕХАНИЗАЦИИ СКЛАДСКИХ И ПОГРУЗОЧНО-РАЗГРУЗОЧНЫХ РАБОТ — "СКЛАД. ТРАНСПОРТ. ЛОГИСТИКА-2007".

Важнейший для экономики России выставочный форум был организован под патронатом Торгово-промышленной палаты РФ и Правительства Москвы, при участии и содействии структур Министерства транспорта РФ, Федеральной таможенной службы, Министерства сельского хозяйства РФ.

В этом году выставка достигла своего рекордного уровня: на площади около 5600 м^2 около 240 участников из 24 стран мира представили современную технику, услуги и решения.

Широко были представлены отечественные складские, транспортные и логистические компании, в числе которых — Ant Technologies; Солво, Максстор, ДатаКрат-Е, Глобал Ориент, Складские технологии и логистика, ГК "Севертранс", Межтрансавто, NaviCon, Шелвер и др.

Основные тенденции современного рынка диктуют предприятиям необходимость постоянного совершенствования бизнеса и снижения логистических издержек. В связи с этим растут требования и к программному обеспечению, особенно в части специализированного прикладного функционала WMS. Сотрудники LogistiX отметили укрепление тенденции использования излишков складских площадей для оказания услуг ответственного хранения. В связи с этим, представители потенциальных заказчиков интересовались возможностью совмещения в системе функций управления процессами оперативной логистики производственного предприятия или распределительного центра с функционалом ведения договоров (Contract Management) и биллинга, что реализовано специалистами компании LogistiX в системе "LEAD WMS 3PL+".

В целом для компании LogistiX и других участников Международная выставка "СТЛ-2007" стала площадкой для делового общения, где можно найти не только новых клиентов, но и развивать сложившиеся партнерские взаимоотношения и обменяться опытом с коллегами.

В выставке приняла участие также компания Ant Technologies, представившая Logistic Vision Suite — комплекс продуктов для управления складом (WMS) и цепочкой поставок в целом. Эта система предназначена для автоматизации логистических бизнес-процессов крупных предприятий и ориентирована на развитие бизнеса компаний, работающих в различных сегментах. Компания представила также Radio Beacon WMS — систему управления складом в реальном времени с малыми сроками установки и быстрым возвратом инвестиций. Рынок ИТ-решений для логистики очень динамичен, и характеризуется постоянным появлением новых, специфических требований клиентов. Компания Ant Technologies представила два новых решения в области автоматизации логистики: Syncron DF&RP — решение в области планирования цепочки поставок и Pick to light — систему безбумажного отбора заказов.

Следует отметить также экспозицию компании NaviCon — Золотого Партнера Microsoft. Компания специализируется на оказании профессиональных консультационных услуг по внедрению ERP, CRM, WMS, BPM-систем — Microsoft Dynamics NAV, Microsoft Dynamics AX, Microsoft Dynamics CRM, Plan Designer, Cognos, BasWare, Radio Beacon и предлагает широкий перечень услуг и сервисов, связанных с постановкой учета, процессами автоматизации деятельности предприятия. В комплекс услуг, оказываемых компанией NaviCon, входят все виды работ по внедрению ERP-систем, начиная с проведения предпроектного обследования и формирования рекомендаций по оптимизации бизнес-процессов и заканчивая непосредственно внедрением систем и последующей поддержкой.

"СТЛ-2007" продемонстрировала новые проекты и оборудование в складском, транспортном и экспедиторском бизнесе при решении комплекса логистических задач. В рамках выставки проводился комплекс научно-практических мероприятий по всем тематическим направлениям. Деловая программа выставки позволила обсудить самые наболевшие проблемы отрасли, найти решения, обеспечивающие защиту интересов отечественных транспортных операторов и транспортной системы России в целом.

Неуклонный рост числа посетителей свидетельствует о росте интереса к выставке, которая является местом делового общения специалистов в области, ставшей за последнее десятилетие насущно необходимой.

Микросхемы SmartMX полностью поддерживают требования к ИБ, установленные в спецификации EAC, и предоставляют ряд расширенных функций для приложений eGovernment.

Эта микросхема прошла сертификацию в соответствии с наивысшим уровнем Общих критериев (CC), установленных Федеральным ведомством Германии по информационной безопасности (Bundesamt fur Sicherheit in der Informationstechnik). Благодаря использованию асимметричной криптографии на базе эллиптических кривых обеспечивается хранение и безопасность информации, содержащейся в ИС. Емкость запоминающего устройства EEPROM (перепрограммируемое ПЗУ с электронным стиранием) каждой микросхемы составляет 80 кб, что позволяет включить в документ биометрические данные, например фото владельца, отпечатки пальцев, имя, дату, страну рождения, однозначно идентифицирующие владельца паспорта.

SmartMX содержат ряд уникальных функций ИБ, предохраняющих от атак с использованием источника света и лазеров, а также специализированный аппаратный межсетевой экран, защищающий определенные разделы микросхемы. Кроме того, в этих ИС удалось повысить скорость чтения и записи за счет оптимизации оборудования и ПО, что примерно в 3 раза ускоряет персонализацию паспортов по сравнению с их первым поколением. Возможна поставка микросхем SmartMX компании NXP в самом тонком для отрасли корпусе (250 мкм), что обеспечивает удобство их использования в разнообразных бесконтактных приложениях eGovernment.

Nokia Siemens Networks и Intel дополняют решение IPTV функциями Home Networking

Использование стандартов UPnP (Universal Plug and Play) и DLNA (Digital Living Network Alliance) в домашних сетях открывает новые возможности для обмена фотографиями, видео и другими типами мультимедийных файлов, хранящихся на ПК — на экране телевизоров. Некоторые из этих функций IPTV реализуются с помощью процессорной технологии Intel®Viiv для потребительских ПК, ориентированных на цифровые развлечения.

Комплексное решение IPTV компании Nokia Siemens Networks позволяет существенно расширить спектр предоставляемых пользователям услуг, а также повысить удобство их применения и управления. Оно состоит из головной телевизионной станции, системы управления цифровыми правами и закрытия контента, сервера контента и приставки к телевизионному приемнику. Наряду с возможностью выбирать, смотреть и записывать обычные телевизионные программы через интерфейс электронного навигатора (EPG), пользователям доступны услуги по загрузке контента, интерактивные игры, программные средства на базе web-технологий.

Современные ПК на базе технологии Intel Viiv оснащаются двух- и четырехядерными процессорами, интегральными микросхемами а также программным и аппаратным обеспечением.

Функции Digital Home Networking, решения IPTV компании Nokia Siemens Networks, позволяют просматривать контент персональных компьютеров с домашних телевизионных приемников, оснащенных приставкой. Благодаря технологии Intel® Smart Streaming, пользователи могут использовать свои телевизионные экраны для просмотра видео, хранящегося на персональных компьютерах.

CA Storage Day

КОМПАНИЯ CA ПРОВЕЛА ЕЖЕГОДНУЮ КОНФЕРЕНЦИЮ ДЛЯРОССИЙСКИХ ПАРТНЕРОВ — STORAGE DAY. В ЭТОМ ГОДУ ОНА ПОСВЯЩЕНА ТЕМЕ УПРАВЛЕНИЯ ВОССТАНОВЛЕНИЕМ ДАННЫХ — RECOVERY MANAGEMENT.

В мероприятии принял участие глобальный партнер CA — компания Sun Microsystems, которая представила преимущества совместного решения для хранения данных Sun и ПО для постоянной защиты данных CA XOSoft.

В исследовании "Recovery Management", проведенном для CA независимой консалтинговой компанией Gyro International весной 2007 г., отмечается растущий спрос на менее сложный по структуре подход к резервированию данных. 91% опрошенных утверждают, что неоспоримым плюсом является постоянное резервирование. Однако только 40% опрошенных IT-менеджеров либо уже используют CDP (постоянную защиту данных), либо планируют внедрить эту систему в течение ближайшего года.

В связи с постоянно растущим объемом информации и строгими нормами соответствия, на средства защиты данных и их доступность возлагаются высокие требования. Традиционные средства защиты данных не справляются с задачами. Компания CA предлагает модульное решение для управления восстановлением, которое сочетает дублирование, аварийное восстановление, непрерывную защиту данных, автоматическое преодоление отказа для высокой готовности. Все это интегрируется в единый пакет, который обеспечивает защиту критически важных данных и сокращает время простоя.

Многофункциональное решение CA Recovery Management, разработанное специально для среднего бизнеса, упрощает и автоматизирует резервирование и восстановление данных, позволяя контролировать расходы и уменьшать сложность операций, связанных с резервированием. Кроме того, благодаря этому решению можно минимизировать риски и добиться соответствия требованиям развития бизнеса, одновременно повысив доступность данных, приложений и эффективность работы пользователей

На мероприятии выступили зарубежные специалисты CA: Роберт Дэвис, старший вице-президент и генеральный менеджер, руководитель решений Storage для среднего бизнеса CA, Артур Фритц, ведущий консультант департамента технических продаж по решениям в области систем хранения данных, CA EMEA, и Танги Де Ла Ори, вице-президент CA по продажам через партнерскую сеть, CA EMEA. В программу мероприятия вошли практические семинары по решениям компании в области систем хранения данных, включая резервирование, восстановление и постоянную защиту информации.

Мероприятие прошло при поддержке MONT и Interprocom Lan.

Nokia Siemens Networks сертифицировала оборудование для систем связи 3-го поколения

Компания Nokia Siemens Networks получила российский сертификат соответствия на оборудование подсистемы базовых станций для сетей мобильной связи третьего поколения стандарта UMTS с поддержкой технологии HSDPA и HSUPA. Сертификат соответствия был выдан Органом по Сертификации АНО "ЦЭС" Инфоком". Срок действия сертификата с 25 сентября 2007 г.

Согласно полученному сертификату соответствия, оборудование подсистемы базовых станций для сетей мобильной связи 3-го поколения (включая функциональность HSDPA и HSUPA) производства Nokia Siemens Networks признано соответствующим установленным требованиям "Правил применения оборудования базовых станций и ретрансляторов систем подвижной радиотелефонной связи стандарта UMTS", утвержденных приказом Миниформсвязи России №102 от 27.08.2007 г.

Инфофорум-Поволжье-2007

1-я МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ И ВЫСТАВКА В ПРИВОЛЖСКОМ ФЕДЕРАЛЬНОМ ОКРУГЕ.

В очередной раз ставший уже традиционным "Инфофорум" объединил на региональном уровне представителей государственных структур и ведущие российские компании, работающие в сфере обеспечения информационной безопасности. Форум организован Комитетом Государственной Думы РФ по безопасности, Аппаратом Полномочного представителя Президента РФ в Приволжском Федеральном округе, Аппаратом Губернатора и Правительства Нижегородской области, Федеральным агентством по промышленным технологиям и Некоммерческим партнерством "Инфофорум".

Информационные технологии относятся к важнейшей части общественной жизни государства. Россия уверенно вступила на путь построения информационного общества. В июле 2007 г. при участии Мининформсвязи России утверждена Стратегия развития информационного общества. Главным результатом реализации которой станет реальное повышение качества жизни населения, формирование открытого общества и создание условий для дальнейшего развития демократических процессов в России. Важнейшую роль в этих процессах занимает задача обеспечения информационной безопасности и защиты информационных ресурсов.

Сделаны существенные шаги по развитию системы электронных государственных услуг. Правительство РФ на своем заседании в августе 2007 г. одобрило Концепцию формирования электронного правительства до 2010 г., среди ключевых моментов которой — создание защищенной системы межведомственного электронного документооборота. В ходе реализации Концепции большое внимание уделяется вопросам обеспечения информационной безопасности.

Символично, что "Инфофорум-Поволжье" прошел в одном из крупнейших военно-промышленных центров страны — Нижнем Новгороде — в городе с без малого восьмисотлетней историей, славном своим историческим прошлым, динамичным настоящим и весьма перспективным будущим. Практические шаги по внедрению безопасных информационных технологий во многом определяются развитием и внедрением разработок на региональном уровне.

В России в настоящее время созданы все технологические условия перехода от бумажных к электронным технологиям поддержки государственного управления всех ветвей и уровней власти, т. е. к "электронному государству". ФЦП "Электронная Россия (2006-2010 гг.)" предусматривает повышение эффективности государственного управления на основе создания высокозащищенной информационно-технологической инфраструктуры, использующей современные технологии информационной безопасности и формирующей доверительную среду информационного обмена, как на межведомственном уровне, так и для предоставления государственных услуг для бизнеса и населения.

"Инфофорум-Поволжье" способствует внедрению новейших отечественных разработок в сфере информационных технологий, построению систем комплексной информационной безопасности не только в Приволжском федеральном округе, но и во всех регионах РФ. Впервые на региональном уровне рассмотрены конкретные проблемы развития информационных технологий и информационной безопасности и найдены пути их решения в отдельных отраслях региональной экономики.

Участие в Межрегиональной конференции и выставке широкого круга представителей органов государственной власти федерального уровня и всех 14 субъектов РФ, входящих в Приволжский федеральный округ, создает условия для всестороннего обсуждения насущных организационных, правовых, технических проблем в деле построения информационного общества и обеспечения информационной безопасности в России, для обмена передовыми идеями и опытом, выработки эффективных решений.

На Форуме обсуждались вопросы информационной безопасности и национальной экономики, регионального развития, информационного обеспечения деятельности органов власти в субъектах РФ и органов местного самоуправления, комплексные решения в сфере информационной безопасности на предприятиях промышленности, транспорта и связи, проблемы защиты персональных данных.

В рамках Форума прошла церемония награждения победителей Всероссийского конкурса электронных СМИ в Приволжском федеральном округе "За освещение проблем развития информационного общества в России".

Nortel и Polycom дополнят спектр решений Unified Communications средствами HD Video и Telepresence

Действуя на основе анонсированного в мае 2007 г. глобального соглашения о дистрибуции и сервисном обслуживании, компания Nortel ввела в эксплуатацию демонстрационную сеть, позволяющую потенциальным заказчикам из всех стран мира лично убедиться в преимуществах подлинного телеприсутствия.

Унифицированная коммуникационная система, созданная совместно компаниями Nortel и Polycom, позволяет одним щелчком компьютерной мыши получить доступ не только к функциям телефонной связи, мгновенного обмена сообщениями и электронной почты, но и к средствам видеоконференцсвязи в режиме HD Video.

Благодаря проведенной компаниями интеграции платформ Polycom RMX 2000 Real-Time Media Conferencing Platform и Nortel Multimedia Communication Server (MCS) 5100 пользователи клиентского решения Nortel MCS могут организовывать сеансы голосовой связи, видеоконференцсвязи и обмена контентом высокой четкости в реальном масштабе времени, причем как в двухточечном (point-to-point), так и в многоточечном (point-to-multipoint) режиме.

Демонстрационная сеть компании Nortel контролируется из восьми мультимедийных центров управления сетью, расположенных в разных странах мира. К концу 2007 г. она объединит почти 30 площадок, среди которых развернутые компанией Nortel комплексы Polycom RealPresence Experience (RPX) во Франкфурте, Нью-Йорке, Торонто, Далласе и Роли (штат Северная Каролина). Запланировано также открытие дополнительных площадок в Лондоне, Пекине, Нью-Дели, Сингапуре и Чикаго.

КРУГЛЫЙ СТОЛ

Системная интеграция: комплексное видение достоинств и недостатков вендоров

Сергей Головин

Валерий Андреев

Сергей Щербина

Общеизвестно, что современные предприятия все больше зависят от информационных систем, и чем дальше, тем эта зависимость прочнее. Компании, работающие на совершенно разных рынках, создают центры обработки данных, внедряют системы управления предприятием и CRM-системы, налаживают сквозную финансовую отчетность и внедряют интегрированные системы бизнес-процессов, охватывающие все подразделения и территориальные единицы организации. На эти общие тенденции накладывается специфика отраслей и стремление ускорить внедрение, точнее оценить и максимально повысить возврат инвестиций. Все это приводит к изменениям на ИТ-рынке. И, в частности, к изменению отношений между интеграторами и вендорами как основными участниками процесса создания и внедрения ИТ-решений.

Рассказать об этих изменениях редакция попросила Валерия Андреева, директора по науке и развитию компании ИВК, Сергея Головина, заместителя генерального директора по маркетингу компании "Энвижн Груп", и Сергея Щербину, директора по маркетингу компании "Квазар-Микро".

1. Современные технологии, оборудование и ПО становятся все сложнее, причем в сфере бизнес-систем верхнего уровня вендоры стремятся сделать свои продукты проводником наилучших практик на местные рынки. Не становится ли тогда интегратор простым проводником технологий вендора? Или, напротив, с ростом сложности элементов требуется все более высокая квалификация, чтобы создать из них эффективное решение?

СЕРГЕЙ ГОЛОВИН: Верны оба ответа — это две стороны одной медали. Да, в основном, российские системные интеграторы сегодня внедряют технологии и продукты, разработанные за рубежом (хотя есть и исключения). И именно там производители отрабатывают свои решения, создают их отраслевые модификации (если говорить об информационных системах) или доводят до "блеска" в процессе внедрения в крупных инфокоммуникационных системах. Хотя сейчас уже и не редки случаи, когда самые новейшие технологии начинают впервые внедряться и в России.

При этом все эти новейшие технологии так сложны, что без квалифицированных специалистов, а в России — это специалисты интеграторских компаний, — внедрение просто невозможно. Это тем более касается информационных систем — достаточно упомянуть уже набившие оскомину "особенности российской экономики и практики ведения дел". Именно быстрое усложнение технологий и необходимость использования для их внедрения специалистов высокого класса вызвало, в частности, значительный кадровый кризис на ИТ-рынке, когда спрос на квалифицированные кадры значительно превышает предложение.

ВАЛЕРИЙ АНДРЕЕВ: Для вендора стремление стать проводником наилучших практик понятно. Ведь выйдя на уровень бизнес-решений, он попадает в сферу гораздо более высоких норм прибыли,

чем при поставках ПО и оборудования. Но есть масса нюансов в слове "практика". И нюансы эти касаются возможности и целесообразности переноса чужой бизнес-практики в новую среду. Ведь бизнес-практика — это не просто алгоритм: это и стиль ведения бизнеса, и социальная среда внутри компании и на рынке в целом, и закрепленные в менталитете человека представления о допустимых отклонениях от формализованных процедур и регламентов. Если говорить о России, то здесь все еще сложнее: без серьезных изменений почти никакая практика не может быть перенесена на наши реалии. Тем более практика, выработанная в неблизкой нам экономической среде и достаточно давно. Поэтому интегратор не приближается, а удаляется от состояния простого проводника. Ведь что не существует таких западных продуктов, которые легко и просто "легли" бы на местные рынки, особенно на российский. Наш опыт однозначно показывает, что при внедрении стандартизованной бизнес-системы в РФ приходится переделывать заново практически все. В общем, работы у интегратора всегда будет много.

Естественно, и ответ на второй вопрос — положительный. Все более глубокая квалификация интегратора требуется не только для реализации местной практики, но и для критического осмысления того многообразия предложений вендора, которое предстоит адаптировать под реальные условия.

СЕРГЕЙ ЩЕРБИНА: Задача системного интегратора — выбор и реализация оптимального для заказчика решения, наилучшим образом удовлетворяющего его бизнес-потребности и вписывающегося в отведенный бюджет. Для этого требуется не только тщательный анализ продуктов, предлагаемых вендорами, но и способность адекватно трансформировать их с учетом отраслевой специфики. А это возможно только при условии понимания особенностей бизнеса именно на локальном рынке. Естественно, вендоры ведут самостоятельную работу с заказчиком и стремятся продвинуть свои платформы, не всегда имея возможность глубоко погрузится в долгосрочную стратегию заказчика, объективно существующие рамки бизнеса, связанные, например, с имеющимися предпочтениями и корпоративной политикой. В свою очередь интегратор глубже "сидит" в инфраструктуре и проблематике заказчика, лучше понимает его видение ИТ-стратегии, и в нужный момент готов предложить свои компетенции в продуктах и технологиях вендоров. Вместе с тем, прямое общение заказчика с вендором часто оказывается продуктивно в том случае, если ИТ-стратегия заказчика четко определена на годы вперед.

2. На современном рынке есть как примеры разработки интегратором собственного продуктового портфеля, так и примеры консалтингового участия вендора в проектах. Свидетельствует ли это о новой тенденции размывания грани между моделями бизнеса вендора и интегратора или интеграторы стремятся "переквалифицироваться" в вендоры?

СЕРГЕЙ ЩЕРБИНА: Сейчас немного компаний, которые можно назвать "чистыми" интеграторами, или "чистыми" вендорами. И вендор, и интегратор заинтересованы в успешном завершении внедрения и в финансовой отдаче ИТ-проекта, а значит стремятся предлагать комплексные решения и свою компетенцию по их реализации. Консалтинговая составляющая проектов неуклонно повышается, поэтому при реализации сложных, уникальных проектов необходимо объединение знаний и опыта партнера и вендора. Где не хватает экспертизы партнера, включаются разработчики и сервисные специалисты вендора; где продукт не дотягивает до требований заказчика, команда интегратора берет на себя "доводку" продукта.

Причем такая "доводка" идет по всему "фронту" — от технологий бизнеса и отраслевой специфики до внедрения и обслуживания. Наша компания выдвигает на рынок свои собственные разработки и отраслевые решения, выходя за рамки классического портфеля услуг системной интеграции. Разработка своих продуктов — часть стратегии компании, и под этот портфель строятся, конечно, новые модели его продвижения на рынок, сходные с "вендорской" моделью.

ВАЛЕРИЙ АНДРЕЕВ: Глубокий анализ и сопоставление того, что нужно заказчику, с тем, что предлагает вендор, часто ставит интегратора в тупик именно глубиной различий реальной практики и практики, импортируемой извне. И глубина этих различий может достичь той черты, когда лучше сделать свой продукт, взяв у вендора основной функционал системы. При этом вопрос о том, что именно взять под конкретный проект, решается интегратором и вендором совместно. Кроме того, подтолкнуть к разработке собственного решения может подтолкнуть и излишне жесткая позиция вендора.

Хочу особо подчеркнуть, что все эти "болячки" происходят оттого, что у нас самих ничего своего нет. Продуктовая модель очень привлекательна — не менее, чем проектная. Но по этому пути пойти может только компания, способная сконцентрировать значительные интеллектуальные и денежные ресурсы, без которых разработка, внедрение и продвижение высокотехнологичного продукта просто невозможны.

Причем такой компании придется преодолеть и недоверие к уровню российских разработок, и серьезное противодействие зарубежных компаний, производящих сходные продукты. Говорю это, опираясь на реальный опыт, который наша компания приобрела при создании и сертификации целого ряда системообразующих технологий и программных продуктов.

СЕРГЕЙ ГОЛОВИН: Участие специалистов вендора в проектах — это обычное явление, и не является ничем новым. Причем некоторые западные компании-производители имеют в своей структуре отдельные консалтинговые подразделения, которые часто выступают в проектах самостоятельно либо в альянсе с партнером — системным интегратором.

Что касается разработки интегратором собственного продуктового портфеля, то чаще всего это "отраслевой" или специализированный "тюнинг" продуктов вендоров, что, кстати, очень часто невозможно без согласования с производителем. Интегратор продает услуги — и создание подобных продуктов чаще всего предназначено для расширения спектра или "глубины" ИТ-услуг, а вовсе не является следствием стремления стать "вендором" или конкурировать с западными производителями на уровне продуктовых линеек.

3. Какая схема взаимодействия вендора и интегратора приводит к наиболее эффективному маркетингу? Насколько современная практика близка к этой идеальной схеме, и какие изменения происходят в этом вопросе?

СЕРГЕЙ ГОЛОВИН: Существующая практика мне кажется вполне работоспособной и я пока не вижу реальной возможности или потребности ее менять. Если несколько огрубить, вендор занимается маркетингом своих продуктов и технологий, его партнер — продвижением и продажей решений на базе этих продуктов на конкретных рынках. Разумеется, степень "локализации маркетинга" у разных вендоров различна. Интересный пример — норвежская компания TANDBERG, крупнейший мировой поставщик видеооборудования, запустила специальную международную программу по выявлению и поддержке наиболее интересных идей и эффективных маркетинговых программ, предложенных компаниями-партнерами для своих рынков. Если такие возможности есть, партнер должен ими пользоваться. Кстати, в упомянутом конкурсе мы участвовали и победили.

СЕРГЕЙ ЩЕРБИНА: Если понимать маркетинг как продвижение продуктов и услуг к целевой аудитории, то системный интегратор, ориентированный на корпоративный сектор, осуществляет маркетинг на каждом этапе работы с заказчиком — от пресейла до технической поддержки. Участие вендора в каждой из этих стадий может принести ему более прочное положение у заказчика. С другой стороны, интеграторы стремятся участвовать в наиболее интересных маркетинговых инициативах и событиях, организуемых вендорами, в том числе направленных на расширение рынка. В идеале, по каждому вертикальному (отраслевому) и горизонтальному (продуктовому) направлению должны формироваться совместные маркетинговые программы и создаваться центры компетенции. Мы учимся у наших поставщиков стратегическому видению рынка и стараемся формировать собственную маркетинговую стратегию, основываясь на имеющихся ресурсах и компетенциях.

ВАЛЕРИЙ АНДРЕЕВ: С маркетингом всегда было непросто, а сейчас, когда решения становятся сложнее и сложнее, то совсем трудно. Эффективным сегодня остается "практический" маркетинг, основанный на реализации местных практик, т.е. местная "история успеха", но построенная на внешнем решении.

Есть другой способ — продвижение конкретных техник, методов, выделение в списке продуктов наиболее интересных и передовых. Это делается порой и в сфере ПО, но на уровне того, что публикуется какой-то новый интерфейс известного продукта и описывается чуть ли не положение кнопок. Маловато, но расчет тут на то, что все равно никто ничего не поймет, а картинку запомнит.

Сегодня серьезная ставка на визуальный ряд в продвижении сложных программных продуктов оправдана лишь если этот продукт совершает прорыв в организации интерфейса "человек-машина". Прорыв, который дает заказчику или пользователю новое качество в общении с системой. Сейчас этому уделяется очень мало внимания, но я уверен, что это просто необходимо. Ведь системы становятся сложными, а их интерфейсы — громоздкими и запутанными. Пока вендоры особенно не напрягаются — рассчитывают на специалистов компании-интегратора, которые разберутся и так. Но это пока. Серьезные изменения все равно неизбежны.

Вообще "продуктовый" маркетинг в сфере "тяжелого" корпоративного ПО и автоматизированных систем находится в латентном состоянии, чего не скажешь, например, о рынке средств вычислительной техники.

Автоматизация управленческого учета на предприятии:
практические советы системного интегратора

Алексей Колесов,
"Энвижн Груп"

ЛЮБОЕ ПРЕДПРИЯИЕ СТАЛКИВАЕТСЯ С ПРОБЛЕМОЙ ВЫБОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ АВТОМАТИЗАЦИИ УПРАВЛЕНЧЕСКОГО УЧЕТА. СЕЙЧАС НЕВОЗМОЖНО НАЙТИ ОТЕЧЕСТВЕННУЮ КОМПАНИЮ, В КОТОРОЙ НЕ ИСПОЛЬЗОВАЛИСЬ БЫ ИНФОРМАЦИОННЫЕ СИСТЕМЫ. ПРИ ЭТОМ ВРЕМЯ ОТ ВРЕМЕНИ ПРЕДПРИЯТИЯ ПРИНИМАЮТ РЕШЕНИЯ ПО ОБНОВЛЕНИЮ ИНФОРМАЦИОННЫХ СИСТЕМ. ЧТО ЗАСТАВЛЯЕТ ИХ ПРИНИМАТЬ ТАКИЕ РЕШЕНИЯ?

Роль и критерий полезности управленческой системы

Зачем компаниям вообще нужна управленческая система, и на основании чего можно судить, насколько хорошо она выполняет свою роль? Прежде всего, система конкретной компании должна быть по-своему уникальна. Дело в том, что компания, которая ее применяет, является единственной в своем роде, поэтому и система должна в точности повторять все ее контуры. Выбор информационной системы можно в чем-то сравнить с выбором человеком одежды или обуви для себя: вряд ли кто-то согласится по собственной воле носить туфли на два размера меньше своего и покупать дорогую одежду без примерки.

Известно, что компания представляет собой объединение активов и сотрудников. Сами по себе активы — это всего лишь объекты собственности, и только сотрудники могут заработать компании своей квалификацией, трудом и талантом столь необходимую ей прибыль. Таким образом, уникальность компании определяется тем, как организовано управление сотрудниками и какая модель поведения специалистов сложилось в компании. Назначение автоматизированной системы управленческого учета — это улучшение и формализация управления и взаимодействия между сотрудниками.

Однако, никакая автоматизированная система управления никак и никогда не сможет заменить собой свод негласных правил, применяемых в компании. В конечном счете, цель любого руководителя — максимально высокая производительность и качество выполняемых подчиненными работ в тех конкретных условиях, в которых сейчас находится компания; при этом использование информационной системы должно способствовать этому росту. Таким образом, полезность информационной системы определяется критерием повышения эффективности работы сотрудников при ее использовании.

Оптимизация системы управления сотрудниками

В современном мире компании подвержены воздействию большего количества внешних и внутренних факторов: изменение технологий, рост и развитие бизнеса, воздействие конкурентов и т.д. Под влиянием этих изменений руководство вносит коррективы в систему управления сотрудниками, сложившуюся в компании. Типичным примером таких изменений является работа компаний после появления Интернета. При этом нередко бывают и случаи, когда менеджмент не успевает вовремя отреагировать на воздействия среды, и это приводит к тому, что внутри компании падает эффективность работы сотрудников.

Любопытную историю рассказали в своей книге К. Нордстрем и Й. Риддерстрале о компании Ford Motors. Так, руководство компании приняло решение сократить на 100 человек отдел дебиторской задолженности и выполнило свое решение, преодолев при этом поднятый недовольными шум. Недовольство мотивировалось тем, что все сотрудники еле справлялись с работой, когда в отделе было 500 сотрудников, а в условиях работы 400 человек справляться с работой будет еще более затруднительно. Некоторое время спустя компания Ford Motors провела сравнительный анализ, взяв ближайшего конкурента — Mazda. И как были удивлены в Ford узнав, что Mazda в аналогичном отделе имеет всего 5 человек. Просто процессы в Mazda были в большей отлажены и автоматизированы.

Нужно отметить, что система управленческого учета оказывает консервирующее воздействие на систему управления сотрудниками. На каждое существенное изменение в системе управления придется включать дополнительные расходы, связанные с внесением симметричных изменений в информационную систему. Эти затраты заключаются в привлечении ресурсов для внесения изменений в систему. Поэтому перед внедрением системы мы бы рекомендовали производить анализ текущей ситуации на предприятии и внести корректирующие изменения до начала использования информационной системы. Это позволит избежать лишних затрат и усилий в будущем. Можно проводить подобный мониторинг положения дел в компании на регулярной основе.

Грамотно проведенный анализ текущей модели бизнес-процессов позволит сформировать четкое представление о том, что и как должно быть автоматизировано. Как покупателю, не знающему, что конкретно он хочет приобрести, легко ошибиться в своем выборе, так и компании без грамотного набора требований к информационной системе легко попасть в положение, когда полученный результат не соответствует ожиданиям. Только в этом случае проект автоматизации будет успешен, а средства, выделенные на него, обязательно окупятся.

Определение требований к системе управленческого учета

При взаимодействии с информационными системами компания проходит несколько стадий, это: определение потребности в информационной системе; выбор решения; реализация проекта; работа с информационной системой и принятие решения о модернизации или прекращении дальнейшего ее использования.

Управленческий учет — это процесс получения, хранения, анализа, интерпретации, подготовки и предоставления финансовой информации менеджменту, должный помочь ему в планировании, оценке и управлении организацией для обеспечения оптимального использования ее ресурсов и полноты учета. Поэтому, как правило, инициаторами внедрения новой информационной системы управленческого учета выступают финансовые службы компании. Однако надо учесть, что информационная система наполняется данными о хозяйственной деятельности предприятия и вносить эти данные будут сотрудники других подразделений. Таким образом, необходимо учесть влияние, которое окажет система на другие подразделения.

Для четкого формирования требований к информационной системе рекомендуется составить компетентную комиссию из сотрудников предприятия. Выбранные сотрудники должны быть профессионалами в своей области и знать положение дел в компании. Желательно, чтобы подобную комиссию возглавлял либо генеральный директор, либо представитель высшего руководства, лично заинтересованный в успешности начинания. Обязательно необходимо учесть и тот факт, что представители разных подразделений будут стараться "тянуть одеяло" на себя, поэтому способность председателя комиссии придерживаться интересов компании будут иметь особую ценность и вес. Целью данной комиссии является необходимость учета пожеланий специалистов с тем, чтобы впоследствии наложить их на интересы компании. Дело в том, что нередко при внедрении системы организация процесса первичного сбора информации и принятия решения игнорируется — или же она ведется одним экспертом; такой подход может стать причиной провала.

Результатом деятельности подобной комиссии являются четко сформулированные требования к информационной системе. Если, например, в результате работы комиссия придет к решению, что требуется исправить сам подход к организации деятельности компании, то работа над формированием требований к информационной системе приостанавливается на время внесения изменений в систему управления сотрудниками.

Комиссией рассматриваются бизнес-требования к системе, поэтому на данном этапе следует привлекать ИТ-специалистов компании. Дело в том, что ИТ-специалисты будут иметь в этой ситуации особый вес и могут начать склонять комиссию в сторону той или иной информационной системы, как бы подбирая требования предприятия к определенной функциональности. При таких подходах обычно создается прецедент, при котором работа по анализу и внесению изменений в системе управления может вылиться в попытку вогнать бизнес-процессы компании в рамки существующей известной информационной системы. Это не решает задачу предприятия и не дает возможности сосредоточиться на решении ключевой задачи, для которой реализуется проект построения автоматизированной системы.

Плюсы и минусы готовой и разрабатываемой системы

ИТ-специалисты привлекаются к работе комиссии на этапе выбора конкретной системы. Задача ИТ-службы будет заключаться в том, чтобы ориентируясь на предложенные бизнес-требования подобрать различные варианты ИТ-решения. При этом нужно обязательно исходить из того факта, что первичными являются именно требования, выдвигаемые к информационной системе, а не возможности того или иного решения. На текущий момент рынок решений информационных систем управленческого учета насыщен большим количеством вариантов, а сами решения сторонних разработчиков за десятилетия прошли долгий путь совершенствования, так что, скорее всего можно сказать с высокой долей вероятности, что найдется решение способное удовлетворить ваши бизнес требования.

Обычно выбор стоит между готовыми решениями или самостоятельной разработкой компании. Написание своими силами информационной системы имеет как и преимущества, так и недостатки. Существенное преимущество самостоятельно разрабатываемых решений заключается в том, что руководство может в любой момент отдать задание на изменение программного кода и это часто очень нравиться владельцам бизнеса. С другой стороны, поспешно принимаемые решения об изменении программного кода вносят неразбериху в работу и редко документируются, создавая при этом дополнительные трудности. К другим недостаткам относятся: высокая стоимость такого проекта для компании; сложность поддержки (с уходом ведущих специалистов компания рискует потерять поддержку и развитие системы); неизбежные ошибки и большое количество сбоев при работе системы.

Готовые решения от сторонних разработчиков в отличие от самостоятельных разработок более надежны: проблемы, связанные с поддержкой и устранением ошибок, берут на себя разработчик ПО и группа специалистов, занимающихся внедрением. В процессе внедрения ряд компонентов может быть доработан, согласно требованиям заказчика в четко указанные сроки, а также реализована интеграция с другими системами компании.

Выбор системы и ее развитие

Если требованиям, выдвигаемым комиссией к будущей системе, удовлетворяет несколько решений, то имеет смысл просто сравнить данные решения между собой. Ориентирами можно выбирать по аналогии с другими крупными проектами, например, насколько полно предлагаемое производителем программное обеспечение соответствует требованиям, какова репутация производителя ПО, суммарная стоимость владения решением и условия технического обслуживания? Среди других вопросов: применение решения другими отечественными и зарубежными предприятиями соответствующей отрасли; наличие офисов, технической поддержки и центров компетенции производителя программного обеспечения на территории России.

После выбора решения компания должна определиться с выбором подрядчика, который будет заниматься его внедрением. Стоит предостеречь компании от идеи содержать специалистов по информационной системе в своем штате, хотя она может сначала показаться довольно привлекательной (не нужно платить за услуги подрядчику), но на проверку может оказаться очень дорогой. Плата за услугу — это фактически плата за выполненную работу, а заработная плата штатного сотрудника — это плата за проведенное время на работе. Как правило, в случае со штатными специалистами начинают проявляться те же проблемы, что и при самостоятельной разработке информационной системы: проблемы с кадрами, с поддержкой и решением периодически возникающих проблем.

Самым простым и правильным подходом будет воспользоваться услугами системного интегратора. Как правило, такие компании уже накопили существенный опыт успешной реализации проектов автоматизации управленческого учета. Стоит отметить один важный факт: при общении с системными интеграторами необходимо делать упор на требования, которые были разработаны комиссией, а не на способность интегратором внедрять те или иные решения. На базе собранных данных и проведенного анализа совместно со специалистами подрядчика необходимо разработать техническое задание.

Нужно отметить, что, к сожалению, разрабатываемые мировыми производителями программного обеспечения, отраслевые решения в области управленческого учета, редко подходят отечественным компаниям в силу специфики бизнеса. Поэтому каждой отечественной компании требуется индивидуальный подход при автоматизации управленческого учета. В свете этого работа по формированию требований к информационной системе, проведенная комиссией на первом этапе, становиться еще более важной. Индивидуальный подход позволит дать четкое представление о том, что должна уметь информационная система — и это будет являться гарантией успеха проекта.

10-я ЮБИЛЕЙНАЯ МЕЖДУНАРОДНАЯ ВЫСТАВКА И КОНФЕРЕНЦИЯ

CSTB - 2008

4-7 ФЕВРАЛЯ МОСКВА КРОКУС ЭКСПО

- ПЛАТНОЕ ТВ: КАБЕЛЬНОЕ И СПУТНИКОВОЕ ТВ, IPTV, HDTV, КОНТЕНТ, МОБИЛЬНОЕ ТВ
- ЦИФРОВОЕ ВЕЩАНИЕ
- ШИРОКОПОЛОСНЫЙ ДОСТУП
- СПУТНИКОВАЯ СВЯЗЬ

ГИПЕРМАРКЕТ НОВЫХ ТЕХНОЛОГИЙ

www.cstb.ru

Организатор: MIDexpo — Международные выставки и ярмарки

Генеральные партнеры: АКТР России; iabm

Со-организатор конференции: ib

Генеральные информационные спонсоры: Теле Спутник; 625

Отраслевой медиа-партнер: Кабельщик

Генеральный Интернет-партнер: COMNEWS

Официальный турагент: MID TRAVEL — www.midtravel.ru

За дополнительной информацией обращайтесь по тел.: (495) 737 74 79

Доступность и безопасность

Выбор абонентских приемников для цифрового платного телевидения

ГЛАВНАЯ ЗАДАЧА СИСТЕМ БЕЗОПАСНОСТИ — ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. В СЛУЧАЕ ПЕРЕХОДА НА ЦИФРОВОЕ ВЕЩАНИЕ ОПЕРАТОРАМ ПРЕДСТОИТ РЕШИТЬ ВАЖНУЮ СТРАТЕГИЧЕСКУЮ ЗАДАЧУ: ВЫБОР СИСТЕМЫ БЕЗОПАСНОСТИ С МИНИМАЛЬНЫМИ ВЛОЖЕНИЯМИ НА НАЧАЛЬНОМ ЭТАПЕ И В ПРОЦЕССЕ РАЗВИТИЯ АБОНЕНТСКОЙ БАЗЫ, ОБЕСПЕЧИВАЮЩЕЙ МАКСИМАЛЬНУЮ ЗАЩИТУ КОНТЕНТА И ДОХОДОВ ОПЕРАТОРА.

Макаровская Л.Ю.,
глава представительства
Conax AS в России

Решение компании Conax AS является классическим решением системы условного доступа к цифровому контенту кабельных, спутниковых и наземных операторов. Под классическим решением мы понимаем работу системы условного доступа в режиме подписки на услуги оператора соответствующую общей архитектуре условного доступа для DVB:

- Мультиплексор создает контрольное слово (CW) и запрашивает, чтобы ECM-генератор системы Conax встроил его в сообщение ECM.
- ECM-генератор системы шифрует сообщение ECM и возвращает его в мультиплексор для включения в транспортный поток DVB.
- На принимающей стороне абонентский приемник (STB) получает сообщения ECM и направляет их к пользовательской смарт-карте Conax.
- Пользовательская смарт-карта Conax сначала дешифрует сообщение ECM, затем сопоставляет текущие время и дату, информацию об услугах и правах доступа в ECM с соответствующей информацией об услугах и правах доступа, временем начала и завершения, датой, хранящимися в памяти пользовательской смарт-карты Conax. Если данные совпадают — пользовательская смарт-карта Conax передает контрольные слова в STB.
- STB использует контрольные слова для дескремблирования исходного сигнала.

Взлом и клонирование пользовательской смарт-карты Conax требует колосальных вложений "хакера" и может занять несколько месяцев. "Пиратская карта" откроет доступ на очень короткий отрезок времени для "хакера" и затем придется все начинать с начала. Взлом пользовательских смарт-карт для операторов, использующих систему условного доступа Conax в настоящее время не актуален.

Наиболее актуальная проблема — это распространение контрольного слова (card sharing/CW distribution), но эта проблема возникает не в системе условного доступа как таковой, а на стороне абонентского приемника (STB), т.е. в процессе передачи контрольного слова от пользовательской смарт-карты в STB.

Дополнительной мерой безопасности, со стороны Conax, является интеграция модуля pairing — кодирование контрольного слова на этапе его передачи в STB. Оператором с помощью данного модуля осуществляется привязка смарт-карт и абонентского приемника.

Conax pairing реализуется в двух вариантах. В первом варианте информация прошивается в чипсете (chipset pairing) до того как чипы будут поставлены производителю STB. Смарт-карты в этом случае конфигурируются в соответствии с чипом STB. Во втором варианте информация прошивается в памяти процессора (memory pairing) во время производства STB.

У оператора модуль pairing может быть активирован на определенные пакеты ТВ-программ, например, содержащие дорогостоящие каналы. Паралельно в сети могут использоваться как STB с функцией pairing, так и без нее.

Возвращаясь к стоимости всего проекта для оператора, цена абонентского приемника играет значительную роль. Conax по-прежнему

Уровень	Специалист	Время взлома каждого приемника	Стоимость оборудования для взлома, долл.	Абонентский приемник
4	Эксперт	5-12 недель	20 000	Приемник с chipset pairing, рекомендованный Conax. Может использоваться у крупных операторов (от 200 000 абонентов) и для дорогостоящего контента или контента в HD (высокого разрешения).
3	Высококвалифицированный хакер	3-6 недель	10 000	Приемник с memory pairing, рекомендованный Conax. Может использоваться у операторов средних размеров (от 50 000 абонентов) и для пакетов программ класса ипремиум.
2	Компетентный хакер	1-3 недели	2000	
1	Мотивированный новичек	1 неделя	500	
0	Новичек	2 дня	0	Дешевый приемник без функции pairing, не прошедший тестирование в Conax. Может использоваться у оператора для базового пакета программ или не дорогого контента.

не берет отчислений с производителей STB за то, что они встраивают систему условного доступа Conax. Но компания фокусирует свой интерес не только на безопасности собственного решения, но и на безопасности абонентского приемника.

В настоящее время около 200 производителей абонентских приставок интегрируются с Conax. Это создает конкурентную борьбу и низкие цены на STB с Conax. Но далеко не все производители действительно рекомендованы Conax.

В таблице приведены общие данные: какой уровень знаний требуется "хакеру" для того чтобы взломать абонентский приемник и получить доступ к контрольному слову, время взлома, примерная стоимость оборудования для взлома и уровень безопасности по оценке Conax.

Поговорка "взломать можно все" отчасти верна, но для того чтобы у "хакеров" исчезла мотивация к взлому абонентской приставки со встроенной системой условного доступа Conax или взлом оказался бы нецелесообразным, Conax предъявляет дополнительные требования к уровню безопасности абонентских приставок для производителей.

Операторы, выбирающие Conax в качестве системы безопасности для цифрового вещания, прежде всего из-за доступности и низкой стоимости STB, для обеспечения максимальной надежности всего проекта, должны запрашивать от производителей абонентских приемников следующие документы:

- Лицензию Conax на STB
- Уровень безопасности STB, полученный в результате оценки в Conax
- Результаты заключительного тестирования с системой Conax CAS.

В свою очередь компания Conax готова предоставить оператору максимальную поддержку на любом этапе перехода на цифровое вещание, и в том числе предоставить информацию по сопутствующему оборудованию для реализации всего проекта.

Телекоммуникационные компании боятся инсайдеров

СТАТЬЯ ПОСВЯЩЕНА ПРОБЛЕМАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КОТОРЫЕ ИСПЫТЫВАЮТ РОССИЙСКИЕ ОПЕРАТОРЫ СВЯЗИ. В КАЧЕСТВЕ БАЗЫ ДЛЯ ОСНОВНЫХ ВЫВОДОВ ИСПОЛЬЗУЕТСЯ ИССЛЕДОВАНИЕ ОТЕЧЕСТВЕННОЙ КОМПАНИИ INFOWATCH "ВНУТРЕННИЕ ИТ-УГРОЗЫ В СЕКТОРЕ ТЕЛЕКОММУНИКАЦИЙ 2006". В РАМКАХ ИССЛЕДОВАНИЯ ЭКСПЕРТЫ INFOWATCH ОПРОСИЛИ СОТРУДНИКОВ ИТ- И ИБ-ДЕПАРТАМЕНТОВ 300 РОССИЙСКИХ ТЕЛЕКОМ-КОМПАНИЙ.

Данил Анисимов,
Независимый эксперт
по ИТ-безопасности

Не секрет, что тема информационной безопасности (ИБ) достаточно широко освещается в современных СМИ. Для этого сравнительно нового рынка характерно большое количество решений, разбивающихся на огромное количество классов. В ежегодном отчете американского института компьютерной безопасности (Computer Security Institute, CSI) "2007 CSI Computer Crime and Security Survey", рынок ИБ поделен на 19 (!) продуктовых сегментов, для каждого из которых существуют собственные технические решения. Как следствие, компаниям (в лице руководителей ИТ-департаментов или начальников служб информационной безопасности) крайне тяжело разобраться в таком многообразии и выявить те системы, внедрять которые критически необходимо.

В этом смысле, телекоммуникационным компаниям приходится вдвойне труднее. Их бизнес по определению завязан на информации, а значит — эту информацию необходимо качественно защищать. Подчеркнем, что операторам связи приходится думать не только о безопасности собственных корпоративных данных, но и о сохранности данных клиентов, идущих по принадлежащим оператору каналам. Другими словами, решать похожую задачу два раза подряд. Поэтому ошибка в выборе тех или иных средств обеспечения безопасности может привести оператора к двойным материальным потерям.

Внешние и внутренние угрозы информационной безопасности

Первый значимый вопрос исследования

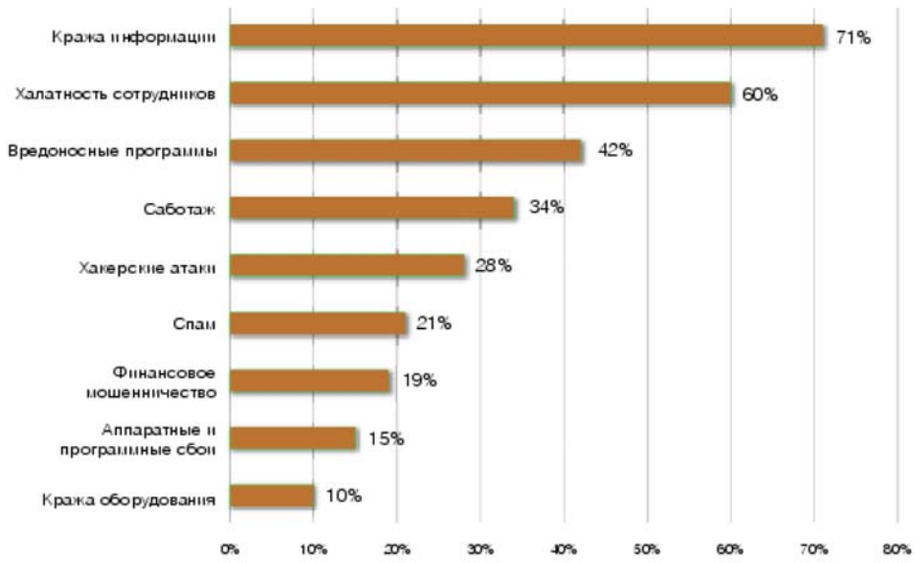


Рис. 1. Наиболее опасные угрозы ИБ

InfoWatch касался наиболее опасных угроз в области ИБ. Приводимая ниже раскладка является упрощенной в том смысле, что одна и та же угроза (например, кража информации) может материализоваться в силу различных причин. Однако, исходя из полученных данных, можно сделать несколько интересных выводов.

Все угрозы, приведенные на рис. 1. можно разбить на три основные группы. Во-первых, существуют "чисто внешние" угрозы (вредоносные программы, хакерские атаки, спам), которые объясняются действиями внешних мошенников. Во вторую группу попадают "чисто внутренние" угрозы (прежде всего, халатность сотрудников и финансовое мошенничество), возникающие из-за случайных или злонамеренных действий сотрудников компании (инсайдеров). Наконец, смешанные угрозы (кража информации, сбои, кража оборудования), объясняются в каждом конкретном случае по-разному.

Легко видеть, что телеком-компании обеспокоены, прежде всего, внутренними угрозами. Угроза "кражи информации", расположенная на первом месте списка (71% голосов), обычно возникает именно из-за действий инсайдеров. Первая значимая внешняя угроза (вредоносные программы) беспокоит менее половины опрошенных респондентов.

Сравнивая полученные результаты с межотраслевым распределением (см. исследование InfoWatch "Внутренние ИТ-угрозы в России 2006"), можно увидеть еще одну интересную тенденцию. Телекоммуникационные компании опасаются практически всех типов угроз чуть больше, чем все компании по рынку в целом. Например, индекс популярности угрозы "кража информации" в секторе телекоммуникаций на 5% опережает аналогичный показатель по всем отраслям (71% против 66%). Скорее всего, такое положение вещей объясняется более высоким профессионализмом операторов связи, которые гораздо глубже связаны с ИТ, чем другие организации.

Если исключить из рассмотрения смешанные угрозы и суммировать голоса, полученные "чисто внешними" и "чисто внутренними" вариантами ответа, то опасность внутренних угроз относится к опасности внешних примерно как 55:45. На самом деле, реальное соотношение даже больше, поскольку смешанные угрозы (кража информации, различные сбои и кража оборудования) чаще квалифицируются как внутренние.

Таким образом, российские операторы связи обеспокоены, прежде всего, действиями собственных сотрудников, а не внешних мошенников. Эта тенденция вполне логична и имеет сразу несколько основных предпосылок. Решения, предназначенные для защиты компании от внешних угроз, появились на рынке значительно раньше, они гораздо дольше эволюционировали и поэтому находятся на более высоком уровне зрелости. К тому же, сама проблематика внутренних угроз концептуально сложнее, нежели проблематика внешних. Если сравнить корпоративную сеть с просторным помещением, то "внешняя" безопасность аналогична установке мощного замка на дверь. А безопасность внутренняя — контролю легальных посетителей помещения, обладающих ключами к этому замку. Понятно, что вторая задача значительно сложнее и многограннее первой.

Следующий вопрос исследования InfoWatch касался опасности различных внутренних угроз. На первых двух местам в полученном распределении (рис. 3) находятся угрозы "утечки информации" (85%) и ее "искажения"(64%). А на третьем месте располагается мошенничество (49%) — и это достаточно необычно. Дело в том, что в целом по рынку эту угрозу отметили только 19% респондентов. По всей видимости, в высокой опасности мошенничества проявляется еще одна специфика телеком-компаний, которая объясняется широким применением информационных биллинговых систем.

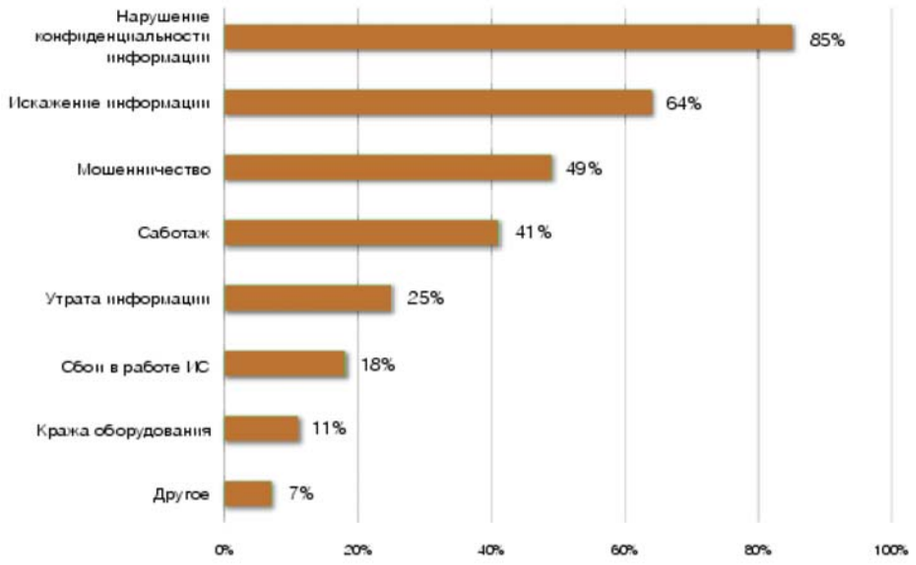


Рис. 3. Наиболее опасные угрозы внутренней ИБ

Утечки данных: последствия, каналы и количество

Обобщая ответы на предыдущие вопросы, приходим к выводу о том, что угроза "утечки конфиденциальной информации" является наиболее опасным риском ИБ в целом (не только внутренней, но и внешней ИБ). В связи с этим возникает логичный вопрос — а чем же опасна эта угроза, и почему телекоммуникационные компании так сильно ее боятся? На рис. 4 приведены ответы респондентов на этот вопрос.

Как выяснилось, наиболее плачевным последствием утечки является удар по репутации компании (51% голосов). В России пока не существует законов, которые обязывают оповещать об утечке различные органы, однако если эта информация попадает в прессу, то репутация "отличившейся" компании мгновенно падает. Чтобы привести какую-то конкретику вспомним инцидент с компанией "Вэб Хостинг", предоставлявшей услуги хостинга под торговой марке Valuehost. Напомним, что в октябре прошлого года ряд интернет-магазинов выложили на свои прилавки "Базу данных Valuehost.ru со всеми логинами и паролями". Всего за 300 долларов любой желающий мог купить базу реквизитов 70 тыс. пользователей хостинг-оператора. Данный инцидент широко освящался в российский прессе и привел "Вэб Хостинг" к серьезным финансовым потерям.

Отметим, что для телекоммуникационных компаний репутация является весьма важным активом. Особенно если не рассматривать крупные общероссийские корпорации, контролирующие уникальные каналы связи. Абсолютное большинство операторов не могут похвастаться уникальным положением и, более того, им приходится играть на рынке с высоким уровнем конкуренции. В таких условиях репутация является одним из основных факторов успеха.

Второе "плачевное" последствие утечки неразрывно связано с первым. Понятно, что очевидным результатом ухудшившейся репутации является потеря потенциальных (а также вполне реальных) клиентов. Это последствие отметили 43% респондентов.

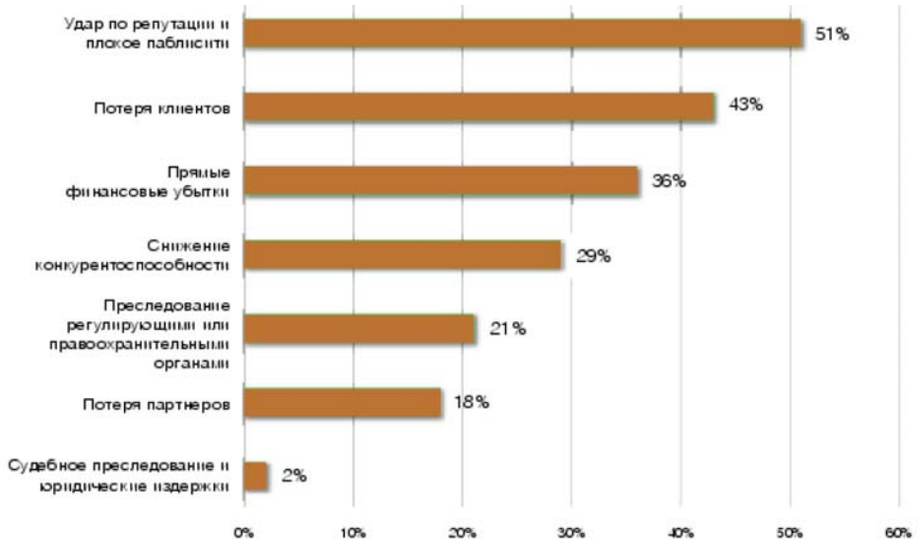


Рис. 4. Наиболее затратные последствия утечки данных

На следующих позициях списка находятся "прямые финансовые убытки" (36%) и "снижение конкурентоспособности" (29%). Эти последствия имеют другую природу: они предполагают утечку интеллектуальной собственности, а не приватных данных клиентов (сотрудников) компании. Но, так или иначе, независимо от типа исчезнувших данных, последствия для компании будут весьма серьезными.

Добавим, что "юридические" последствия (преследование различными органами, а также судебные издержки) находятся в самом конце списка. Оно и понятно — государственное регулирование информационной безопасности в России находится пока на зачаточном уровне. Некоторые законы, правда, уже приняты, однако пока они носят рекомендательный характер или же просто не применяются на практике. Ниже мы расскажем о законодательном регулировании ИБ в телеком-компаниях более подробно.

Завершая разговор о последствиях утечек, приведем несколько цифр исследования американского института Ponemon Institute — . Аналитики Ponemon Institute попробовали посчитать, сколько же стоит утечка приватной записи всего одного клиента компании. Оказалось, что прямые издержки на ликвидацию утечки в среднем составляют примерно , а косвенные потери (удар по репутации и как следствие — потеря клиентов) — . Конечно, в России эти показатели заметно ниже, однако по ним можно понять порядок расходов на ликвидацию того или иного инцидента. Так, утечка всего 10 тыс. приватных записей в России (а это довольно частый случай) сопряжена с серьезными долларовыми потерями, которые измеряются шестизначной цифрой. Один такой инцидент способен перебить все расходы, идущие на внедрение системы защиты.

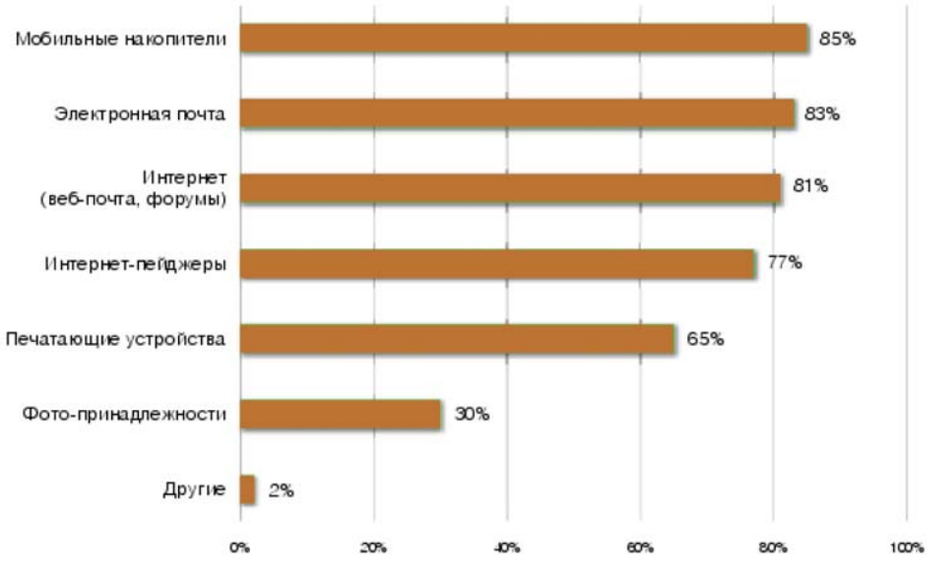


Рис. 5. Опасность различных каналов утечки данных

Утечка конфиденциальных данных всегда происходит по некоторым каналам. Из списка наиболее опасных каналов утечки (рис. 5) следует один главный вывод. Легко увидеть, что практически все имеющиеся каналы действительно опасны (кроме, быть может, фото-принадлежностей), а значит — каждый из них требуется как-то контролировать. В этом смысле очевидное преимущество имеют комплексные системы, обеспечивающие защиту всех имеющихся каналов утечки, а не только какого-то подмножества из них.

Все разговоры о возможной опасности утечек были бы беспочвенны, если бы эти самые утечки не происходили. Согласно данным InfoWatch (рис. 6) более половины телеком-компаний (47%) испытали за последний год хотя бы одну утечку данных, а еще 38% затруднились ответить на данный вопрос. Скорее всего, большинство организаций, входящих в эту долю, все же испытали утечки, однако просто от них не знают.

Добавим, что только 15% респондентов уверенно заявили, что их компании не допустили за прошедший год ни одной утечки данных. Несмотря на то, что этот показатель незначительно (на 1,3%) выше общеотраслевого, он все равно критически низок.

ИБ в телекоммуникационных компаниях и законодательство

Специфика телекоммуникационных компаний также проявляется в вопросах нормативного регулирования. На сегодняшний день существует два основных закона, оказывающих влияние на их деятельность.

Во-первых, операторы связи часто ориентированы на предоставление услуг физическим лицам, а потому аккумулируют в своей корпоративной сети огромные объемы персональных данных граждан. Следовательно, руководству департаментов ИТ и ИБ необходимо обратить внимание на ФЗ "О персональных данных", который предъявляет целый ряд требований к безопасности приватных сведений граждан.

Вторым нормативным актом, который неизбежно повлияет на жизнь операторов, станет стандарт "Базовый уровень информационной безопасности операторов связи". Ряд положений этого документа напрямую адресует внутренние угрозы ИБ и проблему защиты персональных данных. Например, раздел 3.16 рекомендует оператору "обеспечивать конфиденциальность передаваемой и/или хранимой информации систем управления и автоматизированных систем расчета за услуги связи (биллинга), сведений об абонентах (персональных дан-

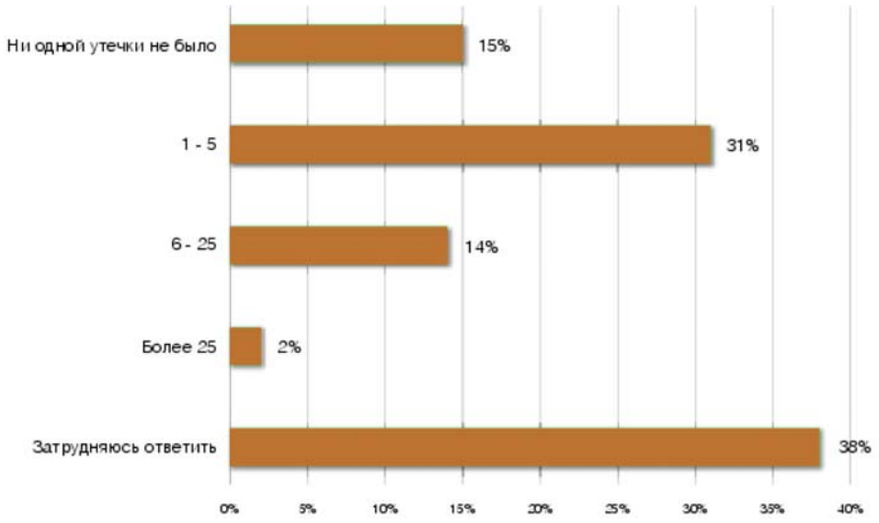


Рис. 6. Количество утечек данных

ных физических лиц) и оказываемых им услугах связи, ставших известными операторам связи в силу исполнения договоров об оказании услуг связи". Согласно разделам 3.17 и 3.18, компания должна вести журналы регистрации событий ИБ и хранить их, исходя из сроков исковой давности (в России общий срок — 3 года). Более того, "для фильтрации потока первичных событий рекомендуется применять технические средства корреляции событий, оптимизирующие записи в журналах инцидентов по информационной безопасности". Также нельзя обойти вниманием пункт 4.4: "Оператору, допустившему утрату баз данных абонентов (клиентов) других (взаимодействующих)операторов, рекомендуется информировать последних об этом в кратчайшие сроки". Таким образом, российский сектор телекоммуникаций становится все ближе к передовому опыту — ведь в США и Евросоюзе компании уже давно несут ответственность за утечку приватных данных. Более того, они не могут скрыть этот инцидент, так как по закону обязаны поставить пострадавших в известность об утечке. Судя по всему, со временем в России тоже появится такая норма.

На рис. 7 представлена ожидаемая степень влияния на отрасль двух описанных нормативов. Легко увидеть, что влияние "базового уровня", скорее всего, окажется заметно весомее. Сегодня в телекоммуникационной отрасли бытует мнение о том, что ФЗ "О персональных-данных" является практически беззубым нормативом.

Такая ситуация объясняется сразу рядом причин. Во-первых, данный нормативный акт выдвигает самые общие требования: операторы обязаны обеспечить конфиденциальность приватных сведений, но сделать это они должны по собственному разумению. Во-вторых, закон не предусматривает явной ответственности за утечку информации для руководства или бизнеса. В-третьих, федеральный орган, уполномоченный следить за выполнением закона (ФСТЭК России), до сих пор не выпустил стандарт безопасности персональных данных. Между тем, этот стандарт необходим, чтобы компании знали, какие меры по обеспечению конфиденциальности закон и регулирующие органы считают достаточными. Наконец, в-четвертых, в России отсутствует правоприменительная практика в сфере борьбы с утечками: судьям, следователям и милиции необходим опыт борьбы с инсайдерами и продавцами приватных данных.

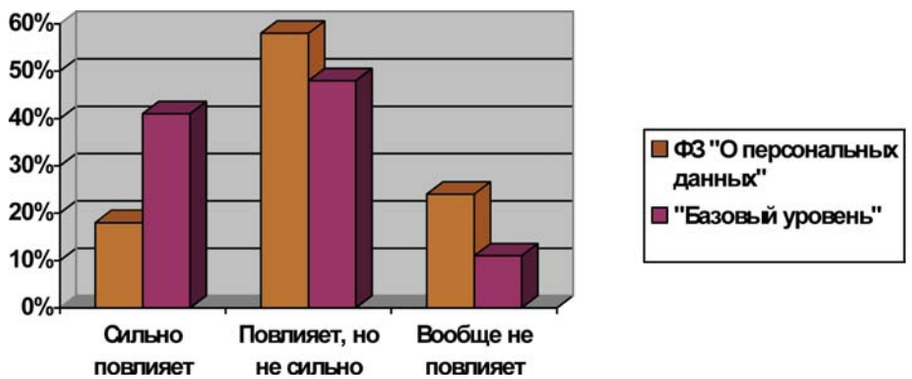


Рис. 7. Влияние различных законов на бизнес телекоммуникационных компаний

В отличие от Федерального закона "Базовый уровень" является всего лишь рекомендацией, а значит — соответствие этой рекомендации не является обязательным. Однако в некоторых случаях оно может оказаться критически важным. В частности, регуляторы могут сделать "Базовый уровень" важным условием для получения каких-либо лицензий. А крупные и серьезные операторы могут выдвигать похожие условия для более мелких игроков, желающих присоединиться к их сети. К тому же, соответствие стандарту является серьезным маркетинговым преимуществом, которое можно использовать для получения более высоких доходов. Если оператор соответствуют "Базовому уровню" он может продавать собственные услуги по более высокой стоимости — беря дополнительные деньги за гарантию безопасности клиентов.

Средства защиты

Заключительная часть исследования InfoWatch была посвящена инструментам обеспечения безопасности в российских телекомкомпаниях. На рис. 8 представлены технические средства, которые применяются операторами связи для защиты собственной инфраструктуры. Абсолютное большинство используемых инструментов (антивирусное ПО, межсетевые экраны, антиспам) по-прежнему связаны с внешними угрозами, а системы защиты от утечек данных внедрили только 8% респондентов. Казалось бы, этот показатель критически низок, если не учесть одно обстоятельство — еще в конце 2005 года доля таких компаний не превышала 2%. Таким образом, спрос на системы защиты от утечек вырос за год на космическую цифру в 400%. Можно смело утверждать, что в нынешнем году эта тенденция продолжилась, и доля защищенных компаний существенно выросла.

Однако, несмотря на очевидный рост интереса к теме внутренних угроз, имеется ряд препятствий, которые тормозят внедрение систем защиты (рис.9). Главным из них является отсутствие стандартов (30%) — далеко не все операторы понимают, как можно обезопасить себя от утечек. Похожее препятствие — нехватка квалифицированного персонала (15%) — оказалось на четвертом месте списка. 22% респондентов считают основным препятствием бюджетным ограничения, что также вполне объяснимо. Многие компании потратили существенные средства на безопасность в течение последних лет, и теперь им крайне трудно убедить руководство в важности дальнейших инвестиций.

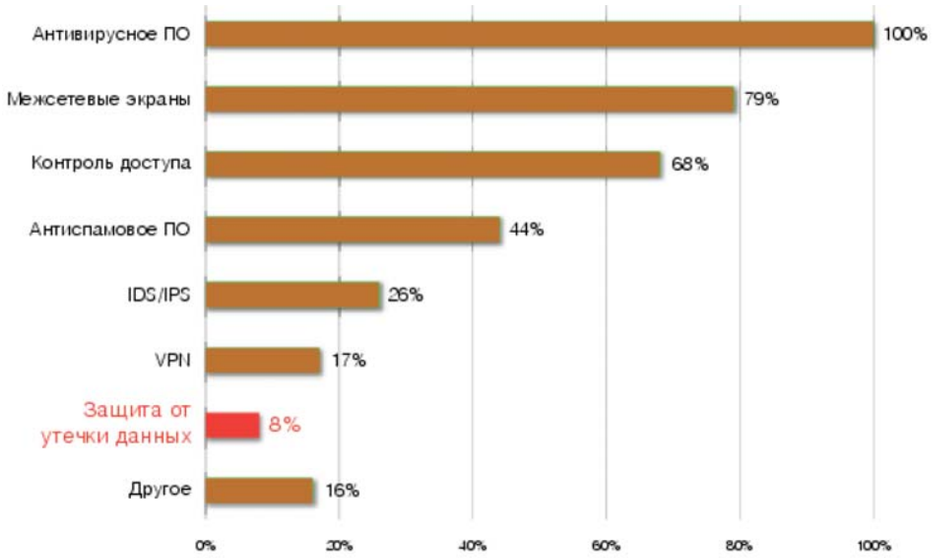


Рис. 8. Используемые средства информационной безопасности

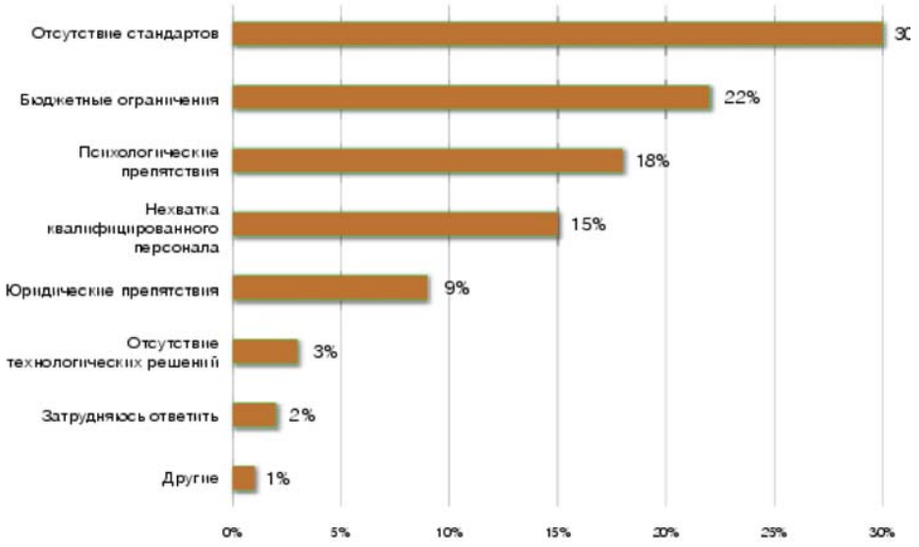


Рис. 9. Препятствия внедрения системы защиты от утечки данных

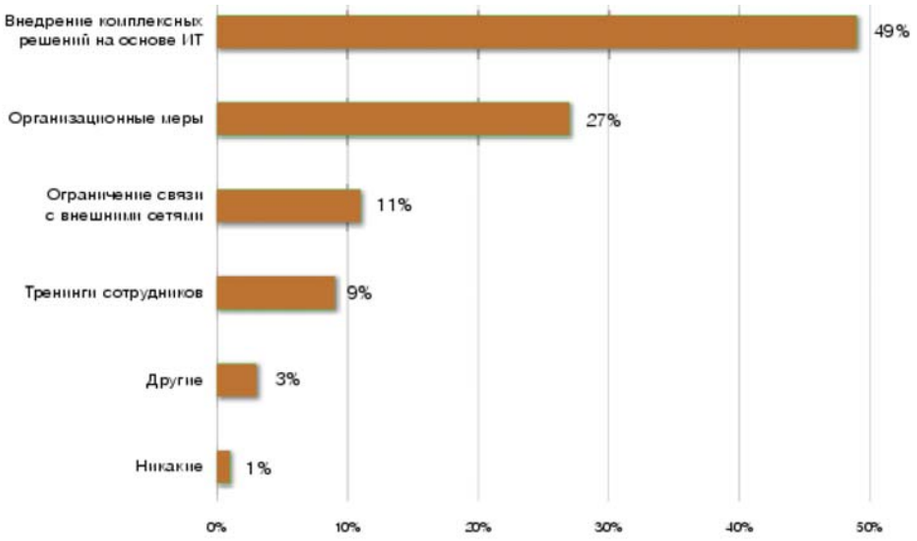


Рис. 10. Наиболее эффективные пути защиты от утечки данных

Полученные результаты интересно сравнить с общеотраслевыми. В опросе среди всех секторов экономики на первых позициях списка располагались психологические ограничения (25%), в то время как отсутствие стандартов находилось только на пятой строчке рейтинга (12%). Отсюда напрашивается вывод, что сектор телекоммуникаций подходит к проблеме внутренней ИБ более зрело, чем другие отрасли. Операторы связи уже перешагнули психологический барьер и активно присматриваются к внедрению систем защиты. Отметим, что такие системы уже доступны на рынке, поскольку отсутствие технологических решений отметили только 3% респондентов. Другое дело, что из-за отсутствия стандартов компании не понимают, каким образом надо эти системы внедрять.

На следующем этапе исследования респонденты попытались оценить эффективность различных подходов к защиты ИТ-инфраструктуры компаний от утечек данных (рис.10). Наиболее эффективным способом оказалось внедрение комплексных информационных систем — этот вариант отметили 49% респондентов. Следом располагаются организационные меры (27%), а также ограничение связи с внешними сетями (11%).

Таким образом, проблема утечек данных не решается только запретительными мерами. Если компания хочет обезопасить себя от утечек, не снизив при этом эффективность собственного бизнеса, ей придется внедрять комплексные системы. Банальное ограничение использования Интернета, электронной почты или ICQ сегодня уже, к сожалению, не работает.

Заключение

Несмотря на то, что российские телекоммуникационные компании довольно зрело относятся к ИБ в целом и внутренним угрозам в частности, им все равно еще есть, куда работать. Во-первых, уровень использования систем защиты от утечек в российских компаниях до сих пор крайне низок. И, во-вторых, существует ряд препятствий для массированного внедрения подобных систем.

С другой стороны, имеется и несколько противоположных предпосылок — как объективных (общие тенденции развития рынка ИБ), так и субъективных (нормативное регулирование). Но если сдерживающие факторы являются, скорее, временным явлением, то предпосылки, напротив, будут наблюдаться постоянно. Поэтому рискнем предположить, что телеком-компании будут активно внедрят системы внутренней защиты в собственную ИТ-инфраструктуру. И более того, это направление станет главным вектором развития ИБ на вертикальном рынке операторов связи.

Киберпреступность становится все более профессиональной

ОТЧЕТ ОБ УГРОЗАХ ИНТЕРНЕТ-БЕЗОПАСНОСТИ ПОКАЗАЛ, ЧТО ХАКЕРЫ, ЧТОБЫ УСПЕШНО ОСУЩЕСТВЛЯТЬ ВРЕДОНОСНУЮ ДЕЯТЕЛЬНОСТЬ, БЕРУТ НА ВООРУЖЕНИЕ НОВЫЕ СТРАТЕГИИ, АНАЛОГИЧНЫЕ СТРАТЕГИЯМ КОММЕРЧЕСКИХ ПРЕДПРИЯТИЙ

Киберпреступники все чаще становятся профессионалами и даже предпринимателями, разрабатывая, распространяя и используя вредоносные коды и сервисы. Киберпреступность продолжает преследовать цель финансового обогащения, однако теперь злоумышленники используют все более профессиональные методы атак, инструменты и стратегии.

В период с 1 января по 30 июня 2007 г. Symantec наблюдала усиление интенсивности использования киберпреступниками наборов мощных инструментов для организации вредоносных атак. Примером этой стратегии служит MPack, профессионально разработанный набор инструментов, который продается на черном рынке. Купив его, злоумышленник может использовать программные компоненты MPack для установки вредоносных программ на тысячи компьютеров во всем мире, а затем следить за успехом операции по разным характеристикам, отображаемым на защищенной паролем онлайновой консоли контроля и управления. MPack служит также примером средства для организации скоординированных атак, при которых злоумышленники применяют разные виды вредоносной деятельности.

В мире профессиональной и коммерческой киберпреступности доступны также инструменты фишинга, которые представляют собой серии готовых сценариев, позволяющих злоумышленникам автоматически создавать фишинговые web-сайты, имитирующие легитимные. Три наиболее широко используемых набора инструментов фишинга ответственны за 42% всех фишинговых атак, зарегистрированных за отчетный период.

Киберпреступники все чаще эксплуатируют пользующиеся доверием сайты

Злоумышленники не прямо преследуют свои жертвы, а сначала эксплуатируют уязвимости в программном обеспечении пользующихся доверием серверов, таких как web-сайты популярных финансовых учреждений, социумных сетей и служб трудоустройства. Symantec обнаружила, что 61% всех уязвимостей относятся к web-приложениям. Взломав пользующийся доверием web-сайт, преступники могут использовать его в качестве источника распространения вредоносных программ с целью последующего взлома отдельных компьютеров. Этот метод атак позволяет киберпреступникам, вместо того чтобы активно разыскивать жертв, дожидаться, пока они придут сами. Web-сайты социумных сетей особенно привлекательны для злоумышленников, так как они предоставляют доступ к большому числу людей, многие из которых доверяют серверу и считают его безопасным. К тому же эти web-сайты могут содержать много конфиденциальной информации, которую впоследствии можно использовать для попыток совершения "кражи личности", онлайнового мошенничества или для получения доступа к другим web-сайтам, через которые можно организовать новые атаки.

Рост популярности многоступенчатых атак

За первые шесть месяцев 2007 г. заметен рост интенсивности многоступенчатых атак, состоящих из первоначальной атаки, не рассчитанной на прямую вредоносную деятельность, с последующим использованием ее плодов для организации дальнейших атак. Одним из примеров многоступенчатой атаки служит многоразовый загрузчик, который позволяет злоумышленнику заменять загружаемый компонент угрозами любого типа, отвечающими его целям. Согласно ISTR, Symantec обнаружила, что 28% из топ-50 образцов вредоносного кода представляли собой многоразовые загрузчики. Примером угрозы этого типа служит троян Peacomm, широко известный как Storm Worm. Он же стал тем новым семейством вредоносных программ, о котором Symantec получила больше всего сообщений в течение отчетного периода. MPack, кроме того, что это набор инструментов для организации атак, тоже служит примером многоступенчатой атаки, включающей компонент многоразового загрузчика.

Отчет об угрозах интернет-безопасности

Том XII отчета об угрозах интернет-безопасности Symantec выпускается два раза в год и охватывает период с 1 января по 30 июня 2007 г. Он основан на данных Symantec, собранных от более чем 40 тыс. датчиков, развернутых в 180 странах. Их дополняет база данных, содержащая свыше 22 тыс. записей об уязвимостях, которые влияют более чем на 50 тыс. технологий от восьми с лишним тысяч поставщиков. Symantec обследует также свыше 2 млн учетных записей-приманок, которые собирают сообщения e-mail в 20 странах и позволяют измерять глобальную деятельность, связанную со спамом и фишингом.

- За этот период товаром, наиболее часто рекламируемым на серверах черного рынка, были кредитные карты, на долю которых пришлись 22% всех рекламных объявлений; близко к ним подошли банковские реквизиты с 21% объявлений.
- Symantec зафиксировала 237 уязвимостей в плагинах веб-браузеров. Это значительно больше, чем 74 уязвимости, зафиксированные во втором полугодии 2006 г., и 34 в первом полугодии 2006 г.
- На долю вредоносного кода, пытающегося украсть информацию об учетных записях в онлайновых играх, пришлось 5% из топ-50 образцов вредоносного кода по потенциалу заражения. Онлайновые игры становятся одним из наиболее популярных видов деятельности в интернете, и в них часто фигурируют товары, которые можно продать за реальные деньги, а это сулит хакерам потенциальные барыши.
- Спам составил 61% от всего контролируемого трафика e-mail; это несколько меньше, чем за последние шесть месяцев 2006 г., когда в качестве спама классифицировались 59% электронной почты.
- Кражи и утери компьютера или другого носителя данных стали причиной 46% от всех случаев утечки данных, способных привести к "краже личности". В подтверждение этого Отчет об управлении ИТ-рисками Symantec показал, что 58% предприятий ожидают как минимум одного серьезного случая утечки данных в течение пяти лет.

По материалам компании Symantec

Наблюдение за внутренними угрозами

МНОГИХ ИТ СОТРУДНИКОВ В УЧРЕЖДЕНИЯХ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ НЕ БЕЗ ОСНОВАНИЙ БРОСАЕТ В ДРОЖЬ, КОГДА РЕЧЬ ЗАХОДИТ О ЗАЩИТЕ ОТ ВНУТРЕННИХ УГРОЗ. КРОМЕ МИЛЛИОНОВ ЛЮДЕЙ, РАБОТАЮЩИХ В ГОСУЧРЕЖДЕНИЯХ, МНОЖИТСЯ ЧИСЛО ФЕДЕРАЛЬНЫХ СЛУЖАЩИХ И ТЕХ, КТО РАБОТАЕТ НА ПРЕДПРИЯТИЯХ-ПОДРЯДЧИКАХ НАД ФИНАНСИРУЕМЫМИ ГОСУДАРСТВОМ ПРОЕКТАМИ ИЛИ В ОРГАНИЗАЦИЯХ, ПОЛУЧАЮЩИХ ГОСУДАРСТВЕННЫЕ ГРАНТЫ. ДОБАВЬТЕ К НИМ РАБОТНИКОВ ПОЧТЫ И ВОЕННЫХ, И "РЕАЛЬНЫЙ РАЗМЕР" ФЕДЕРАЛЬНОГО ПРАВИТЕЛЬСТВА ПРИБЛИЗИТСЯ К 14,6 МЛН РАБОТНИКОВ — ТАКОВЫ ДАННЫЕ ПРОФЕССОРА ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ НЬЮ-ЙОРКСКОГО УНИВЕРСИТЕТА ПОЛА К. ЛАЙТА.

Алексей Чередниченко,
Технический эксперт Symantec
в России и СНГ

ИТ-угрозы со стороны сотрудников или подрядчиков — это реальная проблема, причем одна из наиболее сложных проблем, с которыми сталкиваются менеджеры — ввиду доверия, которым пользуются собственные сотрудники. По разным оценкам, до 80% угроз для безопасности исходят от собственных сотрудников организации. Один человек может причинить данным, системам, работе и репутации учреждения непоправимый ущерб. Зависимость государственных учреждений от взаимозависимых систем связи значительно повышает риск причинения ущерба, причиной которого может стать внутренняя подрывная деятельность. Поэтому важно, чтобы госучреждения имели возможность выявлять своих злоумышленников по их поведению и использовать средства безопасности, предназначенные для обнаружения и отражения таких угроз.

Поведенческий анализ

Возможность распознавать определенное поведение или характерные признаки подготовки сотрудников к ИТ-атаке может способствовать предупреждению потенциальной проблемы. Исследование, проведенное Секретной службой США в 2006 году, показало, что внутренние взломы компьютеров и сетей редко бывают импульсивными действиями. В большинстве случаев они планируются заранее, и подготовленные сотрудники и внимательные менеджеры часто могут заблаговременно заметить признаки готовящейся атаки.

Вот некоторые другие результаты исследования Секретной службы:

- 80% сотрудников, организовавших атаки против своих компаний, проявляли недоброжелательность перед инцидентом.
- В 92% случаев инциденту предшествовало негативное для виновника событие, связанное со службой, такое как понижение в должности, перевод, предупреждение или уведомление об увольнении.
- На момент инцидента 59% были бывшими сотрудниками или подрядчиками, тогда как 41% еще оставались в штате компании.
- Среди бывших сотрудников 48% были уволены, 38% вышли в отставку и 7% были уволены временно.
- 86% работали на технических должностях. Из них 38% были системными администраторами.
- 21% были программистами, 14% — инженерами и 14% — специалистами по ИТ.
- В 96% случаев злоумышленниками были мужчины.
- Чуть менее трети инсайдеров имели судимость.
- 57% выражали признаки раздражения.
- Большинство злоумышленников взламывали учетные записи, создавали несанкционированные тайные учетные записи или использовали для своих атак коллективные учетные записи.
- Для организации большинства атак использовался удаленный доступ.
- Наиболее часто называемым мотивом была месть.

В июне 2007 г. Управление национальной контрразведки США распространило собственные рекомендации, призванные помочь сотрудникам госучреждений в выявлении и последующем донесении о поведении, указывающем на потенциальную внутреннюю угрозу.

Меры безопасности

При всей важности ИТ-защиты по периметру сети от внешних угроз не менее важное значение имеет знание и контроль за тем, кто чем занимается внутри этого периметра. Для этого требуется контроль за доступом к сети, а также

решения для обеспечения безопасности конечных точек сети и базы данных.

• Symantec Network Access Control гарантирует, что каждое конечное рабочее место, подключенное к сети, отвечает правилам безопасности и политике доступа учреждения.

• Symantec Endpoint Protection заблаговременно анализирует поведение приложений и сетевые коммуникации, выявляя и блокируя атаки. Если рассерженный сотрудник попытается применить на своем компьютере такие эксплойты, как руткиты или шпионские программы, это будет обнаружено заранее. Защита блокирует также команды чтения/записи/исполнения, поступающие со сменных дисков, и предотвращает исполнение неавторизованных приложений в защищенных системах.

• Symantec Database Security обнаруживает вредоносную деятельность с базами данных со стороны легитивных пользователей и создает контрольный след всех действий при работе с данными. Интеллектуальная технология профилирования этого решения автоматически изучает "нормальный" характер работы с базой данных и предупреждает администраторов о подозрительных действиях.

Заключение

Внутренние угрозы становятся все более распространенными, и их особенно трудно обнаружить и предотвратить. Государственные ИТ-системы содержат информацию, критически важную для национальной безопасности, и риск внутреннего взлома слишком велик. Однако знание признаков, за которыми надо следить, и сочетание этого знания с внутренними мерами ИТ-безопасности — лучший способ гарантировать защиту государственных сетей и национальную безопасность.

Новое решение для защиты конечных пользователей сети

Корпорация Symantec объявила о выпуске во всем мире продуктов Symantec Endpoint Protection 11.0 и Symantec Network Access Control 11.0. Symantec Endpoint Protection объединяет Symantec AntiVirus с передовой технологией предотвращения угроз в едином агенте, управляемом с единой консоли, что гарантирует беспрецедентную защиту серверов, настольных ПК и ноутбуков от вредоносного программного обеспечения и потери данных.

В программе открытого бета-тестирования Symantec Endpoint Protection приняли участие свыше 10 тыс. индивидуальных пользователей, которые прислали множество отзывов, способствовавших подготовке окончательного продукта, а также предлагаемых сегодня услуг и поддержки. Одним из заказчиков, принявших участие в организованной Symantec программе бета-тестирования, стала компания Johnson Controls, предложившая свои комментарии: Johnson Controls — мировой лидер в области систем для салонов автомобилей, автомобильного электрооборудования и оборудования для создания комфорта в жилых помещениях. Компания занимает 67 место в списке крупнейших компаний Америки за 2007 г., который ведет журнал Fortune. 140 тыс. ее сотрудников работают в 75 регионах мира, обслуживая заказчиков в 125 странах. Примерно половина из них работает с информацией, вооружившись настольными ПК и ноутбуками, и регулярно обращается к корпоративной сети, поэтому защита конечных точек сети имеет для компании критическое значение. В компании внедрили бета-версию Symantec Endpoint Protection 11.0 для ограниченной целевой группы. В этот продукт эффективно интегрированы все инструменты безопасности. Бета-версия оказалась простой в установке, а единая консоль значительно упрощает управление. Не жертвуя никакой функциональностью, компания добилась повышения эффективности работы при значительно меньших занимаемых ресурсах.

Symantec Endpoint Protection обеспечивает преимущества важнейших технологий (антивирус, антишпионское ПО, клиентский межсетевой экран, предотвращение вторжений, управление устройствами и управление приложениями) в виде единого интегрированного агента и администрируется посредством единой консоли управления. Symantec Endpoint Protection включает новую, упрощенную консоль управления, встроенный и готовый к работе компонент **Network Access Control** (NAC) и целый ряд предложений по обучению и поддержке партнеров и заказчиков для ускорения процесса внедрения.

Symantec Endpoint Protection и Symantec Network Access Control обслуживают широкий спектр заказчиков — от малых предприятий без ИТ-подразделений до глобальных организаций с тысячами конечных точек сети, которыми надо управлять. Так как каждая система уникальна, Symantec разработала ряд новых инструментов и услуг аутсорсинга, чтобы направлять заказчиков в процессе модернизации, внедрения нового продукта, его эксплуатации и управления с целью повышения уровня безопасности конечных точек сети.

Symantec предоставит также заказчикам доступ к дополнительным возможностям по восстановлению и контролю конечных точек сети, чтобы они могли быстрее получить еще большие выгоды от Symantec Endpoint Protection 11.0. Новый компонент Symantec Endpoint Protection Integration Component представляет собой бесплатный инструмент, объединяющий Symantec Endpoint Protection с платформой управления Altiris, помогая заказчикам рационализировать развертывание системы, осуществить переход с конкурирующих продуктов и создать безопасные конфигурации конечных точек сети. Интегрированные технологии защиты и управления для конечных точек сети обеспечивают защищаемые системы всеми средствами восстановления, помогая повысить готовность приложений и безопасность данных при уменьшении общей стоимости владения.

Лицензирование и начало поставок

Symantec Endpoint Protection 11.0 и Symantec Network Access Control 11.0 уже поставляются, и их можно приобрести через всемирную сеть авторизованных реселлеров, дистрибьюторов и системных интеграторов Symantec.

WWW.GLONASS-FORUM.RU WWW.NAVIGATION-FORUM.RU РЕГИСТРАЦИЯ: +7 (495) 797 62 22 INFO@NAVIGATION-FORUM.RU

МЕЖДУНАРОДНЫЙ ФОРУМ ПО СПУТНИКОВОЙ НАВИГАЦИИ 2008

ВЫСТАВКА

КОСМИЧЕСКИЕ ТЕХНОЛОГИИ ДЛЯ БИЗНЕСА

- **Системы ГЛОНАСС, GPS и GALILEO состояние и перспективы**
- **Российский рынок навигационных услуг**
- **Принципы российской государственной политики в области использования спутниковых навигационных систем**
- **Новые типы высокорентабельного бизнеса на основе технологии спутниковой навигации**
- **Использование навигационных технологий в региональных и муниципальных программах**
- **Опыт ведущих российских и зарубежных компаний в разработке и использовании оборудования и технологий спутниковой навигации**

ЦЕЛЕВАЯ АУДИТОРИЯ ФОРУМА

- Предприятия и организации нефтегазовой отрасли
- Энергетические компании
- Телекоммуникационные компании
- Автотранспортные предприятия
- Торговые сети, крупные организации с собственным автомобильным парком
- Компании, занимающиеся железнодорожными, воздушными и морскими перевозками
- Строительные фирмы
- Логистические и экспедиторские компании
- Дистрибьюторы сотового оборудования и услуг
- Контент-провайдеры
- Провайдеры охранно-поисковых услуг
- Службы городского ЖКХ
- Аварийно-спасательные службы
- Геодезические и картографические организации
- Разработчики и производители абонентского оборудования и системных приложений
- Представители государственных ведомств и организаций
- Представители областных, городских и районных администраций

ОРГАНИЗАТОР ФОРУМА:

PROFI-CENTRE ПРОФЕССИОНАЛЬНЫЕ КОНФЕРЕНЦИИ

ПРИ ПОДДЕРЖКЕ:

Роскосмос

Мининформсвязи

ГЛОНАСС/ГНСС Форум — Ассоциация ГЛОНАСС/ ГНСС-Форум

ЭКСПЕРТНЫЕ ПАРТНЕРЫ:

РНИИ КП

ЦНИИМАШ TSNIIMASH — ЦНИИМАШ

M2M — M2M телематика

Навигационные системы на рынке B2B

В ПРОШЛЫХ НОМЕРАХ ЖУРНАЛА УЖЕ ОСВЕЩАЛАСЬ ТЕМА РАЗВИТИЯ КОСМИЧЕСКИХ ТЕХНОЛОГИЙ И СОЗДАНИЕ СПУТНИКОВЫХ СИСТЕМ ПОЗИЦИОНИРОВАНИЯ НА БАЗЕ СИСТЕМ ГЛОНАСС И GPS. В СТАТЬЕ УФИМЦЕВА А. "ГЛОНАСС И GPS: В БУДУЩЕЕ ВМЕСТЕ?" ОПИСЫВАЛИСЬ ТЕХНИЧЕСКИЕ АСПЕКТЫ И СРАВНЕНИЕ ЭТИХ СИСТЕМ.

НАСТОЯЩЕЙ СТАТЬЕЙ ХОЧЕТСЯ ПРОДОЛЖИТЬ ЭТУ ТЕМАТИКУ И БОЛЕЕ ПОДРОБНО РАССКАЗАТЬ О ПРИМЕНЕНИИ НАВИГАЦИОННЫХ СИСТЕМ НА РЫНКЕ B2B, А ИМЕННО О ВНЕДРЕНИЯХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ МОНИТОРИНГА И УПРАВЛЕНИЯ ТРАНСПОРТОМ НА БАЗЕ СИСТЕМ В КОРПОРАТИВНЫХ АВТОПАРКАХ ПРЕДПРИЯТИЙ РАЗЛИЧНЫХ ОТРАСЛЕЙ.

Светлана Хадонова,
директор по маркетингу
компании "M2M телематика"

Росту популярности спутниковых систем мониторинга и управления способствовали достижения в разных областях науки и техники. Автотранспорт становится совершеннее и все больше оснащается различными электронными устройствами. Электронный блок управления двигателем и бортовой маршрутный компьютер с необходимыми им датчиками и периферийными устройствами — непременные атрибуты автомобилей XXI века.

Кроме того, меняются подходы в самом управлении корпоративными автопарками. Все больше и больше компаний стремятся максимально автоматизировать внутренние процессы управления.

Что же представляет собой подобная автоматизация, и какую выгоду она приносит предприятию?

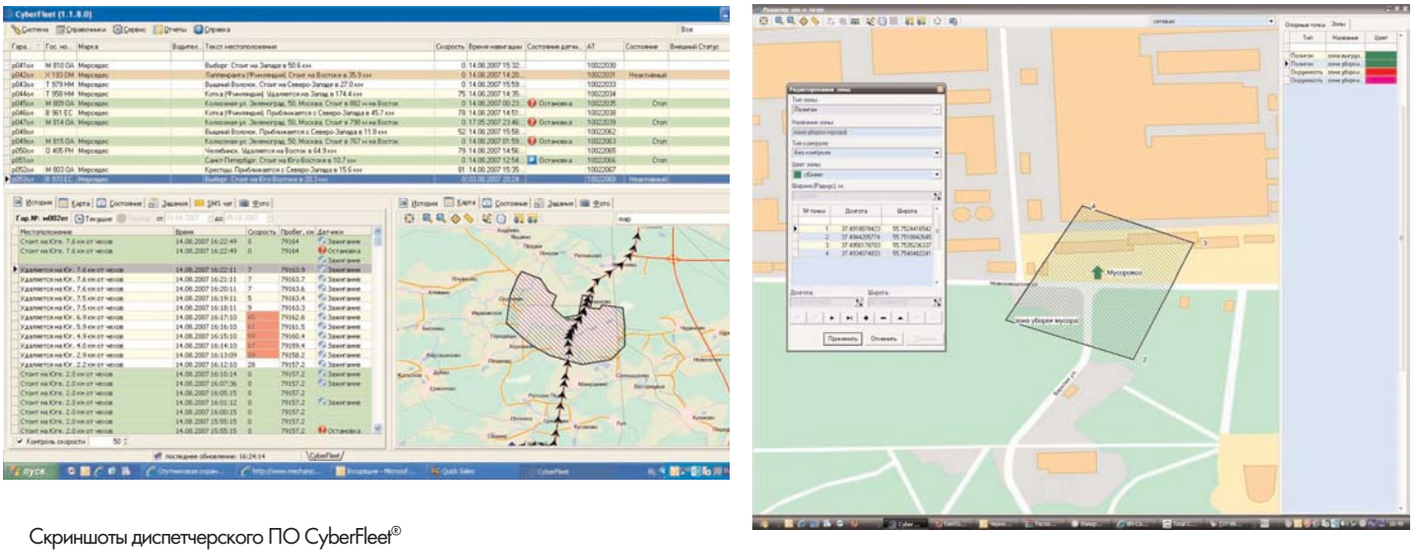
Начнем с первого и самого главного. Меняются и совершенствуются технологии, меняются подходы к управлению, но одно всегда остается неизменным — ***человеческий фактор***.

До сих пор любое предприятие в собственном автопарке сталкивается с большими проблемами, такими как слив топлива, "левые рейсы", сговоры между диспетчерами и водителями о приписанном километраже, простои по вине водителей и диспетчеров и т.д. Целая комбинация проблем.

Как их решать, каким образом осуществлять административный контроль? Наверное, каждый руководитель задает себе часто подобный вопрос.

Вот тут на помощь приходит мониторинг и навигация.

Простейший пример. Навигационная система ГЛОНАСС или GPS при добавлении к ней специального оборудования и программного обеспечения становится ***мощным инструментом административного контроля***. А если дополнить ее различной периферией (датчиками расхода топлива, открытия дверей фургона,



Скриншоты диспетчерского ПО CyberFleet®

поднятия кузова самосвала, тревожной кнопкой вызова водителя, громкой связью с водителем), то можно получить совершенно достоверную картину работы водителя и транспортного средства.

Как это работает?

Механизм работы таких систем выглядит следующим образом: абонентский ***ГЛОНАСС/GPS-терминал***, установленный на транспортное средство, определяет его местоположение, скорость, направление движения. Эти данные, а также данные от датчиков по каналам связи, направляются в центр сбора и обработки информации, откуда по выделенным линиям или через Интернет попадают на компьютер (рабочее место) диспетчера или руководителя.

В системах могут использоваться различные каналы спутниковой и сотовой связи. Чаще всего для мониторинга транспортных средств используются каналы сотовой связи GSM/GPRS. Для АТП, чьи транспортные средства перемещаются в больших городах и их окрестностях, использование сотовых сетей, поддерживающих протокол передачи данных GPRS (***система BN-City®***), является наиболее оптимальным решением как с точки зрения надежности установления и поддержания соединения, так и с точки зрения затрат.

В случае если предприятие осуществляет междугородние или международные грузоперевозки, целесообразно использовать систему мониторинга ***BN-Global®***, использующую каналы спутниковой связи Инмарсат. Такое решение особенно актуально, если перевозки осуществляются в Сибири или Заполярье, там, где сотовая связь зачастую отсутствует.

Специальное диспетчерское ПО ***CyberFleet®***, установленное на рабочем месте, обеспечивает привязку информации о подвижном объекте к цифровой карте, а также доступ к базе данных транспортных средств и дополнительный информационный и коммуникационный сервис.

ПО CyberFleet® контролирует состояние по многим параметрам, планирует и проверяет выполнение маршрутов, сигнализирует об их нарушении, оптимизирует их, контролирует отклонение от маршрута, вход и выход из заданных географических зон. Программа отслежи-

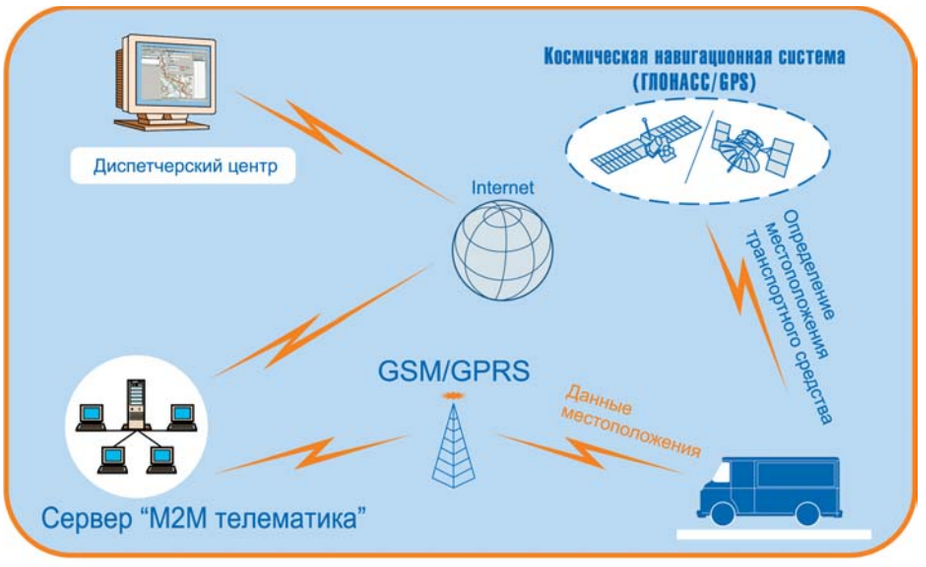


Схема работы автоматизированной системы мониторинга и управления транспортом BN-City®

Абонентский ГЛОНАСС/GPS/GPRS терминал M2M-Cyber GLX
(производство Россия, "М2М телематика")

вает работу двигателя и расход топлива, контролирует доставку груза в срок, время и место погрузки и выгрузки, начало и окончание работы, нецелевое использование техники. Программа автоматически определяет состояние автомобиля и всех его систем по показаниям датчиков включения зажигания, открытия дверей, срабатывания различных сигнальных устройств, подъема кузова, изменения температурного режима. Она передаст диспетчеру внеочередное сообщение при длительном простое и начале движения, при нажатии водителем его тревожной кнопки.

С помощью программы можно в любой момент вызвать водителя по громкой связи или через зуммер. Через нее можно вести обмен сообщениями с мобильным телефоном водителя. Эта переписка будет сохранена в базе данных. Кроме этого CyberFleet® автоматически ведет журнал нарушений и нештатных ситуаций, а также запоминает все команды и действия диспетчера. Она автоматически заносит в память данные об абонентских терминалах с телематического сервера (если он установлен), создает разнообразные справочники для перекрестного ввода информации об автомобилях и персонале, которые можно распечатать в виде отчета, формирует отчеты в широко распространенном формате Excel, позволяющие иметь исчерпывающее "личное дело" на каждый автомобиль и груз.

Кроме отображения на карте, ПО диспетчерского пункта, как правило, предоставляет возможность ведения базы данных транспортных средств, фиксирует данные об автомобилях, например, тип и модель машины, ее государственный регистрационный номер, Ф.И.О. водителя и другую сопутствующую информацию.

В итоге, внедрив на предприятии систему мониторинга и управления транспортом, мы получаем мощный административный механизм, который, во-первых, может наконец положить конец "левым" рейсам водителей, причем как совершаемым водителями по собственной инициативе, так и в сговоре с персоналом диспетчерских пунктов. Во-вторых, полностью контролировать расход топлива, скорость, простои и отклонения от маршрута. Результат — увеличение пробега автотранспорта, затрат на топливо, увеличение длительности прохождения маршрута.

Перечень возможных дополнительных функций неисчерпаем. Можно установить на автомобиле видеокамеру, передающую изображение диспетчеру. Данные о работе подвижного состава легко архивируются, распечатываются в виде таблиц и графиков, суммируются и анализируются. Полученная информация позволяет оптимизировать работу предприятия, разработать более эффективные маршруты перевозок, исключить неоправданные простои.

Выгода очевидна

В этой статье затронута лишь одна из многих проблем, возникающих при управлении автопарком на предприятиях — влияние на процесс человеческого фактора.

Прозвучавшие рекомендации оставили в стороне множество других задач, решаемых автоматизацией на базе навигационных спутниковых систем — это объективная информация, полученная "здесь и сейчас", снижение рисков, повышение эффективности использования автотранспорта, отслеживание и ликвидация всевозможных помех и простоев, экономия затрат на диспетчерскую службу, оптимальное планирование перевозок и решение маршрутной задачи, точное документирование всех данных, оперативное предоставление информации о транспорте и грузе, объективный анализ работы автопарка и ряд других не менее важных моментов.

В заключение можно сказать, что цены на подобные системы стали доступны любому предприятию, имеющему собственный автопарк от одного транспортного средства и более. Сроки окупаемости систем — от 1 недели до 3-х месяцев.

Выгода — очевидна!

Питание и охлаждение для устройств VoIP и IP-телефонии

Висвас Пурани,
директор отдела разработки
новых технологий и приложений
компании APC,
Род-Айленд, США

ПРИ РАЗВЕРТЫВАНИИ ТЕХНОЛОГИИ VOIP МОГУТ ВОЗНИКАТЬ НЕОЖИДАННЫЕ И НЕПРЕДВИДЕННЫЕ ТРЕБОВАНИЯ К МОЩНОСТИ И ОХЛАЖДАЮЩЕЙ СПОСОБНОСТИ ДЛЯ КАБЕЛЬНЫХ ШКАФОВ И КАБЕЛЬНЫХ ПОМЕЩЕНИЙ. ПОНИМАНИЕ ОСОБЫХ ПОТРЕБНОСТЕЙ В ОХЛАЖДЕНИИ И ОБЕСПЕЧЕНИИ ПИТАНИЯ ОБОРУДОВАНИЯ ПОЗВОЛЯЕТ СПЛАНИРОВАТЬ УСПЕШНОЕ И ЭКОНОМИЧЕСКИ ВЫГОДНОЕ РАЗВЕРТЫВАНИЕ ТЕХНОЛОГИИ VOIP.

В СТАТЬЕ РАЗЪЯСНЯЕТСЯ, КАК СПЛАНИРОВАТЬ ОБЕСПЕЧЕНИЕ ПИТАНИЯ И ОХЛАЖДЕНИЯ ОБОРУДОВАНИЯ VOIP, А ТАКЖЕ ОПИСЫВАЮТСЯ ПРОСТЫЕ, БЫСТРЫЕ, НАДЕЖНЫЕ И ЭФФЕКТИВНЫЕ СТРАТЕГИИ ДЛЯ МОДЕРНИЗАЦИИ СТАРЫХ И СОЗДАНИЯ НОВЫХ РЕШЕНИЙ.

При замене существующих телекоммуникаций и офисных телефонных систем технология VoIP и IP-телефония должны обеспечить аналогичную или более высокую доступность. Одной из главных причин высокой доступности традиционной системы является то, что в АТС встроена резервная батарея, рассчитанная на длительный срок эксплуатации, обеспечивающая питание телефонов в сети. В IP-телефонии должна использоваться испытанная временем концепция обеспечения питания вместе с сигналом для достижения ожидаемой доступности. Традиционный кабельный шкаф, в котором размещались пассивные устройства, например коммутационные панели и концентраторы, теперь должен вмещать высокомощные коммутаторы, маршрутизаторы и ИБП, рассчитанные на длительный срок эксплуатации. Охлаждение и воздухоциркуляция в этих кабельных шкафах приобретают важное значение для обеспечения гарантии непрерывной работы.

Типичная сеть IP-телефонии строится по уровням, и каждый из них состоит из компонентов, которые размещаются в одном из четырех физических местоположений (рис. 1). Требования к мощности и охлаждающей способности для этих четырех местоположений варьируются, как это описано в последующих разделах.

Устройства связи

Типичными устройствами связи/конечными точками являются IP-телефоны и беспроводные концентраторы (рис. 2), а также переносные компьютеры с установленными на них программами телефонной связи, обеспечивающими стандартные функции телефонии. Эти IP-телефоны обычно потребляют 6-7 Вт, но некоторые устройства могут потреблять больше энергии. В новом проекте инструкции IEEE 802.3af средний ток, потребляемый такими устройствами с кабелей CAT5, ограничен до 350 мА, а также указаны контакты, через которые может подаваться питание. Сеть, соответствующая этому новому стандарту, будет передавать электроэнергию мощностью 15 Вт на расстояние до 100 м. При более высокой потребляемой мощности устройства связи должны использовать другие источники питания наподобие подключаемых адаптеров.

Условия эксплуатации

Устройства связи размещаются на рабочих столах, иногда монтируются на стене и используются в офисе. В современных разворачиваемых или модернизированных сетях эти устройства, вероятнее всего, питаются от линий передачи данных. Однако в некоторых случаях они должны питаться от розеток электросети.

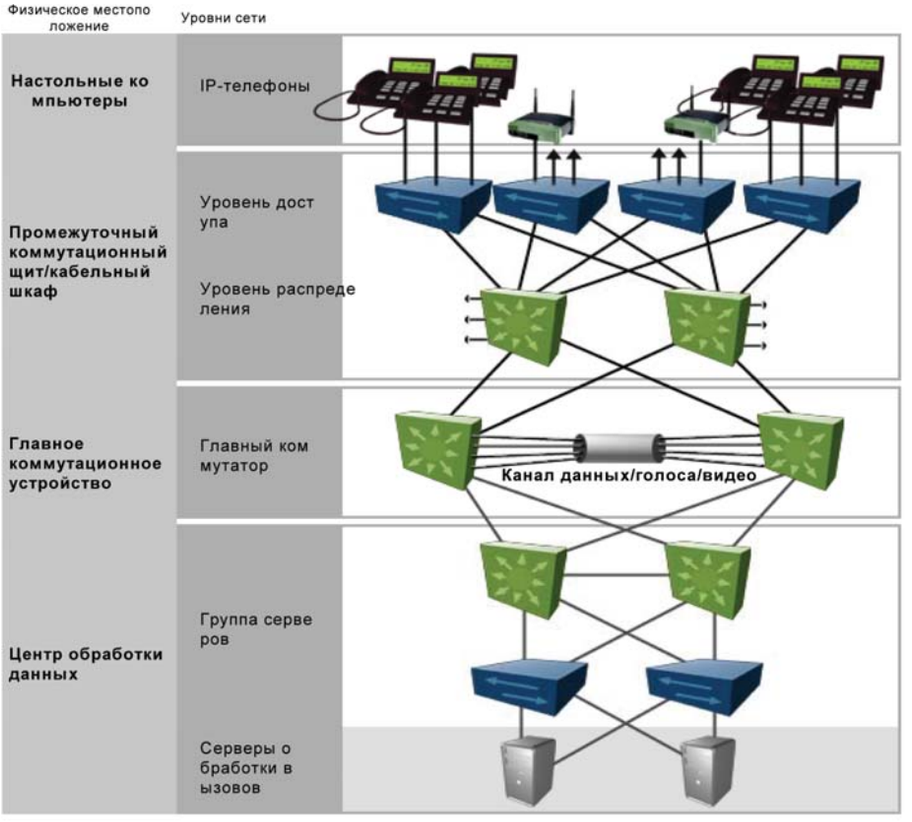


Рис. 1. Уровни и местоположения типичной сети IP-телефонии

Проблемы

IP-телефоны, как правило, должны быть доступны, как и обычные телефоны, на смену которым они приходят. Главной проблемой, которая должна быть решена в этой ситуации, является непрерывная работа устройств даже во время длительных перерывов в энергоснабжении.

Оптимальные методы

Самый оптимальный способ решения этой проблемы — передача питания (так называемого линейного питания) на телефон по линии передачи данных. Тем самым устраняется проблема обеспечения питания в том месте, где располагается рабочий стол. Питание на телефон теперь подается с помощью сетевого коммутатора, расположенного в кабельном шкафу, для поддержки которого используется система ИБП, рассчитанная на продолжительное время автономной работы. Для устройств связи, которые питаются от розеток электросети (т.е. не используют линейное питание), можно предусмотреть систему ИБП с батареей, обеспечивающей резервное питание в течение продолжительного времени (четыре, шесть, восемь или более часов).

Промежуточный коммутационный щит (IDF)

IDF или кабельные шкафы включают в себя сетевые уровни 2 и 3, коммутаторы доступа и распределения, концентраторы, маршрутизаторы, коммутационные панели, систему ИБП с батареей резервного питания, а также любое другое телекоммуникационное оборудование, смонтированное в стойке с двумя опорами (рис. 3). Для снабжения питанием устройств связи во многих новых коммутаторах имеется встроенная возможность передачи питания по линиям передачи данных (так называемые "оконечные" источники питания). Для коммутаторов, в которых отсутствует такая возможность, подача линейного питания осуществляется с помощью внешнего "врезного" источника питания соответствующих размеров.

Условия эксплуатации

Промежуточные коммутационные щиты или кабельные шкафы обычно скрыты в отдаленных частях помещения с минимальной или отсутствующей вентиляцией и освещением. До тех пор, пока потребитель не переедет в новое здание, он, скорее всего, захочет использовать существующие кабельные шкафы. В традиционных телекоммуникационных сетях кабельные шкафы обычно использовались в основном для монтажных блоков, коммутационных панелей и небольших наращиваемых концентраторов или коммутаторов, однако в большей части нового оборудования IP-телефонии используется

Рис. 2. IP-телефон и беспроводной концентратор

и рассеивается значительно большая мощность. Новые коммутаторы IP-телефонии являются главным образом устройствами для монтажа в 19-дюймовом монтажном шкафу. В них используются различные принципы воздухоциркуляции в зависимости от изготовителя, например с поперечным воздушным потоком, прямо направленным воздушным потоком и т.д. Типичный промежуточный коммутационный щит вмещает оборудование, расположенное в 1-3 стойках, и потребляет от 500 до 4 000 Вт однофазного переменного тока.

Проблемы

При развертывании технологии VoIP и IP-телефонии особое внимание следует уделить питанию и охлаждению для промежуточных коммутационных щитов. Они потребляют мощность в диапазоне от 500 до 4000 Вт однофазного тока напряжением 208 В, что зависит от сетевой архитектуры и типа используемого коммутатора. Обеспечение разъемами нужного типа и соответствующего уровня мощности с необходимой защитой автоматическими предохранителями для всего сетевого оборудования, ИБП и устройств распределения электропитания (PDU) представляет собой сложную задачу. Охлаждение и воздушный поток в этих кабельных шкафах часто являются серьезной проблемой, которой так же часто не придают значения.

Оптимальные методы

Все оборудование в промежуточном коммутационном щите должно быть защищено системой ИБП, выбор которой основывается на следующих факторах.

- общая требуемая мощность в ваттах;
- требуемое время работы в минутах;
- желательный уровень избыточности или отказоустойчивости;
- требуемые напряжения и разъемы.

Размеры системы ИБП определяются в соответствии с суммой номинальных значений нагрузок в ваттах.

Общераспространенный ИБП для монтажа в стойку, например APC Smart-UPS (рис. 4а), обеспечит доступность примерно 99,99 %, тогда ИБП со встроенной обходной цепью (байпасом) и избыточностью N+1, например APC Symmetra RM (рис. 4б), с одним часом автономной работы, обеспечит примерно 99,999 %, что может быть достаточно для многих видов применения. Устройства ИБП поставляются с комплектами батарей, обеспечивающими различное время автономной работы. Продукты,

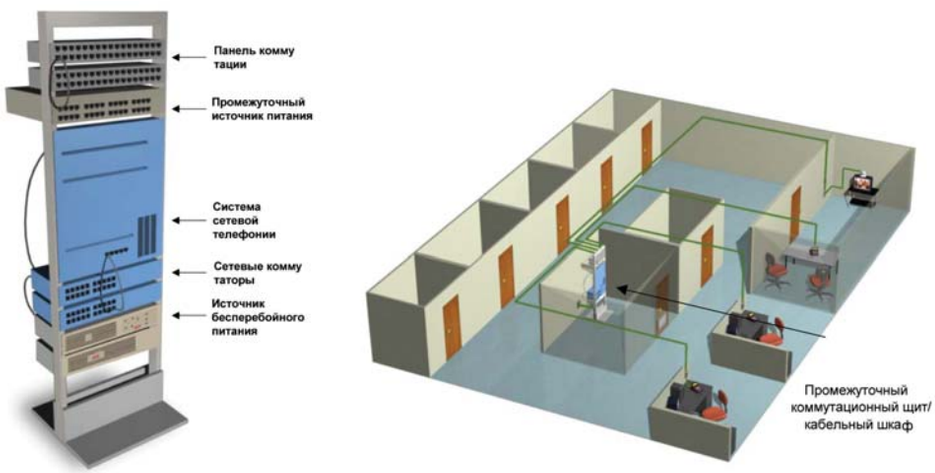


Рис. 3. Типичное расположение промежуточного коммутационного щита

а *б*

Рис. 4. APC Smart-UPS (*а*) и APC Symmetra RM (*б*)

изображенные на рис. 4, поставляются с дополнительными комплектами батарей, с помощью которых время автономной работы можно увеличить до 24 ч.

Высокие уровни доступности (99,9999 или 99,99999%) могут быть необходимы для критически важных служб, например 911. Такие требования можно осуществить, если установить сдвоенные сетевые коммутаторы с двойными блоками питания, два ИБП и одновременно параллельно работающие электрические линии с резервным питанием от генератора. Многие компании, как и корпорация American Power Conversion, создали консультационные службы по вопросам доступности, чтобы оценить и рекомендовать инфраструктуры энергоснабжения высокого уровня доступности для подобных критически важных сетей.

И наконец, следует упомянуть о типах вилок и розеток, необходимых для всего оборудования, включая ИБП в кабельном шкафу. В идеальных условиях все оборудование должно напрямую подключаться к задней панели ИБП или трансформатора; кроме того, следует избегать использования дополнительных удлинителей "пилотов" или устройств распределения электропитания (PDU) в стойке. Однако при большом количестве оборудования это может быть нецелесообразно, и следует использовать шину с PDU для монтажа в стойку. В таком случае необходимо использовать высококлассное устройство, специально предназначенное для этой цели. В устройстве распределения электропитания должно быть достаточное число розеток для подключения всего текущего оборудования и несколько запасных розеток для будущих потребностей.

Предпочтительны PDU с функцией измерения, показывающие текущую потребляемую мощность, так как они снижают вероятность ошибок человеческого фактора, например таких, как случайная перегрузка и возникающие в результате падения нагрузки.

Для обеспечения непрерывной работы оборудования в кабельном шкафу (7*24*365) необходимо обязательно решить такие вопросы, как охлаждение и воздухоциркуляция. Чтобы определить наиболее экономичный способ решения этой проблемы (табл. 1), необходимо рассчитать рассеяние мощности в кабельном шкафу. Самым важным в данной ситуации является то, что многочисленные сетевые коммутаторы потребляют много электроэнергии, однако это не означает, что они рассеивают всю потребляемую мощность в кабельном шкафу. Например, коммутатор уровня 2 может потреблять 1 800 Вт, но в кабельном шкафу может рассеиваться только 200-500 Вт. Остальная мощность подается по сети на многочисленные IP-телефоны, установленные во всех подразделениях офиса, и рассеяние мощности происходит по всему офису.

После того как мощность, рассеиваемая в кабельном шкафу, рассчитана, следуйте общим правилам, изложенным в табл. 2. Для этих кабельных шкафов настоятельно рекомендуется использовать блок контроля микроклимата (т.е. температуры и влажности), так как это позволит отслеживать отклонения от нормальных условий и обеспечит достаточное время для принятия превентивных мер, чтобы предотвратить простой.

Таблица 1

Расчет теплоотдачи в кабельном шкафу VoIP

Обозначение	Необходимые данные	Расчет теплоотдачи
Коммутаторы без линейного питания; другое оборудование ИТ (кроме промежуточных блоков питания)	Суммарная входная номинальная мощность в ваттах	Такая же, как общая полезная выходная мощность ИТ в ваттах
Коммутатор с возможностью подачи линейного питания	Номинальная входная мощность в ваттах	0,6 х номинальную входную мощность
Промежуточные блоки питания	Номинальная входная мощность в ваттах	0,4 х номинальную входную мощность
Освещение	Номинальная мощность любых постоянно включенных осветительных устройств в ваттах	Номинальная мощность
Система ИБП	Номинальная мощность системы ИБП (не нагрузка) в ваттах	0,09 х номинальную мощность ИБП
Итого	Вышеуказанные промежуточные суммы	Общая сумма вышеуказанных промежуточных сумм теплоотдачи

Главный коммутационный щит (MDF)

Главные коммутационные щиты также называются главными аппаратными или точками присутствия. В них размещается самое важное оборудование VoIP и IP-телефонии, например маршрутизаторы уровня 3, коммутаторы и различное другое сетевое, телекоммуникационное и ИТ-оборудование (рис. 5). Телекоммуникационные линии T1 и T3 выходят на главные коммутационные щиты и обеспечивают связь с Интернет-магистралью.

Условия эксплуатации

Главные коммутационные щиты обычно располагаются на цокольном или первом этаже здания вместе с прочими служебными помещениями. Типичный главный коммутационный щит состоит из 4-12 стоек и потребляет от 4 до 40 кВт однофазного или трехфазного переменного тока 220 В. Кроме того, возможно размещение оборудования, для которого требуется 48 В постоянного тока. В большинстве случаев стойки в главном коммутационном щите являются открытыми стойками с двумя опорами, что позволяет выполнять монтаж разнообразного ИТ-оборудования и IP-телефонии. В этом оборудовании могут применяться различные схемы циркуляции воздушного потока, например поперечный воздушный поток, прямо направленный воздушный поток и т.д. Оборудование предназначено для монтажа в 19- или 23-дюймовом монтажном шкафу. Однако большая часть нового оборудования IP-телефонии и ИТ рассчитана для монтажа в 19- или 23-дюймовом монтажном шкафу.

Проблемы

Некоторые помещения главного коммутационного щита не оборудованы ИБП, во многих не обеспечено адекватное время работы от батареи, и зачастую они не имеют выделенной прецизионной системы охлаждения.

Оптимальные методы

Так как эти главные коммутационные щиты питают множество критических сетей и оборудования для ИТ и телефонии, их необходимо рассматривать как небольшие центры обработки данных или машинные залы. Чтобы обеспечить практически подачу питания с уровнем надежности 99,999%, помещения с главными коммутационными щитами должны иметь модульный резервный ИБП с внутренней обходной цепью (байпасом) со временем работы от батареи не менее тридцати минут. Большего времени работы с более высокими уровнями доступности (99,9999 или 99,99999%) можно достичь за счет использования сдвоенных сетевых коммутаторов с двойными кабелями питания, сдвоенных ИБП и параллельно работающих электрических линий с резервным питанием от генератора. Такие компании, как корпорация American Power Conversion, создали консультационные службы по вопросам доступности, чтобы оценить и рекомендовать архитектуру высокого уровня доступности для подобных критически важных сетей.

Главные коммутационные щиты должны иметь собственные прецизионные блоки кондиционирования воздуха с контролем микроклимата. Для критических устройств, требующих увеличения доступности, рекомендуется установить резервные установки кондиционирования воздуха. Для предотвращения образования "горячих" точек в стойках высокой мощности (> 3 кВт/стойка) следует использовать дополнительные устройства распределения и отвода воздуха. В отличие от серверов и систем хранения во многих используется поперечный воздушный поток. Это создает особые проблемы при установке в помещениях с закрытыми стойками.

Центр обработки данных или группа серверов

Центр обработки данных или группа серверов (рис. 6) включает все серверы приложений IP-телефонии, а также их программное обеспечение, например Call Managers, Unified Messaging и т.д. Кроме того, в зависимости от сетевой архитектуры и размера организации сюда же могут входить главные коммутаторы (уровень 3) и коммутаторы распределения (уровень 2). В зависимости от их размера (малый, средний или большой) стандартный центр обработки данных или группа серверов могут включать от нескольких десятков до нескольких сотен стоек, заполненных десятками или сотнями серверов и различных ИТ, сетевых и компьютерных систем, на которых работают такие критические приложения, как ERP, CRM и другие web-службы.

Таблица 2

Решения охлаждения кабельного шкафа VoIP

Общая тепловая нагрузка в кабельном шкафу	Условие	Анализ	Решение
< 100 Вт	Остальная часть здания является кондиционируемым пространством	Проводимость и инфильтрация стен будет достаточной	Нет
< 100 Вт	Остальная часть здания является неблагоприятной средой; система нагревания.	Свежий воздух снаружи помещения нельзя рассматривать как безопасный для использования из-за температуры или загрязненности	Установка автономного кондиционера с компьютерным управлением в шкафу рядом с оборудованием
	вентиляции и кондиционирования воздуха отсутствует		
100 - 500 Вт	Над подвесным потолком имеется система нагревания, вентиляции и кондиционирования воздуха; остальная часть здания является кондиционируемым пространством	Свежего воздуха снаружи кабельного шкафа будет достаточно, если он будет проникать внутрь, однако дверь может быть преградой для попадания воздуха. Попадание воздуха через дверь и вывод через обратный воздуховод системы нагревания, вентиляции и кондиционирования воздуха	Установка рециркуляционной решетки в системе вентиляции в верхней части шкафа; обеспечение вентиляционного проема в нижней части двери шкафа.
100 - 500 Вт	Отсутствие доступа из шкафа к системе нагревания, вентиляции и кондиционирования воздуха. Остальная часть здания является кондиционируемым пространством	Свежего воздуха снаружи кабельного шкафа будет достаточно, если он будет проникать внутрь, однако дверь может быть преградой для попадания воздуха. Попадание воздуха через нижнюю часть двери и вывод через верхнюю часть двери	Установка вытяжной решетки в верхней части двери шкафа; обеспечение воздухозаборника в нижней части двери шкафа.
500 - 1000 Вт	Над подвесным потолком имеется система нагревания, вентиляции и кондиционирования воздуха; остальная часть здания является кондиционируемым пространством	Свежего воздуха снаружи кабельного шкафа будет достаточно, если он будет проникать внутрь постоянно, однако дверь может быть преградой для попадания воздуха, и потребуется непрерывная работа вентилятора, хотя и это не дает полной гарантии	Установка рециркуляционной решетки с дополнительным вентилятором в верхней части шкафа; обеспечение вентиляционного проема в нижней части двери шкафа.
500 - 1000 Вт	Отсутствие доступа из шкафа к системе нагревания, вентиляции и кондиционирования воздуха. Остальная часть здания является кондиционируемым пространством	Свежего воздуха снаружи кабельного шкафа будет достаточно, если он будет проникать внутрь постоянно, однако воздух не попадает внутрь.	Установка вытяжной решетки с дополнительным вентилятором в верхней части двери; обеспечение вентиляционной решетки в нижней части двери шкафа.
> 1000 Вт	Над подвесным потолком имеется система нагревания, вентиляции и кондиционирования воздуха с открытым доступом; остальная часть здания является кондиционируемым пространством	Свежего воздуха снаружи кабельного шкафа будет достаточно, если он будет проникать непосредственно через оборудование, а горячий отработанный воздух от оборудования не рециркулируется в воздухозаборник для оборудования	Установка оборудования в закрытую стойку с системой вывода горячего отработанного воздуха; обеспечение вентиляционной решетки в нижней части двери шкафа.
> 1000 Вт	Система нагревания, вентиляции и кондиционирования воздуха отсутствует; остальная часть здания является кондиционируемым пространством	Воздуха, проникающего через дверь, недостаточно; требуется местное охлаждение отработанного воздуха из оборудования	Установка автономного кондиционера с компьютерным управлением в шкафу рядом с оборудованием

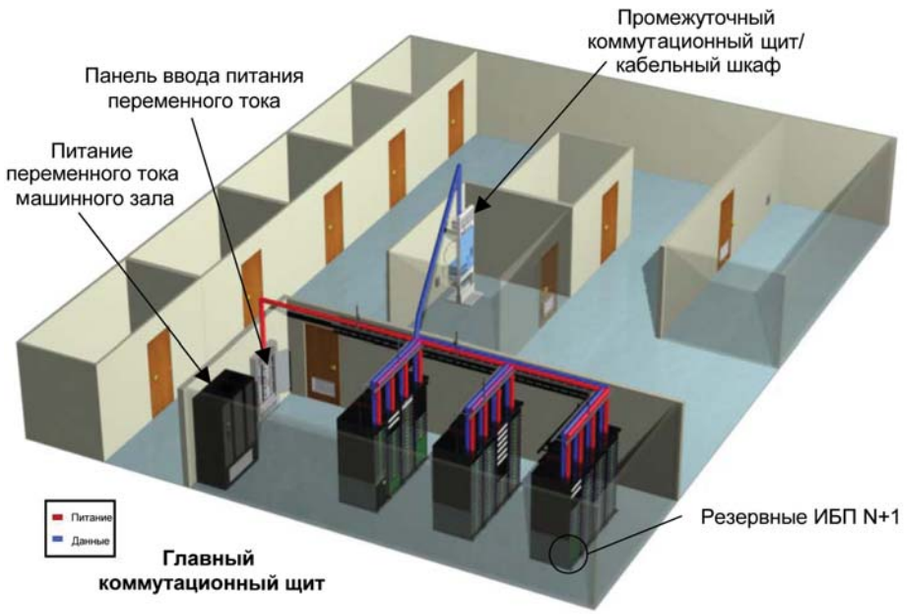


Рис. 5. Главный коммутационный щит (MDF)

Условия эксплуатации

Центры обработки данных обычно расположены в корпоративном офисе, потребляя от 10 кВт однофазного питания 220 В до сотен киловатт 3-фазного питания 380 В. Для подключения некоторых телекоммуникационных устройств может требоваться некоторое число розеток для подключения питания -48 В, но это скорее исключение. В большинстве центров обработки данных имеется ИБП с резервным аккумулятором, генератор и блоки прецизионных кондиционеров.

Проблемы

Серверы и коммутаторы IP-телефонии, как правило, создают неожиданно увеличивающуюся нагрузку для центра обработки данных, и могут требовать большего времени автономной работы, избыточности и доступности по сравнению с другим оборудованием ИТ или сети.

Оптимальные методы

Несмотря на то, что в центре обработки данных может быть собственный ИБП и генератор, во многих случаях для оборудования IP-телефонии, возможно, потребуется установить отдельный, резервный ИБП с большим временем автономной работы от батареи. Определите оборудование IP-телефонии, для которого требуется большее время работы и доступность, и соберите его в отдельном месте, в выделенных стойках центра обработки данных. При необходимости установите отдельный ИБП с большим временем автономной работы и избыточностью N+1 или N+2. Концепция "выделенной доступности" позволяет увеличивать доступность важного для бизнеса оборудования IP-телефонии без больших затрат на модернизацию всего центра обработки данных. В центрах обработки данных и сетях с высокой доступностью рекомендуется устанавливать более мощные резервные системы, например двойные источники с дублированными генераторами, а также два ИБП N+1 с двумя путями подачи питания к серверу и другому важному оборудованию в стойке.Убедитесь, что прецизионное оборудование для кондиционирования воздуха центра обработки данных имеет охлаждающую способность, достаточную для охлаждения дополнительного оборудования IP-телефонии. Для увеличения доступности рекомендуется установить резервные установки кондиционирования воздуха. Для предотвращения образования "горячих" точек в стойках высокой мощности (> 3 кВт/стойка) следует использовать дополнительные устройства распределения и отвода воздуха. Можно избежать типичных ошибок, которые допускаются при установке систем охлаждения и стоек в центрах обработки данных и помещениях для сетевого оборудования и уменьшают доступность, увеличивая расходы.

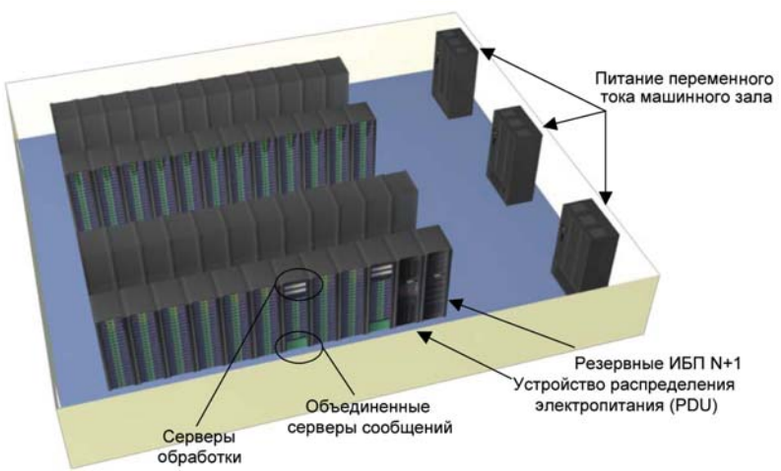


Рис. 6. Типичный центр обработки данных или группа серверов

Выводы

С устройствами связи не возникает никаких проблем, поскольку они используются в офисных помещениях. Соответственно, не существует серьезных проблем с центрами обработки данных или группами серверов, поскольку увеличивающаяся нагрузка оборудования для IP-телефонии добавляется случайным образом. Однако для важных серверов и коммутаторов IP-телефонии можно обеспечить "выделенную доступность". При наличии главных коммутационных щитов могут возникнуть небольшие проблемы, связанные с доступным временем работы, которые можно решить, подключив генератор или большую батарею с ИБП. Самые серьезные проблемы, которые могут возникнуть в связи с питанием и охлаждением, касаются, прежде всего, кабельных шкафов. Небольшой, отдельный ИБП с увеличенным временем работы остается более экономичным решением по сравнению с крупным, централизованным ИБП, который подает питание на все кабельные шкафы. Охлаждение — это особая проблема, возникающая при эксплуатации кабельных шкафов; зачастую одной вентиляции недостаточно. В некоторых случаях требуется точечное кондиционирование воздуха.

12

ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ

по IP-телефонии и IP-коммуникациям

27–28 ноября 2007 г.

Москва,
отель Холидей ИНН Сокольники

Регистрация:
http://iptconf.ru/12

Организаторы

COMPTEK

ИНФОСОФТ

Генеральный Спонсор

AVAYA

Спонсор регистрации

VoIP exchange

Генеральный Информационный Партнер

c·news

Информационная поддержка

itnews

Современные телекоммуникации

технологии и средства связи

журнал Электроника

connect!

Информационно-аналитическое агентство сотовик

COMNEWS

it manager

Журнал Электросвязь

ИКС

МС

T·Comm

VSAT-технологии в рамках нацпроекта "Образование"

"ГЛОБАЛ-ТЕЛЕПОРТ" ПОДВЕЛ ИТОГИ СВОЕГО УЧАСТИЯ В РЕАЛИЗАЦИИ НАЦИОНАЛЬНОГО ПРОЕКТА "ОБРАЗОВАНИЕ". ЗА ПОЛГОДА КОМПАНИЯ ПОДКЛЮЧИЛА К ИНТЕРНЕТУ ЧЕРЕЗ СПУТНИКОВЫЕ КАНАЛЫ СВЯЗИ 5638 ШКОЛ В 53 РЕГИОНАХ РОССИИ. ЕЩЕ ОКОЛО 4 ТЫС. VSAT-ТЕРМИНАЛОВ УСТАНОВЛЕНО В РАМКАХ ДРУГИХ ПРОЕКТОВ "ГЛОБАЛ-ТЕЛЕПОРТА".

Алексей Васильев,
независимый эксперт

Компания "Глобал-Телепорт" (www.gtport.ru) — оператор спутниковой связи. Образована в 2005 г. Входит в группу компаний Synterra. Учредителем компании является ЗАО "Синтерра". Основное направление деятельности компании — предоставление услуг спутниковой связи на базе оборудования и технологий VSAT. Компания располагает четырьмя центральными земными станциями, осуществляющими управление сетями VSAT-станций на территории Российской Федерации, расположенными в Москве, Хабаровске, Новосибирске и Павловом Посаде. Для подключения используется оборудование производства компаний Gilat Satellit Networks Ltd и Hughes Network System.

В 2007 г. в России было развернуто больше малых спутниковых наземных станций (Very Small Aperture Terminal —VSAT), чем за предыдущие 10 лет. Начиная с марта ЗАО "Глобал-Телепорт" ежемесячно устанавливал и вводил в эксплуатацию около тысячи VSAT-станций. Сегодня в его VSAT-портфеле более 10 тыс. терминалов.

Чем можно объяснить подобный невиданный доселе всплеск?

В значительной степени, это происходит благодаря упрощению разрешительных процедур. Использование компанией "Глобал-Телепорт" емкостей спутников "Экспресс-АМ" (в точках 40°, 80° и 140° в.д.) уже вело к упрощенной схеме эксплуатации Ku-диапазона. Но главным драйвером стал приоритетный национальный проект "Образование".

Государство дало первоначальный импульс, ведь для многих школ, находящихся в труднодоступных районах, VSAT-решения стали единственно возможными в рамках реализации нацпроектов по оснащению доступом в Интернет каждой российской школы и по оснащению телефонной связью и доступом в Интернет удаленных населенных пунктов страны (в рамках требований "Закона о связи"). Ни в одной стране мира развитие направления VSAT не происходило без участия государства. Везде были "большие" проекты, реализуемые на бюджетные деньги, которые давали старт широкому внедрению этой технологии в государственном,, корпоративном и частном секторах. Так что российский путь ничем не отличается от опыта других стран.

Для ускорения работ по проекту Мининформсвязи существенно упростило процедуру оформления заявок и получения разрешительных документов. Если обычным порядком на решение этой проблемы уходит около полугода, то для "школьного Интернета" время от момента подачи заявки до оформления документов сократилось до двух недель.

Во многих странах реализация подобных масштабных проектов происходила с привлечением огромного количества людей и техники. Например, в одной из южно-американских стран к установке малых станций привлекали военных. У нас государство пошло по другому пути. Был организован процесс взаимодействия заказчиков, поставщиков, операторов и регуляторов, при этом сами работы были поручены частным компаниям.

Глобал-Телепорт сумел доказать, что такого рода масштабные проекты можно реализовывать силами небольших компаний, при хорошо налаженном взаимодействии. Параллельно с сотнями ежедневных подключений станций, проходило обучение: "Глобал-Телепорт" обучил около 400 бригад (1200 человек, местных связистов), ставших партнерами компании по установке VSAT-оборудования в школах.

Еще один аспект влияния человечекого фактора: из сотни сотрудников "Глобал-Телепорта"

большинство "родом" из "ГлобалТела", опытного игрока рынка спутниковой связи. Именно поэтому компания, созданная в марте 2005 г., так быстро вошла в рынок и смогла за короткое время достичь столь высоких результатов.

Проект школьного Интернета у "Глобал-Телепорта" далеко не единственный. Компания установила 620 VSAT-станций на Алтае, в Хакасии, в Тюменской, Омской, Кемеровской и Новосибирской областях для пунктов коллективного доступа в Интернет в рамках оказания универсальных услуг связи,а также 1187 станций для спутниковой сети доступа к универсальным услугам связи с использованием таксофонов в Сибирском федеральном округе и 178 станций — в Архангельской области. На Дальнем Востоке построена сеть доступа к универсальным услугам с использованием пунктов коллективного доступа в Интернет и таксофонов (607 станций). Для ФГУП "Почта России" установлены 634 VSAT-станций в пунктах коллективного доступа. Поставщик оборудования для всех этих проектов — Gilat Satellite Networks. Реализуются аналогичные проекты в Дагестане и Чеченской Республике, где поставщиком терминалов выступает Hughes Network Systems. Кроме того, компания создает единую спутниковую сеть доступа для ведомственной транспортной сети Федерального казначейства из почти 2000 VSAT-терминалов.

Однако, "зеленая улица" по упрощенной схеме регистрации станций имеет место лишь в рамках национального проекта "Образование". А, например, для некоторых проектов создания спутниковой сети доступа к универсальным услугам с использованием таксофонов компания до сих пор не может получить разрешительных документов из-за бюрократических проволочек. В ряде случаев станции построены и оттестированы, но оператор, для которого эта работа выполнена, не может предоставлять услуги, поскольку станции не введены в эксплуатацию.

На данный момент в рамках договора с ОАО "РТКомм.РУ" — исполнителем государственного контракта по подключению к сети Интернет образовательных учреждений в рамках проекта "Образование", компания "Глобал-Телепорт" организовала спутниковые каналы связи для 5138 образовательных учреждений в 53 регионах, в том числе в Федеральных округах: Дальневосточном — 522 учебных заведения, Приволжском — 702, Северо-Западном — 503, Сибирском — 2034, Центральном — 14 и Южном — 1363. Проведены инсталляционные работы и подключение к спутниковой сети более 500 школ для ОАО "Южная телекоммуникационная компания" и ОАО "ЦентрТелеком".

Учитывая, что работы по установке и подключению спутникового оборудования начались в январе-феврале 2007 г., более 5500 подключенных станций за 7 месяцев — это очень серьезный результат, ставший возможным благодаря объединению усилий сотрудников Глобал-Телепорта и всех партнеров по проекту, включая инсталляторов, сотрудников "РТКомм.РУ" и "Синтерры", ФГУП "Космическая связь", "Россвязьнадзора", "Роспотребнадзора", "Рособразования", представителей местных административных и государственных структур. Для полного выполнения своих обязательств по проекту необходимо до 1 декабря 2007 г. инсталлировать и подключить еще 50 школ, находящихся в таких удаленных регионах, как Таймырский автономный округ. На первый взгляд, это совсем немного по сравнению с тем, что уже сделано, но эти точки самые непростые. Для их своевременного подключения "Глобал-Телепорт" рассчитывает на поддержку местных Администраций и аппаратов полномочных Представителей Президента РФ.

Сегодня ЗАО "Глобал-Телепорт" является лидером предоставления услуг на базе VSAT-решений. Но компания не останавливается на достигнутом и с оптимизмом смотрит в будущее.

Уже в следующем году планируется ввод новых тарифных планов, которые позволят заказчикам арендовать оборудование. Проводятся работы по развитию доставки контента в собственных сетях в рамках других проектов. В дальнейшем VSAT-решения помогут оказывать услуги телемедицины и платного телевидения.

От GERAN/UTRAN к LTE. Перспективы развития и эволюция технологий радиоинтерфейса

Наступит ли предел развития технологий сетей радиодоступа мобильной связи?

А. Голышко,
Технический эксперт АФК "Система"

НАБЛЮДАЯ ЭВОЛЮЦИЮ РАЗВИТИЯ ТЕХНОЛОГИЙ СЕТЕЙ РАДИОДОСТУПА, ПОРАЖАЕШЬСЯ ГЕНИЮ ЧЕЛОВЕЧЕСКОГО РАЗУМА. КАЖДОЕ СЛЕДУЮЩЕЕ ПОКОЛЕНИЕ СЕТЕЙ МОБИЛЬНОЙ СВЯЗИ ПРИНОСИТ ПРИНЦИПИАЛЬНО НОВЫЕ ТЕХНОЛОГИЧЕСКИЕ ВОЗМОЖНОСТИ, ЗНАЧИТЕЛЬНО РАСШИРЯЮЩИЕ СПЕКТР УСЛУГ КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЯМ. ЗНАЯ ПРОШЛЫЙ И ТЕКУЩИЙ УРОВЕНЬ РАЗВИТИЯ ЦИФРОВЫХ СЕТЕЙ МОБИЛЬНОЙ СВЯЗИ И ПОТРЕБНОСТИ АБОНЕНТОВ ИНТЕРЕСНО ЗАГЛЯНУТЬ В БЛИЖАЙШЕЕ БУДУЩЕЕ И ПОНЯТЬ, ЧТО НАС ОЖИДАЕТ.

Тихвинский В.О.
Генеральный директор
ЗАО "СТЕЛТ Телеком"

Терентьев С.В.
Системный архитектор
ОАО "МегаФон"

Анализ развития технологий сетей радиодоступа мобильной связи

Первое поколение цифровых сетей мобильной связи GSM (второе после аналоговых) создавалось с учетом оказания основной услуги — речевой. Так как речевой трафик считается симметричным, то за основу построения сетей радиодоступа был выбран метод частотного дуплекса FDD. Простая интеграция с телефонными сетями общего пользования PLMN, обеспечивающая высокие темпы развертывания сетей GSM в мире, потребовала от разработчиков реализации широко используемого принципа коммутации каналов CS (Circuit Switching) и системы сигнализации SS7. Развитие дополнительных услуг связи инициировало другие асимметричные типы трафика: потоковый, фоновый и в некоторых случаях интерактивный. Кроме того, гигантские темпы развития и эффективность сети Интернет показали высокую актуальность построения сетей по принципу коммутации пакетов PS (Packet Switching). В связи с этим современные сети мобильной связи поддерживают метод временного дуплекса TDD, их развитие строится с учетом концепции "все по IP".

С учетом модели взаимодействия открытых систем OSI [1] наиболее интересно рассмотреть протоколы физического и канального уровней (уровни 1,2), которые являются наиболее важными для радиоинтерфейса. Эти протоколы определяют характеристики так называемого канала связи (передатчик/модулятор — линия связи — приемник/демодулятор). Непрерывное улучшение характеристик канала связи связано с развитием используемых в нем технологий:

- преобразования первичной информации в двоичную последовательность (кодеры и вокодеры);
- повышения помехоустойчивости и эффективности (помехоустойчивого кодирования и декодирования данных; перемежения; расширения спектра; пространственно-временной и поляризационной обработки; пространственно-временного кодирования и т.д.);
- модуляции и структуры сигнала;
- разделения каналов и многостанционного доступа;
- управления параметрами излучаемого сигнала (например, мощностью, несущей частотой), приемо-передающими антенными системами (например, диаграммой направленности);
- оптимального приема и демодуляции и др.

Отличительной особенностью сетей GSM является:

- использование узкополосного сигнала с MSK — модуляцией с полосой 200 кГц и хорошими спектральными и корреляционными характеристиками, обусловленными выбором минимального индекса частотной модуляции и АЧХ сглаживающего фильтра на передающей стороне;
- жесткое распределение радиоресурсов сети между абонентами в режиме TDM;
- использование каскадного помехоустойчивого кодирования (внешний код — блоковый систематический циклический, внутренний — сверточный);
- построение подсистемы коммутации с уче-

том требований к использованию каналов TDM и сигнализации SS7.

Дальнейшее развитие сети GSM в направлении повышения скорости передачи пакетов данных GPRS (до 384 кбит/с) привело к созданию технологии **EDGE**. В ней повышение скорости передачи данных в три раза достигалось за счет перехода от бинарной манипуляции MSK к многопозиционной 8PSK. Однако, такое увеличение ансамбля сигналов (как и любое другое) привело к некоторому ухудшению помехоустойчивости и чувствительности. Другой отличительной особенностью технологии EDGE является реализация метода "повышающейся избыточности" при помехоустойчивом кодировании, суть которого заключается в повышении пиковой скорости передачи данных за счет возможного уменьшения избыточности кодов при адаптации (изменении мощности кодов) к качеству каналов связи.

Принципиально новым этапом развития мобильной связи является разработка и внедрение сетей **UMTS**, позволяющих обеспечить пиковую скорость передачи данных до 2,048 Мбит/с. Главным отличием сети UMTS от GSM/EDGE/GPRS стало использование широкополосных сигналов (ШПС) с полосой 5 МГц и базой сигнала много больше единицы ($B >> 1$). В сетях WCDMA/UMTS используются последовательные ШПС — DS-CDMA (Direct Sequence).

Расширение базы сигнала осуществляется путем ведения частотной избыточности, которая и предает радиосигналу UMTS определенные положительные свойства: высокую помехоустойчивость, устойчивость к воздействию многолучевости (при условии, что разница задержек распространения радиоволн различных направлений распространения больше чем длительность одного элемента сигнала UMTS — Тэ). Кроме того, использование широкополосных сигналов позволило реализовать новый метод разделения каналов в сети — кодовый CDM.

Важная особенность алгоритма доступа, используемого UMTS для кодового разделения каналов CDMA заключается в его чувствительности к мощности принимаемых радиосигналов. Поэтому в UMTS реализовано быстрое управление мощностью излучения. Другими особенностями UMTS являются [1]:

- гибкое распределение радиоресурсов сети радиодоступа UTRAN;
- управление качеством услуг в цепочке "конечный пользователь — конечный пользователь" QoS Bearer Service;
- увеличение эффективности использования физической среды передачи путем введения нового типа каналов — транспортных;
- оптимизация трафика опорной сети Core Network путем внедрения медиашлюзов MGW и SoftSwitch и максимальное расширение использования в сети протокола IP;
- широкое разнообразие адаптивных речевых кодеков (AMR-NB, AMR-WB, AMR-WB+);
- конвергенция с сетями фиксированной связи (использование SS7 поверх MTP3 или Sigtran);
- возможность реализации VoIP.

Дальнейшее развитие UMTS в целях повышения скоростей передачи данных и минимизации задержек передачи данных при использовании протоколов плоскостей пользователя и управления (User-plane, Control-plane) определило разработку технологий HSPA (HSDPA/HSUPA), в которых нашли свое применение многопозиционные сигналы с квадратурной амплитудной манипуляцией 16QAM, 64QAM. Особое внимание в этих технологиях в целях минимизации указанных задержек уделено модернизации прокола доступа к физической среде передачи MAC.

Технический бум вызванный использованием сигнала OFDM в беспроводных сетях передачи данных WiFi/WiMAX не обошел стороной и сети сотовой связи. Начавшийся путь разработки технологии HSOPA (High Speed OFDM Packet Access) вылился в концепцию длительной эволюции **LTE** (Long Term Evolution) системы UMTS.

Совершенствование технологий сетей радиодоступа UTRAN/HSPA в направлении LTE

Началом работы 3GPP — Партнерского проекта по сетям третьего поколения над дальнейшим развитием этих сетей считается семинар по эволюции RAN, проведенный 2-3 ноября 2004 г. в Торонто (Канада). Основными целями и задачами работ по дальнейшему развитию UMTS стали:

- снижение себестоимости на бит информации;
- увеличение количества услуг с ориентацией на требования абонентов;
- повышение гибкости использования имеющихся и новых частотных диапазонов;
- упрощение архитектуры, открытости интерфейсов;
- улучшение рационального потребления энергии абонентскими терминалами.
- обеспечение единых параметров стандартизации и исключение излишних опций.

Таким образом, главными целями эволюции систем 3G к технологии **Evolved UTRAN** (E-UTRAN) является дальнейшее улучшение качества предоставления услуг и уменьшение расходов пользователей, а также и эксплуатационных расходов операторов.

Особенности радиоинтерфейса LTE в линии "вниз" (Downlink)

Радиоинтерфейс LTE поддерживает оба метода дуплексного разделения каналов: частотный FDD и временной TDD [2-4]. Особенностью радиоинтерфейса в линии "вниз" сети E-UTRAN является использование технологии множественного доступа OFDMA, обеспечивающей высокую гибкость распределения и масштабируемость радиоресурсов для каналов передачи данных с различной полосой пропускания. Интервал времени передачи (TTI) в линии "вниз" сети E-UTRAN соответствует длительности подкадра и равен 0,5 мс (как и для технологии HSDPA). При этом обеспечивается низкое время ожидания и высокая эффективность планирования передачи пакетов данных на радиоинтерфейсе. В линии "вниз" поддерживаются следующие виды модуляции: QPSK, 16QAM и 64QAM.

В линии "вниз" предполагается использование технологии MIMO (Multiple Input Multiple Output). Основная конфигурация технологии MIMO предполагает использование двух передающих и двух приемных антенн базовой станции и мобильного терминала. Максимально предполагается использовать четыре передающих антенны базовых станций и 2-4 приемных антенны абонентских терминалов. Технология MIMO обеспечивает передачи данных как многих (MU-MIMO), так и единственного пользователя (SU-MIMO).

Линия "вниз" E-UTRAN подразумевает использование следующих физических каналов [2]:

- PDSCH (Physical downlink shared channel) — распределенный транспортный физический канал линии "вниз";
- PDCCH (Physical downlink control channel) — физический канал управления линии "вниз";
- CCPCH (Common control physical channels) — общий физический канал управления.

Связь транспортных и физических каналов показана на рис. 1. В настоящее время в E-UTRAN для LTE определены четыре транспортных канала:

- BCH (Broadcast Channel) — вещательный канал;
- PCH (Paging Channel) — канал вызова (пейджинга);
- DL-SCH (Downlink Shared Channel) — совмещенный канал линии "вниз";
- MCH (Multicast Channel) — канал вещания в группе.

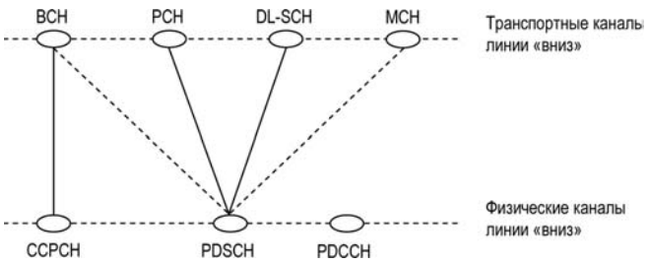


Рис. 1: Связь транспортных и физических каналов в линии "вниз" E-UTRA

Как видно из рис. 1, развитие сетей LTE направлено на максимальное, где возможно, упрощение протоколов обмена информацией. Помимо модуляции OFDM/QAM в каналах линии "вниз" сети E-UTRAN предполагается использование перспективной модуляции OFDM/OQAM.

Модуляция OFDM/QAM в линии "вниз". Технология ортогонального частотного мультиплексирования OFDM (Orthogonal Frequency Division Multiplexing) основана на формировании многочастотного сигнала, состоящего из множества поднесущих частот, отличающихся на величину $\Delta f = \frac{|\omega_n - \omega_{n-1}|}{2\pi}$, выбранную из условия ортогональности сигналов на соседних поднесущих колебаниях (ω_n — радиальная частота n-го поднесущего колебания).

При формировании OFDM-сигнала поток последовательных информационных символов длительностью T_u/N разбивается на блоки, содержащие N символов. Далее блок последовательных информационных символов преобразуется в параллельный, в котором каждый из символов соответствует определенной поднесущей многочастотного сигнала. Причем при этом длительность символов увеличивается в N раз. Таким образом, суммарная ширина спектра многочастотного сигнала соответствует ширине спектра исходного последовательного сигнала.

Целью такого преобразования является защита от узкополосных помех (либо от частичных искажений спектра в результате переотражений и многолучевого распространения). Это достигается тем, что параллельные символы многочастотного сигнала представляют собой кодовое слово помехоустойчивого кода (например, кода Рида-Соломона), который позволяет их восстановить в случае ошибочного приема за счет искажений спектра. Частотно-временное представление OFDM-сигнала представлено на рис. 2. Преобразование сигнала из временной в частотную область обеспечивается дискретным преобразованием Фурье (DFT — Discrete Fourier Transform).

Кроме того, преимущество OFDM заключается в уменьшении необходимого количества временных защитных интервалов. При последовательном сигнале защитные интервалы добавляются между каждыми символами, а при многочастотном — между группами символов (OFDM-символами).

Особенностью сигналов OFDM является:

1. Мультиплексирование несущих колебаний (называемых поднесущими), модулированных информационными символами по выбранному закону (QPSK, 16QAM, 64QAM);

2. Поднесущие ортогональны (взаимная корреляционная функция равна нулю), или, по крайней мере, квазиортогональны (на практике);

3. Каждый OFDM-символ имеет защитный временной интервал для исключения межсимвольной интерференции. Этот защитный интервал выбирается с учетом импульсной характеристики линии связи (физической среды распространения радиосигнала).

Принцип формирования OFDM-сигнала показан на рис. 3.

На практике при формировании OFDM-сигнала используется обратное дискретное быстрое преобразование Фурье (Inverse Fast Fourier Transform — IFFT) на N точек (рис. 4). Это значительно упрощает практическую реализацию приемопередающего устройства OFDM.

На рис. 4 под $a(mN + n)$ обозначен модулированный символ n-го частотного подканала длительностью T_u в интервале времени $mT_u < t < (m+1)T_u$. Вектор $\mathbf{s}_m$ на выходе IFFT представляет собой OFDM-символ. Схема формирования OFDM-символа в передатчике базовой станции сети E-UTRAN показана на рис. 5.

Схема формирования OFDM-сигналов в режиме TDD использует циклические префиксы CP (Cyclic-Prefix) для борьбы с межсимвольной интерференцией с длительностью TCP ≈4,7/16,7 мкс (при разнесении поднесущих на 15 кГц). Временные отрезки (кадры длительностью 10 мс) состоят из 20 подкадров одинаковой длительности $T_{sub\text{-}frame} = 0{,}5$ мс. Параметры сигналов OFDM линии "вниз" в режиме TDD приведены в таблице 1 [1].

Перспективная модуляция OFDM/OQAM в линии "вниз". Модуляция OFDM/OQAM, в отличие от уже ставшей традиционной модуляции OFDM, не требует наличия защитных интервалов (циклических префиксов). Квадратурная амплитудная манипуляция со сдвигом Offset QAM (OQAM) значительно повышает эффективность использования спектра за счет уменьшения интерференционных межсимвольных помех, уплотнения сигнала по времени (рис. 6).

При формировании сигнала OFDM/OQAM символы QAM (c_{mn}) разделяются на две комплексные составляющие: вещественную часть $\mathrm{Re}\{c_{mn}\} = a_{mn}$ и мнимую $\mathrm{Im}\{c_{mn}\} = b_{mn}$, причем мнимая часть сдвигается во времени на величину $T_u/2$ относительно вещественной.

Классический OFDM-сигнал записывается в виде выражения (без учета циклических префиксов):

$$s(t) = \sum_{n=-\infty}^{n=+\infty} \sum_{m=0}^{m=N_u-1} c_{mn} e^{j2\pi m \Delta f t} g(t - nT_u), \quad (1)$$

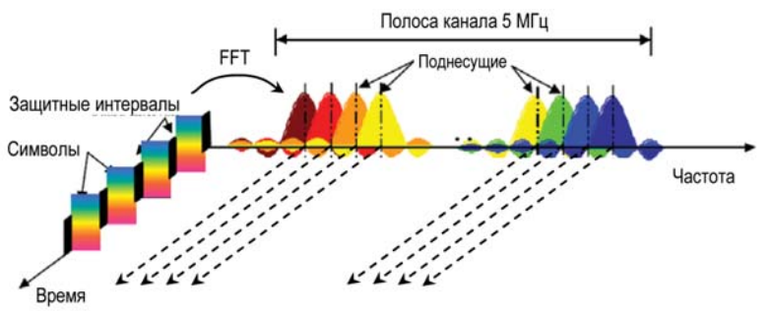


Рис. 2: Частотно-временное представление OFDM-сигнала при ширине спектра 5 МГц

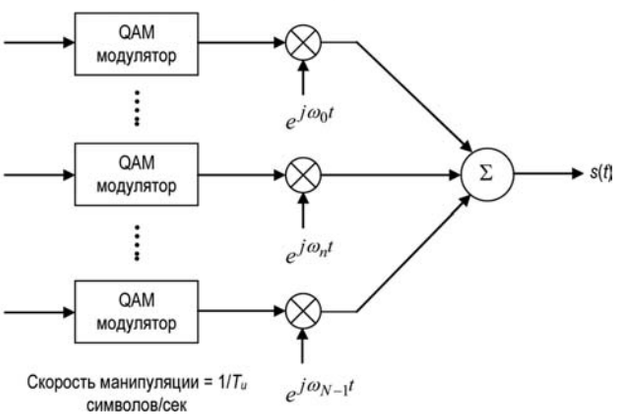


Рис. 3: Принцип формирования OFDM-сигнала

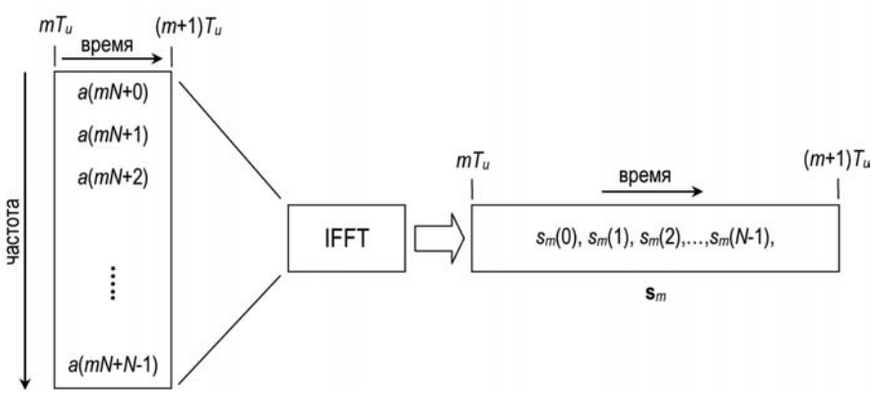


Рис. 4: Использование преобразования IFFT при формировании OFDM-сигнала

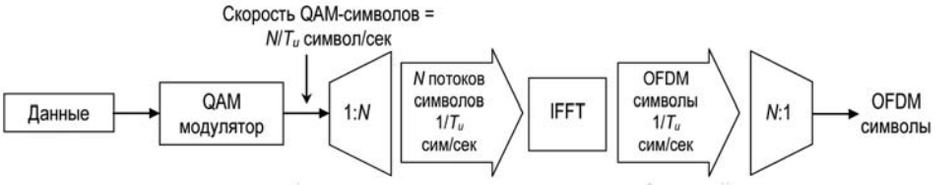


Рис. 5: Схема формирования OFDM-символа в передатчике базовой станции сети E-UTRAN

где $g(t-nT_u)=\begin{cases}1, & \text{при } nT_u<t<(n+1)T_u\\ 0, & \text{вне интервала}\end{cases}$

— прямоугольный видеоимпульс.

Формирование сигнала OFDM/OQAM при разложении cmn на комплексные составляющие может быть представлено выражением:

$$s(t)=\sum_{n=-\infty}^{n=+\infty}\sum_{m=0}^{m=N_u-1}a_{mn}j^m e^{j2\pi m\Delta f\,t}g(t-nT_u)+$$
$$+jb_{mn}j^m e^{j2\pi m\Delta f\,t}g(t+T_u/2-nT_u)=$$
$$=\sum_{n=-\infty}^{n=+\infty}\sum_{m=0}^{m=N_u-1}a_{mn}j^m e^{j2\pi m\Delta f\,t}g(t-nT_u)+$$
$$+b_{mn}j^{m+1}e^{j2\pi m\Delta f\,t}g(t+T_u/2-nT_u). \qquad (2)$$

Выражение (2) можно упростить

$$s(t)=\sum_{n}\sum_{m=0}^{N_u-1}d_{m,n}j^{m+n}e^{j2\pi m\Delta f\,t}\Im(t-n\tau_0)=$$
$$=\sum_{n}\sum_{m=0}^{N_u-1}d_{m,n}\Im_{m,n}(t),\ \tau_0=T_u/2 \qquad (3)$$

где

- $d_{m,n}=a_{m,n}$ или $b_{m,n}$ в зависимости от значения n;
- j^{m+n} определяет тип слагаемого: real (если m+n четное) или imaginer (если m+n нечетное);
- $\Im_{m,n}(t)$ — фильтрующая функция IOTA (Isotropic Orthogonal Transfer Algorithm), обеспечивающая ортогональность поднесущих в OFDM-символе, а также OFDM-символов.

Для функции $\Im_{m,n}(t)$ справедливо выражение

$$\mathrm{Re}\left\{\int_{\Re}\Im_{m,n}(t)\cdot\Im^{*}_{m',n'}(t)dt\right\}=\delta_{m,m'}\delta_{n,n'}.$$

Важным отличием OFDM/OQAM и классической OFDM является то, что скорость передачи сигнальных символов удваивается ($\tau_0=T_u/2$). Схема формирования сигнала OFDM/OQAM в передатчике базовой станции сети E-UTRAN показана на рис. 7.

В схеме, приведенной на рис. 7, модулятор генерирует N вещественных символов (real) $T_0=T_u/2$. Затем (до преобразования IFFT) они мультиплексируются с учетом составляющей j^{m+n}, которая при четном m+n является вещественной, при не четном — мнимой (при этом могут быть как положительными, так и отрицательными). На рис. 8 показана частотно-временная матрица комплексных сигналов OFDM/OQAM и OFDM/QAM.

Важным отличием OFDM/OQAM от классического сигнала OFDM является использование многофазной фильтрации (фильтрующая функция IOTA — g) после преобразования IFFT, исключающей использование циклических префиксов. Алгоритм функционирования передатчика и приемника сигналов OFDM/OQAM представлен на рис. 9.

Одним из упрощенных вариантов многофазной фильтрации (функции IOTA), обеспечивающей ортогональность сигналов, является гауссовская функция во временной и частотной области.

Благодаря функции IOTA происходит локализация спектра (получается более крутой спад по сравнению с классическим OFDM), в ре-

Таблица 1

Параметры сигнала OFDM/OQAM линии "вниз"

Параметры сигнала OFDM/OQAM линии «вниз»							
Полоса сигнала BW		1.25 МГц	2.5 МГц	5 МГц	10 МГц	15 МГц	20 МГц
Длительность подкадра		0.5 мс					
Частотное разнесение поднесущих		15 кГц					
Частота дискретизации (тактовая частота)		1.92 МГц (1/2 × 3.84 МГц)	3.84 МГц	7.68 МГц (2 × 3.84 МГц)	15.36 МГц (4 × 3.84 МГц)	23.04 МГц (6 × 3.84 МГц)	30.72 МГц (8 × 3.84 МГц)
Размер преобразования FFT		128	256	512	1024	1536	2048
Количество поднесущих		76	151	301	601	901	1201
Количество OFDM символов в подкадре (Short/Long CP)		7/6					
Длина CP (мкс/samples*)	Короткий	(4.69/9) × 6, (5.21/10) × 1*	(4.69/18) × 6, (5.21/20) × 1	(4.69/36) × 6, (5.21/40) × 1	(4.69/72) × 6, (5.21/80) × 1	(4.69/108) × 6, (5.21/120) × 1	(4.69/144) × 6, (5.21/160) ×1
	Длинный	(16.67/32)	(16.67/64)	(16.67/128)	(16.67/256)	(16.67/384)	(16.67/512)

* FFT размер = сэмпл ("samples" или выборка, для OFDM равна размеру преобразования Фурье)

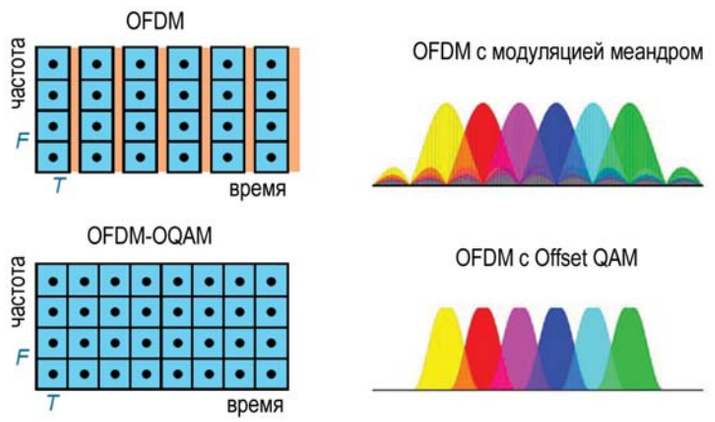


Рис. 6. Преимущество технологии OFDM/OQAM по отношению к OFDM/QAM

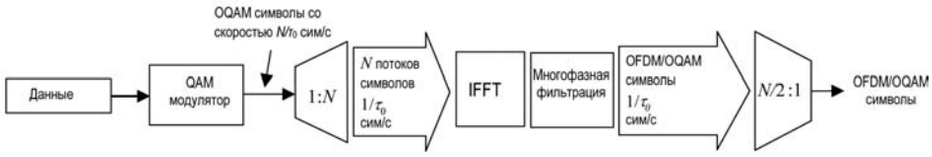


Рис. 7: Схема формирования сигнала OFDM/OQAM в передатчике базовой станции сети E-UTRAN

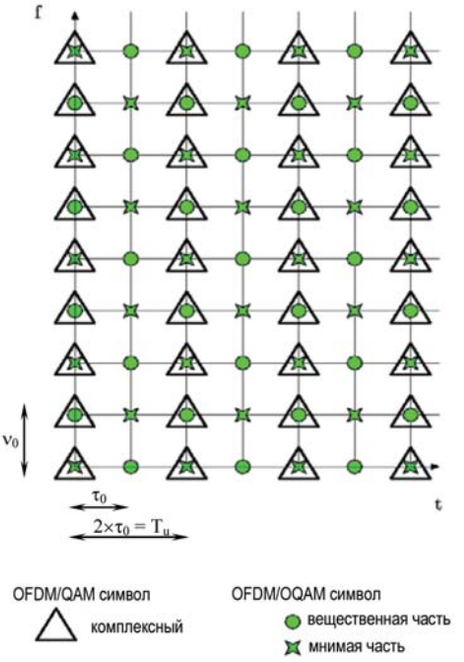


Рис. 8: Частотно-временная матрица сигналов OFDM/OQAM и OFDM/OQAM

зультате чего уменьшаются интерференционные и внутрисистемные помехи в сети. На рис. 10 приведено сравнение спектров сигналов OFDM/OQAM и OFDM с шириной спектра 5 МГц (512 точек преобразования Фурье, 300 поднесущих).

Параметры сигналов OFDM/OQAM с разнесение поднесущих на 15 кГц подобны параметрам OFDM.

Особенности радиоинтерфейса LTE в линии "вверх" (Uplink)

Особенностью линии "вниз" сети E-UTRAN является использование технологии множественного доступа SC-FDMA (Single Carrier — Frequency Division Multiple Access) с одной несущей частотой и средней мощностью передачи PAPR (Peak-to-Average Power Ratio). Исключение взаимного влияния пользователей достигается введением циклических префиксов и использованием эффективных эквалайзеров в приемных устройствах. Интервал времени передачи TTI в линии "вверх" сети E-UTRAN соответствует TTI в линии "вниз" и равен 0,5 мс. Возможно использование увеличенного TTI для специальных типов соединений (услуг). Основная конфигурация антенн линии "вверх" при использовании MIMO предполагает использование двух передающих антенн на мобильном терминале и двух приемных антенн на базовой станции.

В процессе модуляции OFDM в технологии множественного доступа SC-FDMA используется дискретное преобразование Фурье DFT (рис. 11).

При формировании группового сигнала в линии "вверх" для каждого терминала решается, какая часть поднесущих используется (заполняется данными), а какая нет (заполняется "нулями") (см. рис. 12). Между каждыми выходами дискретного Фурье вставляется L-1 нулевых символов.

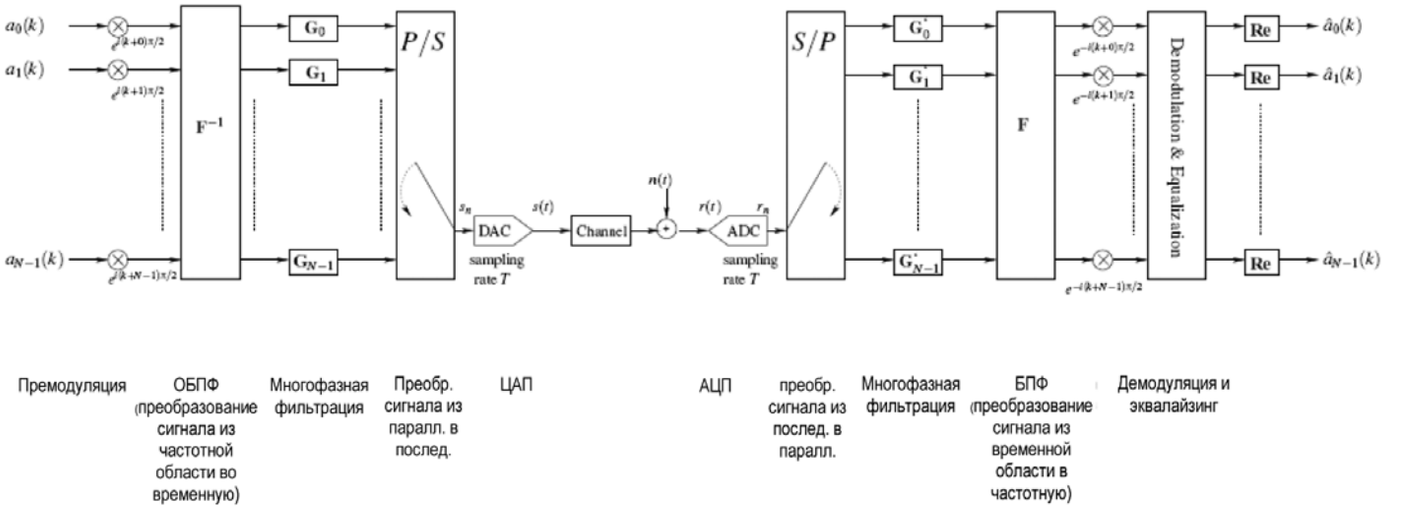


Рис. 9: Алгоритм функционирования передатчика и приемника сигналов OFDM/OQAM

При последовательном распределении поднесущих L=1 (рис. 12, слева), т. е. между сигналами с выхода преобразователя DFT не вставляются нулевые поднесущие (L-1=0). При смешанном распределении (рис. 15, справа) L>1.

Линия "вверх" E-UTRAN подразумевает использование следующих физических каналов:

• PRACH (Physical random access channel) — физический канал произвольного (случайного) доступа;

• PUCCH (Physical uplink control channel) — физический канал управления линии "вверх";

• PUSCH (Physical uplink shared channels) — физический распределенный транспортный канал линии "вверх".

Связь транспортных и физических каналов показана на рис. 13. В настоящее время в E-UTRAN для LTE определено два транспортных канала линии "верх":

• RACH (Random Access Channel) — канал случайного доступа;

• UL-SCH (Uplink Shared Channel) — распределенный канал линии "вниз".

Параметры функционирования радиоинтерфейсов LTE

Для управления качеством в сетях LTE используются два пересекающихся множества, состоящих из параметров качества функционирования сети (Network Perfomances) и параметров качества услуг (Quality of Service). Каждому соединению в сети LTE и радиоинтерфейсах E-UTRAN должно соответствовать некое множество согласованных параметров функционирования сети, связывающих воедино все аспекты QoS, такие как скорость передачи данных, задержка пакетов, джитер, относительное число ошибочно принятых пакетов и доступность сети.

Пиковая (максимальная) скорость передачи данных Peak Data Rates. Значения пиковой скорости передачи данных в линиях "вверх" и "вниз" приведены в таблице 2.

При расчетах пиковой скорости передачи данных учитывалась кадровая структура линий "вверх" и "вниз" (циклические префиксы, временные и частотные защитные интервалы, контрольные символы), виды модуляции и помехоустойчивого кодирования. Кроме того, учитывались служебные заголовки протоколов физического и канального уровней (L1/L2 — сообщения планирования передачи информации, протокола повторной передачи HARQ, сообщения AT об измеренном качестве канала CQI).

В табл. 2 приведены пиковые значения скорости передачи данных в линиях "вниз" и "вверх" в условиях благоприятной помеховой обстановки (C/I > 20 дБ), когда можно исполь-

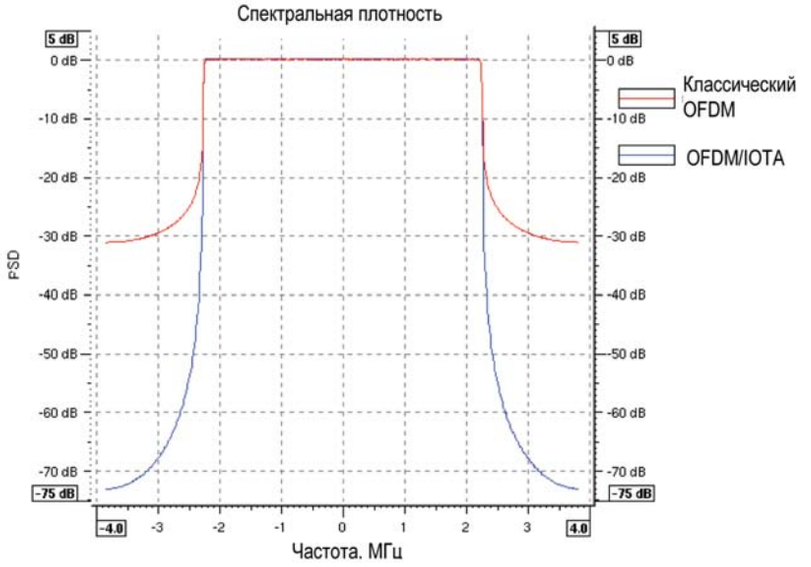


Рис. 10: Сравнение спектральных плотностей сигналов OFDM/OQAM и классического OFDM

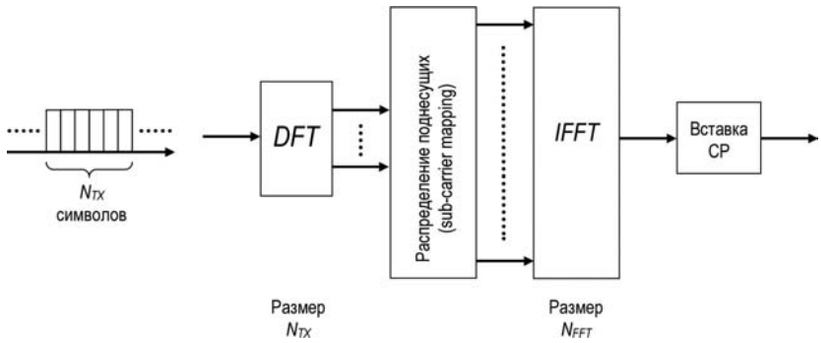


Рис. 11: Структурная схема передающего устройства при множественном доступе SC-FDMA в технологии E-UTRAN

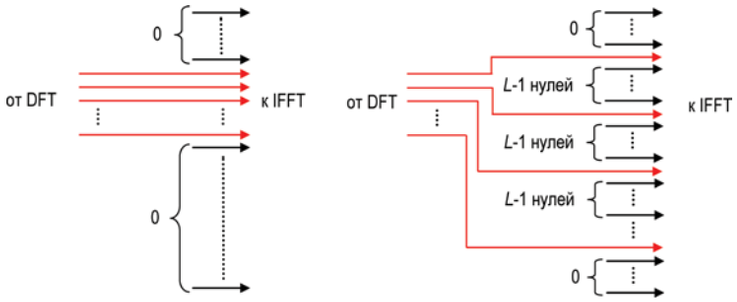


Рис. 12: Методы формирования поднесущих OFDM-сигнала: последовательный (слева) и смешанный (справа)

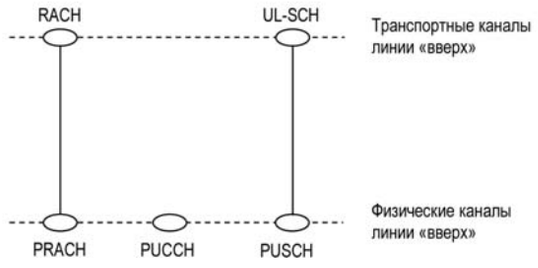


Рис. 13: Связь транспортных и физических каналов в линии "вверх" E-UTRAN

Таблица 2

Пиковая скорость передачи данных технологии E-UTRA

	Линия «вниз»		Линия «вверх»	
Условия	2 TX MIMO, 64 QAM, R=1 10 % сигнала – служебная информация		Один TX, 16QAM, R=1 14 % сигнала – служебная информация	
Единица измерения	Мбит/с в полосе 20 МГц	Бит/с/Гц	Мбит/с в полосе 20 МГц	Бит/с/Гц
Значение	100	5.0	50	2.5
С учетом служебной информации (циклических префиксов, защитных интервалов во времени и на частоте, контрольные символы)	182	9.1	57	2.9
С учетом заголовков протоколов L1/L2 и 29 % служебной информации системы	144	7.2	48	2.4

Таблица 3

Спектральная эффективность в линии "вниз"

	Абсолютное значение, Бит/с/Гц
Средняя спектральная эффективность	до 2.6 (2×2 MIMO)
Средняя спектральная эффективность на одного пользователя в соте (точка 5 % на интегральной функции распределения CDF пользовательской пропускной способности)	до 0.27

Таблица 4

Спектральная эффективность в линии "вверх"

	Абсолютное значение, Бит/с/Гц
Средняя спектральная эффективность	до 0.9
Средняя спектральная эффективность на одного пользователя в соте (точка 5 % на интегральной функции распределения CDF пользовательской пропускной способности)	до 0.15

зовать многопозиционные виды модуляции 16QAM, 64QAM. Ухудшение отношения C/I приводит к уменьшению скорости передачи (рис. 14 — для линии "вниз", 15 — для линии "вверх";).

Как показано на рис. 14 скорость передачи данных зависит от характеристик помехоустойчивости алгоритма приема и обработки сигнала. На рисунке обозначено:

- MMSE (Minimum Mean Squared Error) — линейное детектирование сигналов MIMO по критерию минимума среднеквадратической ошибки;
- QRM-MLD с использованием ASESS (Adaptive Selection of the Surviving Symbol Replica Candidates) — адаптивное нелинейное детектирование QRM (QR decomposition and the M-algorithm) сигналов MIMO по критерию максимума функционала правдоподобия MLD (Maximum Likelihood Detection).

Зная требуемое отношение сигнал/шум и мощность передачи можно определить возможные скорости передачи данных на разных удалениях от базовой станции.

Спектральная эффективность. Улучшенные параметры спектральной эффективности для E-UTRAN приведены в таблице 3 и 4 (для абонентов с низкой мобильностью и частоты радиосигнала в области 2 ГГц).

Задержки передачи пакетов для протоколов плоскости пользователя (User Plane Latency). Обеспечение низких задержек передачи данных важно для услуг в реальном масштабе времени будущих сетей сотовой связи, функционирующих по принципу коммутации пакетов (TCP/IP).

Задержки передачи пакетов для протоколов плоскости пользователя определяются как время передачи пакета данных пользователя с IP-уровня одного узла сети (мобильного терминала, шлюза GW) на IP-уровень другого узла сети. Время передачи пакетов данных пользователя с одного узла сети на другой включает различные типы задержек, приведенные в табл. 5. Средняя суммарная задержка передачи паке-

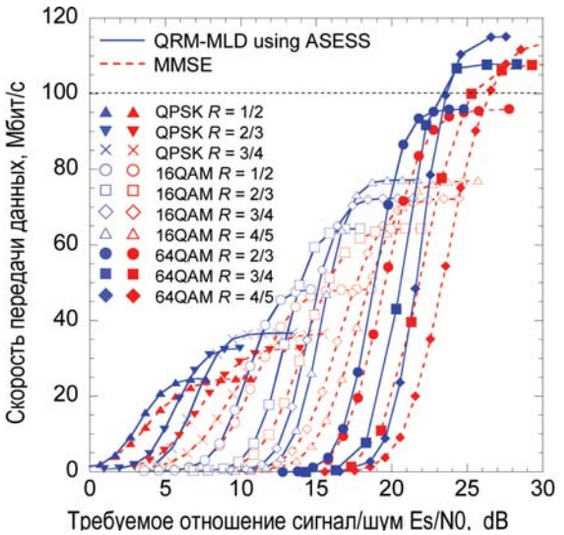


Рис. 14. Зависимость скорости передачи данных от отношения сигнал-шум в линии "вниз" (полоса сигнала 20 МГц, мобильность абонента до 3 км/ч)

Источник: ETSI

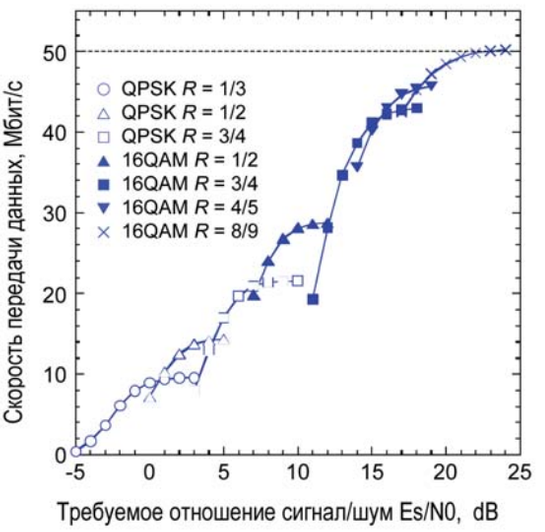


Рис. 15: Зависимость скорости передачи данных от отношения сигнал-шум в линии "вверх" (полоса сигнала 20 МГц, мобильность абонента до 3 км/ч)

Источник: ETSI

Таблица 5

Оценка задержек протоколов плоскости пользователя

Этап	Описание	Значение
0	Активизация терминала	Не учитывается
1	Время обработки задания процессором терминала	1 мс
2	Время цикловой синхронизации	0.25 мс
3	Длительность подкадра	0.5 мс
4	Задержки алгоритма ретрансляции HARQ	0.3*2.5 мс
5	Время обработки задания процессором базовой станции	1 мс
6	Время передачи пакета данных между базовой станцией и шлюзом сети GW	Ts1u (1 мс – 15 мс)
7	Время обработки задания процессором шлюза	0.5 мс
	Общая задержка	4 мс + Ts1u

тов для протоколов плоскости пользователя при передаче данных для E-UTRAN равна 4,0 мс (включая задержку передачи между базовой станцией и шлюзом сети). Возможность сокращения этой задержки до величины 1,0 мс является целью проекта создания радиоинтерфейса будущего в рамках проекта WINNER.

Временная структура сигналов E-UTRAN в режиме TDD

Во временной области физический уровень радиоинтерфейса E-UTRAN имеет кадровую структуру, состоящую из подкадров (sub-кадров) длительностью 0,5 мс. Один радиокадр содержит 20 sub-кадров. Временная кадровая структура сигналов E-UTRAN в режиме TDD приведена на рис. 16.

В режиме временного дуплекса TDD подкадры распределяются между линиями "вверх" и "вниз" с учетом различных типов пользовательского трафика. Подкадры линий "вверх" и "вниз" состоят из целого количества сигнальных символов (некоторые из которых могут использоваться для определения временных задержек распространения радиосигналов). Структура подкадров внутри кадра может изменяться от подкадра к подкадру, адаптируясь к различным профилям трафика и требованиям к задержкам.

В линии "вниз" подкадры содержат сигналы синхронизации и системную информацию. Значительное упрощение абонентского терминала достигается за счет аналогичности структур сигналов синхронизации и системной информации в различных режимах TDD и FDD.

Как видно из рис. 16 радиокадры E-UTRAN имеют одну точка переключения sub-кадров из линии "вниз" в линию "вверх" DUSP (Switching point from downlink to uplink). Различные варианты TDD в технологии, используемой в E-UTRAN, предполагают так же использование и другой точки переключения — точки переключения sub-кадров из линии "вверх" в линию "вниз" UDSP (Switching point from uplink to downlink).

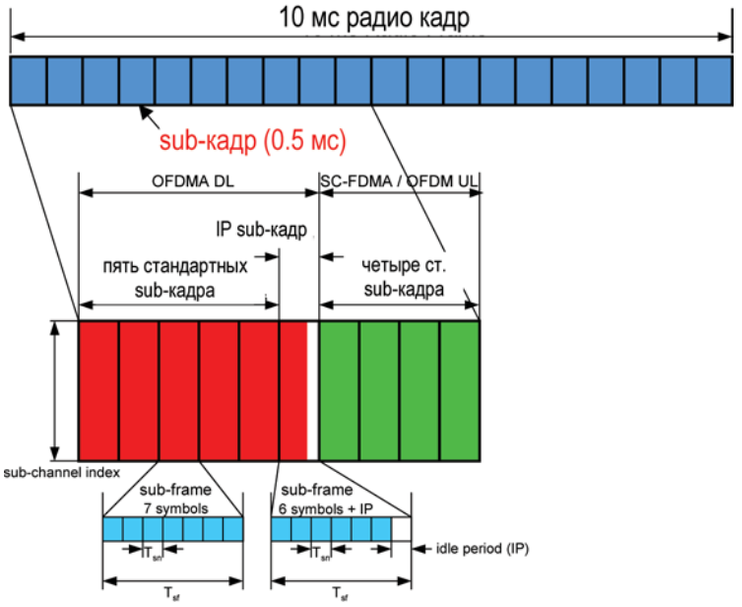


Рис. 16: Временная структура E-UTRAN в режиме TDD

Выводы

Не успев внедриться на телекоммуникационный рынок России технологии HSPA(HSDPA и HSUPA) уже морально устарели и развертывание российскими операторами сетей UMTS на основе Release 5 не спасает эти сети от неизбежной и скорой замены новой технологией LTE.

Основной проблемой при развертывании сетей на основе технологий LTE станет ее стоимость и совместимость с сетями предыдущих поколений. Переход от сетей построенных на основе технологий HSPA+ на системы LTE подразумевает под собой не усовершенствование существующей инфраструктуры сетей UMTS, а замену или ее значительной части, или всей сетевой инфраструктуры.

С другой стороны внедрение LTE позволит операторам сетей UMTS удержаться в лидерах быстроменяющегося телекоммуникационного рынка, основными тенденциями которого являются конвергенция сетей фиксированной и подвижной связи (Fixed Mobile Convergence — FMC) и персонификация услуг для абонентов(индивидуальное управление услугами).

Анализ развития технологий LTE и оценка возможности их своевременного внедрения на сетях IMT-2000/UMTS должны стать долгосрочной политикой российских операторов "большой тройки", так как разработка необходимых технических спецификаций LTE будет завершена в ETSI/3GPP к 2009 г., а к 2011-2012 годам в Европе появятся первые сети на базе технологии LTE.

Литература

1. **Тихвинский В. О., Терентьев С.В.** Управление и качество услуг в сетях GPRS/UMTS. — М.: Эко-Трендз, 2007. — 400 с.

2. **3GPP TR 25.814** Physical layer aspects for evolved Universal Terrestrial Radio Access (UTRA), Release 7, V7.1.0, 2006.

3. **3GPP TR 25.813** Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Radio interface protocol aspects, Release 7, V7.1.0, 2006.

4. **3GPP TR 25.913** Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN), Release 7, V7.3.0, 2006.

Решения Cisco Systems для роста бизнеса

В РОССИИ ВПЕРВЫЕ СОСТОЯЛСЯ "ДЕНЬ РЕШЕНИЙ CISCO ДЛЯ РОСТА БИЗНЕСА КОМПАНИЙ ФИНАНСОВОГО И ПРОМЫШЛЕННОГО СЕКТОРОВ". АКЦИЯ ТАКОГО МАСШТАБА, ОРГАНИЗОВАННАЯ ДЛЯ РУКОВОДИТЕЛЕЙ ФИНАНСОВЫХ И ПРОМЫШЛЕННЫХ СТРУКТУР РОССИИ, ПРОВОДИТСЯ ВПЕРВЫЕ.

На круглом столе-семинаре "Решения и бизнес-модели Cisco для промышленных предприятий" с докладом выступил руководитель производственного отдела Cisco Карлос А. Рохас и директор по вертикальным продажам Cisco Хью Пеглер.

Промышленные предприятия могут использовать возможности сетевой инфраструктуры Cisco для обеспечения прозрачности бизнес-процессов и увеличения своей доходности. О том, как это сделать и вместе с тем повысить качество выпускаемой продукции, участники семинара узнали из первоисточника.

"День решений Cisco для роста бизнеса компаний финансового и промышленного секторов" — еще одно свидетельство пристального интереса к российскому рынку. В недавно закончившемся 2007 финансовом году объем продаж компании здесь увеличился на 4%. Быстрее, по словам главы компании Джона Чемберса, оборот Cisco рос только в странах Ближнего Востока и Африки.

Далее представлены некоторые примеры успешного внедрения решений Cisco:

- Решения GS1 Hong Kong, Cisco и Intel по обеспечению перевозки партии телекоммуникационных продуктов VTech с использованием технологии EPC/RFID стандарта;
- Внедрение IP-телефонии в техническом центре Toyota, в азиатско-тихоокеанском регионе;
- Система беспроводной связи Cisco на стоянках Flying J;
- Точки доступа к беспроводной сети на АЗС компании Statoil;
- Внедрение корпорацией Boeing системы отслеживания местонахождения на базе WLAN для ускорения сборки самолетов;

Автоматическая идентификация продукции в режиме реального времени на основе признанного мирового стандарта

Отслеживание транспортировки телекоммуникационных продуктов компании VTech с предприятия в Донгуане (Гонконг) представляет собой составную часть проекта Hong Kong EPCnetwork, который спонсируется комиссий по инновациям и технологиям (ITC) правительства специального административного региона Гонконг в рамках схемы финансирования технического сотрудничества Гуандун-Гонконг. Цель проекта — обеспечение полной прозрачности цепочки поставок, что позволяет предприятиям региона более эффективно реагировать на запросы клиентов со всего мира.

Компании VTech является поставщиком проводных и беспроводных телефонов и электронных средств обучения. Она первой в Гонконге осуществила транспортировку своих телекоммуникационных продуктов в соответствии с правилами Wal-Mart, предусматривающими маркировку ящиков и поддонов, в которых транспортируются товары, с помощью RFID-меток (Radio Frequency Identification). Сеть EPCnetwork обеспечивает обмен данными о транспортируемых продуктах в реальном времени.

RFID-решение, включающее в себя сервисы Cisco Application Oriented Networking Services for RFID, базируется на платформах, управляемых технологиями Intel, в том числе на серверах с процессорами Intel Xeon, RFID-считывателях и ПК. Cisco также предоставила услуги по поддержке своих решений на протяжении всего жизненного цикла, в том числе по проектированию и планированию архитектуры, поддержке пилотной реализации и внедрения, т.е. методологию развертывания RFID-решения, позволяющую свести к минимуму риски и максимально повысить окупаемость.

Служба поддержки решений Cisco помогает обеспечить оптимальное использование RFID-меток при сохранении прозрачности для существующей корпоративной сети и приложений VTech во время работы системы RFID.

Благодаря финансовой и технической поддержке многие компании смогут получить выгоду от рентабельных решений и обеспечить преимущества для своего бизнеса.

Шаг вперед с помощью IP-телефонии

Совместное решение Cisco и IBM по IP-телефонии стало неотъемлемой частью новой технологии разработки продуктов компании Toyota. Технический центр Toyota в азиатско-тихоокеанском регионе (TTC-AP) создан для проектирования, научных исследований и опытно-конструкторских разработок, а также для изготовления образцов запасных частей. Поскольку к сетям компаний, занимающихся НИОКР, традиционно предъявляются более жесткие требования, чем к сетям обычных коммерческих организаций, то для выполнения повседневных операций, а также научно-исследовательских и опытно-конструкторских работ компании TTC-AP требовалась высокоэффективная и надежная сетевая платформа. В результате руководство приняло решение вложить средства в создание конвергентной сети, обеспечивающей голосовую связь в рамках единой сетевой инфраструктуры. Переход к системе IP-телефонии позволил компании сэкономить значительные средства за счет снижения совокупной стоимости владения сетевой инфраструктурой.

При проектировании и реализации данного решения для TTC-AP компания IBM Global Technology Services работала в тесном сотрудничестве с TTNI. Оказываемые услуги включали проектирование системы, консультирование, реализацию проекта, а также двухмесячное обслуживание внедренной системы на месте с целью обеспечения плавного переход к новым функциям. Решение IP-телефонии Cisco затронуло 300 пользователей, работающих в трех зданиях компании TTC-AP. В числе развернутых продуктов были следующие: коммутаторы Cisco Catalyst 4506 Series, коммутаторы Cisco Catalyst 3560 Series с питанием от сети передачи данных, приложение Cisco Call Manager, IP-телефоны Cisco 7912 и 7960. В перспективе данное решение позволит компании TTC-AP сэкономить значительные средства за счет технического обслуживания.

Система беспроводной связи Cisco — к услугам водителей на стоянках Flying J

Точки доступа Aironet 350 Series, беспроводные мосты и клиентские адаптеры Cisco стали неотъемлемой частью полностью интегрированной коммуникационной системы для водителей-дальнобойщиков. Flying J предлагает эту систему крупным операторам грузоперевозок на всей территории США под маркой CabComm.

Система CabComm с помощью спутниковых и сотовых технологий поддерживает связь водителей с операторами во время движения, а беспроводные мосты обеспечивают связь на стоянках в центрах Flying J. Помимо отправки и приема данных, сообщений голосовой почты и путевых листов, водители имеют доступ в Интернет, могут сканировать квитанцию о доставке, передавать диагностические данные, регистрировать претензии, а также принимать развлекательные видеоканалы поточного видеовещания и пользоваться телефонной связью по IP (VoIP).

Клиентские адаптеры Cisco Aironet 350 Series интегрированы в бортовой модуль CabComm каждого грузовика, а точки доступа (AP) стратегически размещены в центрах Flying J. Каждый объект оснащен 5-10 точками доступа. Точки доступа и клиентские адаптеры соответствуют требованиям стандарта IEEE 802.11b и сертифицированы на функциональную совместимость с Wi-Fi. Cisco Aironet 350 Series основана на технологии прямого расширенного спектра с прямой модуляцией в частотном диапазоне 2,4 ГГц и обеспечивает скорость 11 Мбит/с, сравнимую со скоростью передачи по проводным Ethernet-сетям и оптоволоконным кабелям.

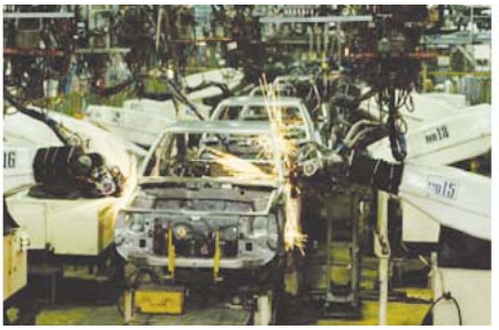
Беспроводные мосты Cisco Aironet 340 Series обеспечивают высокоскоростную связь между территориально разнесенными зданиями. Они заключены в долговечный металлический корпус и способны работать в суровом климате с широким диапазоном температур. В отличие от медных и оптоволоконных кабелей, для беспроводных мостов не являются препятствием водоемы, железные дороги и другие объекты. В планах компании Flying J — развертывание беспроводной системы приблизительно в 130 стояночно-гостиничных центрах, некоторые из которых охватывают площадь до 10 Га.

Директорные антенны на столбах с вывесками Flying J создают зону покрытия беспроводной сети для водителей и позволяют им без дополнительных манипуляций получать доступ к информации и обмениваться сообщениями. Чтобы заполнять документы, водителям совсем не обязательно находиться в центре Flying J. Сообщения и документы будут храниться в бортовой системе грузовика до прибытия в следующий центр Flying J, в котором информация будет считана и передана.

Во время стоянки грузовика в одном из 142 центров сети Flying J водитель может отправлять и принимать информацию практически в неограниченных объемах. Находясь вдали от центра можно дистанционно передавать данные через спутник или сотовую сеть. Система уже применяется в нескольких центрах Flying J.

Еще один важный фактор — средства безопасности. Cisco Aironet 350 Series поддерживает стандартную архитектуру безопасности WEP (Wired Equivalent Privacy — уровень конфиденциальности, сравнимый с проводным подключением) с длиной ключа шифрования 40 и 128 бит и централизованную инфраструктуру безопасности беспроводных локальных сетей (WLAN) по стандарту IEEE 802.1x.

Другим фактором, повлиявшим на выбор компании Flying J, является возможность питания точек доступа от линии передачи данных. Точки доступа, удаленные на значительные расстояния, могут быть запитаны через тот же кабель, по которому производится подключение к Ethernet-сети. Питание может подводиться с коммутаторов Cisco и коммуникационных панелей, предусматривающих такую возможность, или через небольшое линейное устройство, называемое инжектором питания. В результате к точкам доступа прокладывается только один медный кабель категории 5. Беспроводные мосты, как и точки доступа, получают питание для свей работы по Ethernet-кабелю.



Связь в движении

Добыча нефти в суровых условиях и розничная реализация топлива на интенсивно конкурирующих автозаправочных станциях требуют стратегического мышления и непрерывного внимания к возникающим проблемам. Розничное подразделение Statoil Detajhandel является совместным предприятием крупнейшей в Скандинавии компании по добыче нефти, сбыту и розничной реализации нефтепродуктов с участием шведской сети супермаркетов ICA. Как и другим операторам заправочных станций в разных странах, компании Statoil Detajhandel для поддержания конкурентоспособности пришлось расширить пакет розничных предложений, открыв на своих заправках минимаркеты и закусочные. Но секрет настоящего успеха кроется в дифференциации, и именно этого компания достигла с одним из самых амбициозных проектов внедрения беспроводных локальных сетей (WLAN).

Проект WLAN изначально был продиктован внутренними требованиями. Компания Statoil, эксплуатировавшая глобальную сеть на основе технологии Frame Relay, для снижения затрат и повышения эффективности наметила переход на протокол IP. В процессе модернизации предполагалось внедрить виртуальные частные сети (VPN) для объединения розничных точек Statoil Detajhandel. Эта высокозащищенная технология позволяет обмениваться конфиденциальными данными по общественным сетям, создавая в них туннели с использованием средств шифрования. VPN позволяет организовать скоростной и защищенный обмен данными с сотрудниками, которые с каждым днем становятся все более мобильными.

Одновременно изменения в европейском законодательстве о защите данных потребовали более строгого контроля за использованием и хранением данных. Новая IP-инфраструктура Statoil позволяет применять самые прогрессивные средства безопасности, сохраняя гибкость и мобильность, в которых нуждается бизнес.

Было принято решение о внедрении точек доступа к беспроводной сети Cisco Aironet 1200 Series на 300 автозаправочных станциях в Норвегии. Воспользовавшись услугами своего сервис-провайдера Telenor и технологиями Cisco, компания Statoil Detajhandel превратила автозаправочные станции в пункты беспроводного доступа. Компания сделала мощный и, на данный момент, уникальный рекламный ход для мобильного населения Норвегии. Клиентов, которым нужно заправиться бензином или дизельным топливом, обычно мало интересует владелец заправочной станции, но если АЗС предлагает бесплатный и простой доступ в Интернет — это повод остановиться и заправиться именно здесь.

Компания Statoil Detajhandel уже всерьез задумывается над возможностью реализации таких сервисов, как электронное обучение на месте, которое позволит персоналу совершенствовать свою квалификацию прямо на объектах. Также рассматривается возможность размещения плазменных экранов на площадке АЗС для трансляции рекламы, которая сможет принести дополнительный доход бизнесу.

Система отслеживания местонахождения на базе WLAN

В самом крупном здании мира может потеряться что угодно — даже двигатель суперлайнера.

Хотя такого в корпорации Boeing еще не случалось, гигант самолетостроения внедрил систему отслеживания местонахождения на основе беспроводной локальной сети (WLAN), которая позволяет постоянно следить за ценными деталями и производственным оборудованием.

На предприятии Boeing в г. Эверетт (шт. Вашингтон, США), выпускающем самолеты серий 737, 747, 767 и 777, нахождение деталей часто оказывается сложной задачей. Цех, занимающий около 40 Га и обладающий внутренним объемом 13,3 млн м3, является самым "вместительным" зданием мира по версии "Книги рекордов Гиннеса". На этом же объекте собираются суперлайнеры 787 "Dreamliner". Чтобы подготовиться к проекту 787 и ускорить производство самолетов другого типа, ИТ-подразделение Boeing начало внедрять беспроводные системы определения местонахождения. Эта технология позволит инженерам быстрее формировать и собирать наборы деталей и инструментов для самолетов, называемые "комплектами", и улучшить контроль за наличием материалов.

Идея физического отслеживания местонахождения материалов в цехе с помощью сети 802.11 была предложена собственным исследовательским подразделением PhantomWorks. Изначально предполагалось использовать существующую сеть Cisco Aironet WLAN.

Отслеживание местонахождения материалов на складе с помощью меток носит более избирательный характер по сравнению с RFID-маркировкой каждой детали вплоть до болтов и гаечных ключей. Активные метки 802.11, размером со спичечный коробок, содержат батареи и интегральные схемы и стоят от 45 до 60 долл. Метки наносятся только н те компоненты и инструменты, которые "представляют достаточную ценность, оправдывающую использование активной метки". Компания Boeing использует метки Aeroscout а также серверы и ПО этого поставщика для отслеживания местонахождения предметов по сети WLAN.

Все детали — от подъемников, кранов до реактивных двигателей и частей фюзеляжа — снабжаются метками 802.11. Эти устройства непрерывно сообщают о местонахождении предметов, к которым они прикреплены, используя одну из двух технологий: индикацию мощности принимаемого сигнала (RSSI) или расчет разности времени поступления (TDOA).

RSSI позволяет физически контролировать местонахождение объекта в пределах сети 802.11, измеряя мощность сигнала в трех точках, затем рассчитывая фактическое положение методом триангуляции. В TDOA используется аналогичный метод триангуляции метки в сети WLAN, но местонахождение определяется на основании меток времени. Сервер контроля местонахождения позволяет в реальном времени следить за текущим и прежним местонахож-

1 Основные детали самолетов, комплекты инструментов и сборочное оборудование снабжаются активными метками 802.11, которые сигнализируют о местонахождении предмета по сети WLAN.

2 Перемещение помеченного оборудования между самолетами на объекте площадью 400 000 м² отслеживается в реальном времени точками доступа Cisco Airespace, которые определяют местонахождение предмета методом триангуляции и передают эту информацию на сервер в локальной сети.

3 Благодаря тому что инженеры могут в реальном времени наблюдать за всеми основными производственными ресурсами, значительно ускоряются подготовительные операции, связанные со сборкой самолетов.

дением объекта.

Проблема с оборудованием 802.11 состоит в том, что оно предназначено для офиса, поэтому с поставщиками оговариваются условия, необходимые для работы в цехе, который из-за большого внутреннего объема больше похож на открытое уличное пространство.

Физическое расположение точек доступа в цехе достаточно тривиально: есть северная и южная стена, на каждой из них установлены точки доступа, направленные на центр цеха. До того как на WLAN были возложены функции идентификации местонахождения, инженеры с портативными и планшетными ПК использовали сет для доступа к данным из цеха. Однако покрытие площади цеха было весьма фрагментарным.

Способ расширения зоны покрытия заключается в динамической корректировке мощности и ориентации антенн точек доступа. Для контроля местонахождения в реальном времени эта процедура была сопряжена с необходимостью адаптации к существенному изменению физических условий в цехе.

Ранее, с первым поколением оборудования 802.11, требовалось приходить и пересчитывать распределение частотных каналов и мощность антенн в соответствии с текущими условиями. В данном производстве все осложняется тем, что по цеху перемещаются крупные металлические самолеты, экранирующие сигнал. Конфигурации радиоканалов приходилось непрерывно адаптировать: там , где вчера было открытое пространство, сегодня стоит 6-метровая алюминиевая стена, образующая "мертвую зону" сети WLAN. Статически настраиваемое WLANоборудование Cisco Aironet, использовавшееся ранее для доступа к данным в цехе, требовало выполняемой вручную корректировки мощности сигнала и ориентации антенн для устранения "мертвых зон", возникавших во все новых и новых местах. Корпорация Boeing преимущественно использует сети Cisco, но приняла решение искать поставщика WLAN с более гибкими возможностями.

Упрощенный протокол функционирования точек доступа (LWAPP), используемый в беспроводном оборудовании Airespace, прошел испытания в цехе в 2004 г. Это событие существенно повлияло на планы модернизации WLAN в цехе Boeing, открыв путь к более простой конфигурации. Данная технология допускает динамическую адаптацию, исключая из условий задачи все, что связано с анализом текущих условий в цехе.

После поглощения компании Airespace компанией Cisco произошло значительное усовершенствование технологий. Среди практичных нововведений — динамическая настройка мощности радиоканала, централизованные средства безопасности и управления, а также улучшение QoS и надежности.

По материалам компании Cisco Systems

Московская конференция Cisco Expo-2007

Конференция по информационным технологиям Cisco Expo-2007 прошла при участии рекордного числа IT-специалистов, аналитиков и журналистов, став самым крупным IT-событием этого года в странах СНГ. В Москве это мероприятие проводилось уже восьмой год подряд и на сей раз привлекло внимание 2016 человек, съехавшихся из 107 городов России, Азербайджана, Белоруссии, Грузии, Казахстана, Узбекистана, Украины, США, ряда стран Западной и Восточной Европы и Ближнего Востока. Среди них были жители таких отдаленных населенных пунктов РФ, как Владивосток, Находка, Хабаровск, Норильск, Южно-Сахалинск.

Московская конференция Cisco Expo-2007 привлекла внимание представителей различных секторов экономики. Большинство из них, естественно, представляли телекоммуникационные и IT- компании (на их долю пришлось, соответственно, 29 и 26% участников). Кроме того, на форуме побывали специалисты промышленного и финансового секторов (12 и 8%, соответственно) и таких отраслей, как образование, здравоохранение, транспорт, органы государственного управления. Среди представителей бизнеса 59% составили сотрудники малых и средних предприятий.

Московская конференция Cisco Expo-2007 была посвящена инновационным разработкам Cisco в области сетевых технологий. На правах главных спонсоров конференцию открыли представители компаний PANDUIT, Emerson и "АМТ-ГРУП". Вслед за ними с ключевым докладом "Информационные технологии и мы. Взгляд в будущее" выступил руководитель департамента вертикальных продаж Cisco Марк Миллер. Завершил пленарную часть руководитель департамента инженерных систем Cisco Аксель Клауберг, который представил вниманию слушателей доклад "Технологии, которые изменят мир". Дальнейшая работа конференции проходила по четырем техническим потокам:

— маршрутизация и коммутация (Routing&Switching);
— безопасность (Security);
— унифицированные коммуникации (Unified Communications);
— центры обработки данных (Data Centers)

Были организованы специальные сессии по решениям для операторов связи, технологиям построения беспроводных сетей, оптическим решениям, сервисным программам Cisco, вопросам организации сетевой инфраструктуры и образовательным программам Cisco.

Небывалому успеху московской Cisco Expo-2007, безусловно, способствовала поддержка лидеров мировой и отечественной IT-индустрии. Золотым спонсором форума стала компания PANDUIT, серебряным — Emerson Network Power, бронзовым — "АМТ-ГРУП", технологическим спонсором — EMC, специальными спонсорами — компании "Би-Эй-Си" и OCS.

Беспрецедентный интерес к конференции Cisco Expo-2007 проявили и средства массовой информации. Достаточно сказать, что работу форума освещали более ста журналистов.

В течение всех трех дней работы Cisco Expo-2007 в фойе отеля "Рэдиссон САС Славянская" проходила выставка технологий, в которой приняли участие компания Cisco и партнеры конференции.

Фильтрация трафика пользователей как новая услуга ISP

Владимир Бычек,
руководитель направления контентной фильтрации (eSafe) компании Aladdin

Предпосылки появления

Тенденция к непрерывному уменьшению стоимости Интернет-трафика стала причиной увеличения количества пользователей Интернет, приобретающих подписку на безлимитные тарифы доступа к всемирной паутине. В свою очередь, получив неограниченный доступ, среднестатистический пользователь стал чувствовать себя в Интернете гораздо спокойнее и увереннее. География web-серфинга значительно расширилась, многие открыли для себя прелести потокового видео (самого разнообразного содержания), файлообменных сетей, блогов, недорогих и качественных сервисов связи, услуг Интернет-расчетов, публичной почты и пр. При этом упомянутый среднестатистический пользователь, как правило, совершенно не подготовлен к тем неприятностям, которые являются обратной стороной удобства и доступности. А именно сетевым червям, троянам, разнообразному шпионскому программному обеспечению — всему тому, что мы называем вредоносным кодом. На широкополосном доступе заражение происходит практически моментально и последствия его могут быть самыми печальными, в частности, к ним относятся:

- выход компьютера из строя или значительное замедление его работы;
- вынужденное блокирование адреса компьютера пользователя со стороны оператора в случае, если бот, установленный на компьютере, начинает массовую рассылку спама или включается в DDos атаку (некоторые операторы могут в ряде случаев отслеживать подобную активность);
- потеря персональной информации (номеров кредитных карт, например) и др.

Как правило, инфицирование компьютеров происходит при посещении сайтов сомнительного содержания (чаще всего порно, warez и др.) и это тоже проблема, поскольку подавляющее большинство родителей все еще озабочены воспитанием своих детей и хотели бы оградить их от так называемого нежелательного контента, которого в Интернет, к сожалению, предостаточно. Для оператора заражение компьютеров пользователей вредоносным кодом, особенно принимающее массовый характер, также факт весьма неприятный. Пользователь, получивший "сюрприз" из сети Интернет, склонен винить в этом оператора (и не без оснований, замечу). Он требует, как правило, немедленного принятия мер, "нагружая" службу технической поддержки. Не получив должной помощи, пользователь может в большинстве случаев без проблем уйти к другому оператору, благо предложений предостаточно.

Долгое время эта горькая пилюля для оператора в изрядной степени подслащивалась тем, что пользователь оплачивал весь трафик — и свой, и паразитный (являющийся прямым следствием активности вредоносного ПО). Сегодня в силу указанных выше причин, таких пользователей все меньше. Те же пользователи, которые вынуждены использовать тарифы с предоплаченным трафиком по причине отсутствия вблизи их офисов операторов, обеспечивающих подключение по проводу (например, спутниковый Интернет, либо Интернет по GPRS или CDMA), не очень спешат оплачивать паразитный трафик в силу относительно высокой стоимости мегабайта и в ряде случаев предпочитают судиться с оператором с очень высокой вероятностью выиграть процесс.

Что делать

Для многих ответ очевиден — воспользоваться одним из персональных средств защиты, широко представленных на отечественном рынке. Действительно, правильно установленный и сконфигурированный персональный комплект программного обеспечения, включающий в себя антивирус, средство борьбы со шпионским ПО и руткитами, антиспам, персональный межсетевой экран и средство обеспечения "родительского контроля" в состоянии надежно защитить компьютер пользователя от всех современных угроз. Но только при выполнении нескольких "простых" условий:

• пользователь обладает нужными знаниями и квалификацией для того, чтобы аккуратно и вдумчиво выполнить все необходимые настройки;

• пользователь аккуратно и непрерывно будет поддерживать актуальность всех баз, необходимых для работы комплекта средств защиты;

• пользователь будет тщательно разбираться с каждым запросом межсетевого экрана и, возможно, других компонентов комплекта средств защиты, и только после этого запрещать или разрешать соединение, инициированное его компьютером или какое либо действие средства защиты;

• пользователь с пониманием отнесется к временным задержкам, во время которых средства защиты из комплекта будут выполнять свою работу.

Много ли найдется таких пользователей? Полагаю — нет. При этом комплект персональных средств защиты стоит денег, и денег относительно немалых.

Должен быть другой способ, максимально прозрачный для пользователя и при этом обеспечивающий максимально надежную защиту. И такой способ есть. Он заключается в том, что защиту пользователя от угроз Интернет берет на себя оператор, обеспечивающих услугу подключения. Берет, разумеется, не бесплатно, но при этом в выигрыше оказываются все. Пользователь получает реальную защиту, которая при этом его не обременяет, а оператор увеличивает ARPU за счет предоставления новой услуги, кстати сказать, весьма востребованной на Западе.

Проблемы и решения

После того, как мы определились с вопросом "что делать", пришло время разобраться с вопросами какими средствами и каким образом. Далеко не все контентные фильтры, представленные на рынке, обладают достаточной функциональностью, производительностью и масштабируемостью для того, чтобы дать оператору решение, опираясь на которое он сможет предоставить пользователям востребованные слуги очистки почтового и web-трафика от вредоносного кода и спама, а также обеспечить "родительский контроль" с использованием URL-фильтрации Причем, если URL-фильтрацию на объемах трафика оператора способны предложить несколько вендоров, то качественную очистку веб-трафика от вредоносного кода, пожалуй, только Aladdin с его семейством продуктов eSafe.

Определившись с продуктом, и опираясь на богатый опыт вендора в реализации услуг очистки трафика для пользователей мы, казалось бы, могли бы легко применить этот опыт в России и в кратчайший срок внедрить ее у всех операторов, благо маркетинговых схем взаимодействия с оператором предостаточно. К сожалению, специфика работы отечественных провайдеров категорически не позволяет сделать это. А заключается она, прежде всего, в том, что в отличие от своих зарубежных коллег, большинство наших операторов поддерживают собственную локальную сеть с огромным количеством внутренних ресурсов (FTP-серверов, чатов, P2P и пр.) которые либо контролируются очень слабо, либо не контролируются вовсе. Поэтому концентрация вредоносного и нежелательного контента в этих сетях часто повыше, чем в среднем по Интернет. Интересный факт: как правило, доступ в локальную сеть предоставляется оператором бесплатно всем подписчикам на услугу доступа в Интернет вне зависимости от тарифного плана. Поэтому существует достаточно многочисленная группа пользователей, которые приобретают минимальный пакет услуг и практически не выходят в Интернет, довольствуясь контентом локальной сети оператора.

Вторая, более сложная проблема, заключается в интеграции решения в систему управления сетевыми ресурсами или OSS (Operations Support Systems) оператора. Несмотря на то, что опорные сети операторов построены более или менее одинаково и то, что спектр используемого оборудования также не особенно широк (в основном, Juniper и Cisco), OSS системы операторов сильно разнятся. Поэтому говорить о какой-либо унификации сейчас и в близком будущем, к сожалению, не приходится. Таким образом, на сегодняшний день не представляется возможным разработать универсальный программный модуль, который имел бы все необходимые интерфейсы для связи с подсистемами заказа услуги очистки трафика, ее активации, системой сетевого управления, билинга и т. д. Это означает, что возможность использования имеющихся наработок ограничивается общими схемами имплементации, интеграцию же в OSS оператора каждый раз приходится практически делать с нуля. Это непростая задача, требующая привлечения серьезных ресурсов. В своей практике мы предпочитаем передавать эту работу компаниям-партнерам, специализирующимся, в том числе на разработке OSS, например, компании NVision Group.

Как это может выглядеть

Со стороны подписчика услуги доступа в Интернет активация услуги очистки трафика и родительского контроля в самом общем виде выглядит следующим образом:

• после аутентификации в личном кабинете пользователь оказывается в окне активации сервиса, где имеет возможность выбрать из нескольких политик, в соответствии с которыми будет обрабатываться его трафик. Например:

— фильтрация трафика от вредоносного кода (вирусы, трояны, черви, spyware и т. д.);

— блокирование сайтов с нежелательным контентом (порно, насилие, наркотики);

— комбинация двух предыдущих;

• в зависимости от эксплуатируемой OSS, активация услуги и списывание средств с баланса подписчика происходит немедленно, либо в начале следующего месяца, либо как-нибудь еще.

В процессе работы над проектами нескольких отечественных провайдеров было отмечено еще одно существенное отличие отечественного рынка. У зарубежных операторов услуга очистки трафика слабо кастомизирована и при этом очень востребована. Речь идет о том, что трафик подписчика услуги очистки трафика и/или родительского контроля обрабатывается всегда в соответствии с одной и той же политикой. Это значит, что и дети и их родители при работе с Интернет будут подвержены одним и тем же ограничениям.

По прогнозам служб маркетинга операторов, с которыми мы в настоящее время работаем над проектами внедрения услуги очистки трафика, в России потребуется более серьезная проработка вопроса. Предоставляя услугу очистки трафика от вредоносного и нежелательного контента мы должны будем дать оператору возможность сильно кастомизировать услугу. То есть предложить пользователю несколько политик для обработки его трафика. На практике это будет означать, что в рамках одной семьи родители смогут, например, посещать сайты всех категорий без ограничений, а дети не смогут попасть на сайты из категорий эротики, насилия, азартных игр и др.

Подобная кастомизация выглядит привлекательной, но сильно усложняет интеграцию услуги в OSS оператора. При этом она потребует от пользователя более серьезного участия в процессе активации услуги. Ему придется вначале создать несколько бюджетов с соответствующими логинами и паролями (для членов семьи), а затем к каждому из них привязать соответствующую политику.

В каком виде услуга окажется более востребованной и в какой мере отечественный рынок действительно готов ее принять покажет пилотный проект на одном из крупных операторов Москвы, который будет запущен в ближайшее время.

Результатам этого эксперимента будет посвящена отдельная статья.

VIII Международный авиационно-космический салон МАКС-2007

С 21 по 26 августа 2007 г. на территории Государственного научного центра "Летно-исследовательский институт им. М.М. Громова" в г. Жуковском прошел VIII Международный авиационно-космический салон МАКС-2007.

Анонс МАКС-2007 с официальными статистическими данными был опубликован в предыдущем номере журнала.

В Авиасалоне приняли участие все основные мировые производители авиационной техники. Важнейшим отличием МАКС-2007 от предыдущих международных выставок явилось проведение международных научных конференций, семинаров и "круглых столов" с участием ведущих отечественных и зарубежных ученых, конструкторов и инженеров по важнейшим направлениям развития авиационной науки и техники.

В летной программе, помимо самолетов ведущих авиационных компаний и фирм, приняли участие широко известные в мире пилотажные группы: "Русские витязи", "Стрижи", "Патруль де Франс".

Международный авиационно-космический салон был открыт 21 августа в торжественной обстановке при участии Президента Российской Федерации В.В. Путина, который в приветствии участникам Авиасалона подчеркнул, что МАКС обещает стать крупнейшим форумом делового партнерства в сфере авиации и космоса.

В работе МАКС-2007 приняли активное участие члены Правительства Российской Федерации, руководители федеральных министерств, служб, агентств и ведомств, печати, телевидения, радиовещания, генеральные и главные конструкторы авиационной и космической техники, руководители интегрированных структур, НИИ, ОКБ, заводов и руководители ведомств российских регионов, а также многочисленные официальные делегации из зарубежных стран. На авиасалоне был проведен ряд тематических дней: Москвы, Самарской области, Пермского края, Российской авиационной науки, ОАО "Туполев", Парламентский день и др.

Существенно расширилось иностранное участие. В авиасалоне участвовало 247 зарубежных компаний (79 из них — впервые). Значительно возросло число национальных экспозиций. Посетители могли увидеть экспозиции Германии (25 компаний), Франции (22 компании), США (13 компаний), Китая (14 компаний), Бельгии (17 компаний), Украины (15 компаний) и Чехии (8 компаний).

Первые четыре дня Авиасалона были посвящены деловой части, в ходе которой было проведено более 300 бизнес-встреч, включающих подписание контрактов, опционов, соглашений и протоколов о намерениях. Общая сумма подписанных соглашений превысила 75 млрд руб.

В рамках выставки была организована космическая экспозиция под эгидой Федерального космического агентства (**Роскосмос**), в которой принял участие лидер российского космического приборостроения — Федеральное государственное унитарное предприятие "Российский научно-исследовательский институт космического приборостроения" (**ФГУП "РНИИ КП"**).

Посетители авиасалона ознакомились с деятельностью предприятия по созданию, развитию и модернизации глобальной навигационной системы ГЛОНАСС, возможностям отечественной системы навигации, функциональным дополнениям, образцам навигационной аппаратуры.

ФГУП "РНИИ КП" представило на выставке спутниковую систему — КОСПАС-SARSAT. За четверть века ее существования удалось спасти 20,5 тыс. человек. На стенде института специалисты представили различные типы аварийно-спасательного оборудования не только для крупных транспортных компа-

ний, но и для индивидуального пользования.

Огромные возможности, которые открывают спутниковые системы дистанционного зондирования Земли перед государственными организациями и бизнесом, были представлены отдельным разделом. На снимках из космоса, сделанных при помощи спутника "Ресурс ДК", посетители МАКСа увидели египетские пирамиды, московский Кремль и римский Колизей. Впервые ФГУП "РНИИ КП" предоставил возможность всем желающим воспользоваться информационной стойкой с жидкокристаллическим дисплеем.

Современные спутниковые технологии, совмещенные с новейшими выставочными достижениями, позволяют окунуться в удивительным мир космических просторов, совершить виртуальный полет к звездам, получить информацию о возможностях спутниковой навигации, технических новинках и особенностях производства сложнейшей техники.

На открытой площадке перед павильоном Роскосмоса была развернута экспозиция специальной автомобильной техники. Специалисты ознакомились с возможностями современной модели мобильного геодезического комплекса "Пионер" на базе отечественного автомобиля "УАЗ-452", а также с машиной авиационно-космического поиска и спасания фирмы "Дженерал Телеком" на базе внедорожника "Hummer".

Железногорское НПО прикладной механики (НПО ПМ) впервые представило на авиакосмическом салоне в Жуковском полномасштабный проект нового спутника "ГЛОНАСС-К" для российской глобальной навигационной системы. Первый из них отправится на орбиту в 2009 г. и заменит аппараты более ранних модификаций, "ГЛОНАСС-М".

Новые спутники будут вдвое легче, чем "ГЛОНАСС-М" (850 вместо 1415 кг), срок их активного существования составит более 10 лет. Это позволит запускать их менее мощными и более дешевыми ракетоносителями. Сейчас для запуска "ГЛОНАСС-М" используется стартующий с космодрома Байконур "Протон-К". Два спутника серии "К" сможет выводить на орбиту втрое более легкий "Союз-2". Причем запуски "ГЛОНАС-К" будут производиться с российского космодрома Плесецк в Архангельской области. Из-за большого срока службы частота запусков и стоимость поддержания систем ГЛОНАСС будет снижена.

Группа компаний Thales представила на московском авиасалоне свои телекоммуникационные решения в отраслях гражданской авиации. Thales разработала TopFlight, центр спутниковой связи, в соответствии с запросами рынка для представления новой широкодиапазонной услуги Инмарсат Свифт. Эта услуга позволит изменить уровень связи, доступный пассажирам для использования мобильного телефона, и обеспечить Wi-Fi-доступ для IP-телефонии или работу с данными.

Центр спутниковой связи TopFlight является первой ARINC 781 системой спутниковой связи, позволяющей во много раз увеличить возможности, являясь более компактной, чем предыдущее поколение оборудования SATCOM: она совместима с новым поколением компактных антенн ARINC-781 и с предыдущим поколением антенн ФКШТС-741.

Использование связи включает:

— обеспечение улучшенной рабочей среды с широкополосным доступом к глобальным сетям и расширенной связью для мобильных и стационарных телефонов, включая теле- и видеоконференции.

— обеспечение дополнительного дохода для авиалиний, благодаря использованию пассажирами электронных устройств на борту самолета для голосовых звонков, отправки сообщений или операций с данными.

— увеличение возможностей бортовых систем развлечений в процессе полета для обеспечения возможностей покупки, загрузки и связи.

— поддержка эффективности авиалиний посредством установления надежной связи между системами самолета и наземной инфраструктурой.

ОАО "МКБ "Компас" представило на международном авиакосмическом салоне одну из своих последних новинок — носимый приемо-индикатор спутниковых навигационных систем ГЛОНАСС и GPS (в недалеком будущем он сможет подключаться к европейской системе GALILEO). Этот "карманный" навигатор, ничем не уступающий в функциональности и удобстве лучшим зарубежным образцам, обладает очень высокой надежностью и точностью, так как изначально разрабатывался для вооруженных сил России.

К его достоинствам, кроме эксплуатационной надежности и точности позиционирования, благодаря использованию электронных карт Генерального штаба, можно отнести уникально стабильное ПО, разработанное МКБ "Компас", а также высочайшую помехоустойчивость.

Накануне авиасалона МКБ "Компас" выиграло тендерный контракт с РАО "РЖД" на поставку системы контроля за движением поездов. Одним из определяющих факторов стало использование отечественных оборонных технологий и системы позиционирования ГЛОНАСС, что гарантирует государственный контроль за деятельностью стратегически важной железнодорожной отрасли. Комиссия также сочла уникальное программное обеспечение системы более надежным и удобным в эксплуатации.

В авиасалоне приняло участие также и **ОАО "Объединенная авиастроительная корпорация" (ОАК)**, образованное Указом Президента РФ от 20 февраля 2006 г. и зарегистрированное в ноябре того же года с уставным капиталом 96,7 млрд руб. Глобальная цель корпорации — сохранение и укрепление позиций России в качестве одного из центров мирового авиастроения. Доля государства в Обществе составляет 90,1%.

Основным элементом организационной структуры ОАК является переход от существующей структуры управления, где каждая компания — центр прибыли, обеспечивающий полный набор бизнес-компетенций, к структуре, основанной на концепции продуктовых бизнес-единиц. Обеспечение такого перехода подразумевает, во первых, формирование и развитие Корпорации в качестве центра капитализации. Во-вторых, преобразование организационно-правовых форм и корпоративных механизмов управления компаниями, вошедшими в состав ОАК. В-третьих, внедрение стандартов корпоративного управления, учета, и уровня раскрытия информации, необходимых для эффективного привлечения инвесторов и превращения ОАК в публичную компанию. Три бизнес-единицы, которые составляют новую концепцию управления, обеспечат ведение деятельности по основным продуктовым направлениям: военной, гражданской и транспортной авиации. Процесс организационных преобразований должен быть реализован поэтапно в течение 2007-2010 гг.

Педставители компании **"Боинг"** и авиакомпании "Атлант-Союз" в рамках московского авиасалона объявили о том что российская авиакомпания разместила заказ на четыре самолета Боинг 737-700 Next Generation. Стоимость заказа составляет 249 млн долл.

Авиакомпания "Атлант-Союз" является одним из крупнейших чартерных перевозчиков России. В настоящий момент она активно развивает внутренние и международные регулярные перевозки. Базовым аэропортом авиакомпании является Международный аэропорт Внуково. Недавно в состав парка "Атлант-союз" вошли два лайнера Боинг 737 Classic, взятые авиакомпанией в лизинг. Авиакомпания является также официальным перевозчиком Правительства Москвы. К настоящему моменту более 100 авиакомпаний разместили заказы на более 4000 самолетов Боинг Next-Generation.

По словам председателя Совета директоров группы компаний **"Авгуръ-РосАэроСистемы"** Геннадия Вербы, для всей воздухоплавательной общественности этот МАКС стал историческим, на нем впервые был представлен газовый десятиместный дирижабль AU-30 объемом 5 000 м^3. С его появлением Россия встала в ряд ведущих воздухоплавательных держав мира, наряду с США и Германией.

Аппарат AU-30 находится в ряду наиболее современных, оснащенных по последнему слову техники, произведенных из новейших материалов и по самым передовым технологиям. Создателя дирижабля — группу компаний "Авгуръ-РосАэроСистемы" — можно считать не только безусловным лидером отечественного дирижаблестроения, но и одним из крупнейших в мире производителем воздухоплавательной техники, среди таких как Zeppelin Luftschifftechnik GmbH (Германия), TCOM LLC, WorldWide Aeros Corp и American Blimp Corp (США).

Появление этого изделия на отечественном и мировом рынке дает новые возможности по аэрофотосъемке, геологическим изысканиям, экологическому мониторингу, а также элитному туризму и рекламе. Первые два аппарата AU-30 уже в 2007 г. начнут эксплуатироваться ЗАО "АэроСкан" в целях детальной аэрофотосъемки линий электропередач, нефтегазопроводов, дорог и других инфраструктурных объектов. Завершено строительство третьего дирижабля AU-30, который примет участие в международной полярной научно-исследовательской экспедиции для измерения толщин арктических льдов.

В результате успешных демонстрационных полетов на МАКС-2007 дирижабля AU-30, которые стали возможны при содействии ФГУП "Рособоронэкспорт", интерес отечественных и зарубежных потребителей этого дирижабля возрос.

На дирижабле AU-30 установлено два независимых аэросъемочных комплекса — для плановой и детальной аэросъемки. Комплекс плановой съемки, включающий в свой состав авиационный лазерный сканер, цифровую тепловизионную, ультрафиолетовую камеры и радиочастотный регистратор, устанавливается на специальную подвижную раму-платформу, обеспечивающую автоматическую компенсацию угла сноса летательного аппарата. Комплекс детальной съемки включает в свой состав лазерный дальномер, цифровую фотокамеру с длиннофокусным объективом и обзорную видеокамеру. Эта аппаратура размещена в управляемой гиростабилизированной авиационной головке.

По своей представительности и демонстрации авиационной и космической техники МАКС-2007 превзошел все предыдущие выставки МАКС и утвердился в позиции одного из мировых лидеров.

VII международная выставка-форум "Инфокоммуникации России — XXI век"

ИнфоКом — крупнейшее событие российской отрасли инфокоммуникационных технологий, на котором демонстрируются последние достижения отечественной ИКТ-индустрии.

Технологии для всех — так звучит основная тема выставки. Главный ее акцент — практическое применение инфокоммуникационных разработок, которые помогают улучшать качество жизни во всех сферах деятельности.

В рамках **Деловой программы** прошли традиционные конференции и семинары, ежегодно проводимые на площадках ИнфоКома и принципиально новые мероприятия, посвященные актуальным вопросам отрасли.

Среди наиболее ярких событий для гостей Инфокома следует отметить: семинары и мастер-классы на площадке "Школа технологий"; акция "День Интернета"; Ярмарка вакансий; Обучающая площадка infoLinux; традиционный Молодежный фестиваль "Цифровой мир"; День детского Интернета.

В этом году в связи получением г. Сочи статуса столицы Зимних Олимпийских игр 2014 г. регионом-партнером выставки выбран Краснодарский край. Официальные мероприятия форума прошли одновременно в Москве и Краснодаре, во время церемонии открытия между этими городами была организована видеосвязь.

Ключевой теме выставки "Технологии для всех" посвящена специальная экспозиция, подготовленная Министерством информационных технологий и связи РФ. На стенде продемонстрированы новые возможности применения современных информационных технологий и средств связи в государственном и бизнес-управлении, социальной сфере, образовании, культуре и других областях повседневной жизни. В рамках стенда "Технологии для всех" были представлены проекты и решения по следующим направлениям:

"ИКТ в социально-экономической сфере" — комплексная демонстрация возможностей использования ИКТ в образовательном процессе.

"ИКТ в государственном управлении" — демонстрация решений, направленных на повышение качества и эффективности государственного управления на основе организации межведомственного информационного обмена, а также повышение оперативности предоставления государственных услуг, требующих межведомственного взаимодействия.

"ИКТ в сфере культуры" — демонстрация современных сквозных технологий переноса больших и сверхбольших информационных ресурсов сферы культуры с традиционных носителей (бумага, фото, микроформы и др.) в машинообрабатываемый вид с последующим предоставлением возможности широкого доступа общественности к национальному культурному и интеллектуальному достоянию.

"Поддержка отрасли" — представление концепции и проектов реализации государственной программы создания в России технопарков в сфере высоких технологий, организационно-правовая схема управления проектом, проекты строительства и земельных участков.

В марте 2006 г. Правительство РФ одобрило разработанную Мининформсвязи России государственную программу "Создание в Российской Федерации технопарков в сфере высоких технологий", основными задачами которой являются:

— повышение инвестиционной привлекательности высокотехнологичных отраслей экономики, обеспечение увеличения объемов иностранных инвестиций;

— создание условий для размещения международными высокотехнологичными компаниями своих производств на территории РФ;

— увеличение объема экспорта высоктехнологичной продукции и услуг, производимых российскими предприятиями в сфере высоких технологий.

Функции по обеспечению координации работы по реализации государственной программы на межведомственном уровне, а также по планированию бюджетных средств были возложены Правительством РФ на Мининформсвязи России.

В соответствии с государственной программой в 2006-2010 гг. технопарки в сфере высоких технологий создаются на территориях Москвской, Новосибирской, Нижегородской, Калужской, Тюменской областей, Республики Татарстан и г. Санкт-Петербурга.

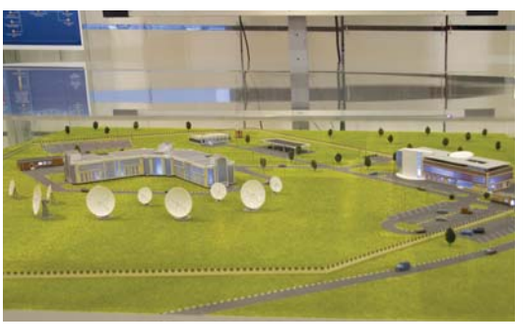
"ИКТ для Олимпийских игр в Сочи-2014" — основные направления развития инфраструктуры связи, необходимой для организации и проведения Олимпийских игр в 2014 г. в Сочи. На стенде размещена информация о планах, сроках реализации и основных показателях работ по созданию современной инфокоммуникационной инфраструктуры г. Сочи и прилегающих территорий.

"Развитие инноваций" — привлечение общественного внимания (в том числе потенциальных инвесторов и партнеров) к перспективным инновационным проектам в области высоких технологий, их популяризация и продвижение на рынок.

Ведущие отечественные и зарубежные компании, работающие на российском рынке, представили свои новейшие продукты.

ОАО "Мобильные ТелеСистемы" продемонстрировало ряд комплексных решений для бизнеса и развлечений:

- "МТС Коннект" — мобильный доступ к сети Интернет и корпоративным ресурсам с ноутбука и стационарного компьютера, работающий в стандарте GSM и в сетях 3G;
- "Office online+" — решение, позволяющее синхронизировать корпоративный почтовый сервер с мобильными устройствами абонентов;
- "Почт@онлайн" — решение, позволяющее получать доступ к корпоративной электронной почте с любой модели мобильного телефона;
- FMC (Fixed-Mobile Convergence) позволяет объединить фиксированные и мобильные телефоны корпоративных абонентов в целостную сеть с единым планом нумерации;
- Деловой портал wap.mtsbiz.ru в рамках WAP-портала МТС — деловые новости от информационных агентств и ежедневных изданий.



Специальный стенд ***Cisco Systems*** посвящен цифровизации сети общего пользования и переходу на IP NGN на базе решений Cisco. В рамках работы выставки представлены решения Cisco в области: IPTV; Wi-Fi Mesh и WiMAX-доступа; информационной безопасности сетей операторов связи и центров хранения данных; мобильных телекоммуникаций.

Специалисты по обслуживанию интеллектуальных систем могут осуществлять их диагностику по сети и загружать необходимое для отладки ПО. Что касается видеоконференции, то она становится обычным способом общения между сотрудниками компаний, а переносимость приложений позволяет переключаться с одного устройства на другое практически без ущерба для сеанса голосовой связи, передачи данных или видеоизображения.

Nokia Siemens Networks продемонстрировала на Форуме лучший в своем классе портфель продуктов. В соответствии с прогнозами, к 2011 г. почти полмиллиарда людей будут смотреть телевизионные передачи по мобильным телефонам (исследование IMS, август 2006 г.). Среди таких передач будут прямые трансляции, например, утренние новости, видео по запросу (VoD) или интерактивные сервисы, такие как голосование, приобретение товаров и услуг или просто загрузка музыки, фильмов и игр.

Уже сегодня компания Nokia Siemens Networks предлагает ряд решений, позволяющих удовлетворить ожидаемый спрос потребителей, включая законченное решение для DVB-H (Digital Video Broadcast for Handheld — цифровое видео для портативных устройств), специально предназначенное для массового рынка. Сети стандарта DVB-H с высокой пропускной способностью дополнят сотовое мобильное ТВ и позволят предложить большое количество телевизионных каналов для массовой аудитории с отличными пользовательскими характеристиками. Среди преимуществ IPTV — контент по запросу, функции PVR (запись по запросу, т.е. постановка на паузу передач прямого эфира).

В данный момент предлагается новая форма технологии высокоскоростного пакетного доступа в Интернет (I-HSPA). Через I-HSPA данные с мобильного телефона проходят более короткий и более прямой

путь, а качество услуг впечатляет пользователя намного больше. Технология I-HSPA предоставит операторам сетей 3G WCDMA более прочную основу для предоставления привлекательных сервисов по передаче данных с мобильных телефонов.

Оборудование LTE (Long-Term Evolution), новая технология радиоинтерфейса, имеет потенциал для существенного снижения сложности сетей. Не будучи стандартной по сути, эта технология обеспечит возможность применения более эффективной с точки зрения затрат структуры ценообразования с фиксированным тарифом, способствуя быстрой адаптации пользователей к сервисам мобильной передачи данных, включая мультимедийные приложения.

Для потребителей технология LTE предоставляет более широкие пользовательские возможности с сервисами реального времени, интерактивными сервисами и бесшовным подключением. Например, LTE обещает обеспечить непрерывность сервисов и покрытие в различных сетях (GSM/EDGE, WCDMA/HSPA), а также роуминг по всему миру. Помимо впечатляющей скорости и увеличенной пропускной способности с быстрым временем отклика (по сравнению с цифровыми абонентскими линиями DSL), технология LTE также предоставляет возможность работы с широким выбором устройств и сервисов, таких как телевидение высокой четкости (HDTV).

Начиная с 2001 г., трафик фиксированной голосовой связи снижается, в то время как мобильный трафик и трафик IP-телефонии постоянно растут, в немалой степени — за счет новых абонентов на развивающихся рынках. Этому процессу также способствует развертывание архитектуры подсистемы IP-мультимедиа (IMS).

IMS приложения компании Nokia Siemens Networks способны адаптироваться к различным потребностям, включая пользовательскую IP-телефонию и мультимедиа, VoIP с IP Centrex для предприятий или мультимедийные приложения, основанные на собственных или внешних разработках.

Компания ***"Энвижн Груп"*** продемонстрировала ряд отраслевых решений для телекоммуникационных компаний, операторов связи, предприятий нефтегазового и металлургического сектора.

Значительная часть экспозиции посвящена новейшим решениям по управлению сетями и ИТ-инфраструктурой.

Представлено OSS-решение нового поколения на базе технологий компании AXIOM, направленное на поддержку задач операторов связи в сфере создания и управления услугами. Это решение учитывает специфику пакетных сетей и сетей следующего поколения (NGN), а также современные требования к сокращению сроков вывода на рынок сервисов IPTV, IP VPN, VoIP.

Представлено также OSS-решение на базе технологий EMC Smarts, автоматически определяющее первичную причину сетевых сбоев и рассчитывающее степень их воздействия на рабочий процесс крупной государственной или коммерческой компании. Работа этого решения базируется на использовании патентованного алгоритма RCA (Root Cause Analysis), позволяющего моделировать сетевые системы, а также контролировать и анализировать события в режиме реального времени, приводя потребности корпораций в управлении сетевыми системами в соответствие с задачами бизнеса.

Важной частью экспозиции "Энвижн Груп" стало решение мобильной видеоконференцсвязи на базе TANDBERG Tactical MXP, активно применяемом в государственных силовых структурах, телемедицинских центрах и корпоративном секторе. Данное решение позволяет организовать высококачественную видеосвязь из любой точки Земли, где отсутствуют наземные линии связи и отличается удобством использования, высокой прочностью и минимальным временем развертывания комплекса, составляющим не более 15 минут.

В этом году на стенде компании ***АМТ-ГРУП*** были представлены решения по обеспечению информационной безопасности и IP TV, развернуты: корпоративная система управления информационной безопасностью на основе решений Checkpoint по защите данных и корпоративной инфраструктуры, система защиты корпоративной электронной почты PineApp.

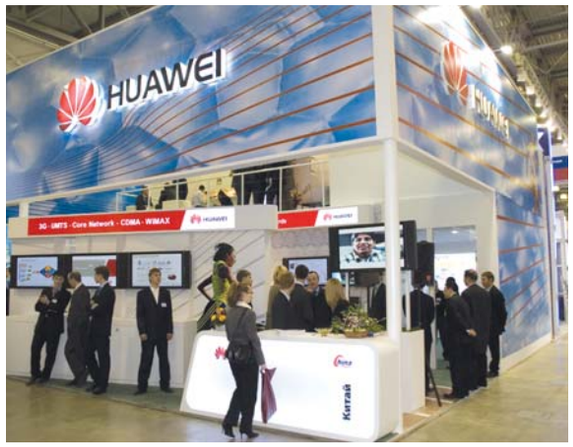
На части стенда компании, посвященной системам цифрового интерактивного телевидения, развернуты комплексные решения на базе DVB и IP-технологий. Наряду с демонстрацией традиционных вещательных и интерактивных ТВ-сервисов для систем IPTV корпоративного и операторского классов на базе Middleware, VOD, CAS/DRM и STB продуктов, АМТ-ГРУП представила новинки в области media-мониторинга качества сигналов, полиэкранного отображения, оформления эфира, интеграцию с web-сервисами.

"Гудвин" представил новое комплексное решение проблемы "последней мили" в сетях NGN для сельской местности на базе универсальной телекоммуникационной платформы "Гудвин Бородино" радиотехнологии DECT.

Экономически целесообразное IP-решение по организации сельской связи и реализации задач приоритетных национальных проектов для операторов электросвязи базируется на интеграции цифрового IP-шлюза в контроллер базовых станций с подключением к Softswitch по протоколу сигнализации SIP.

Среди новых разработок: терминальный абонентский радиоблок "Гудвин Таруса-С8Д" со встроенным фильтром для подавления электромагнитных помех от сетей GSM-1800.

Перспективные модели базового и абонентского оборудования стандарта DECT предназначены для реализации широкополосного доступа: БС9-ETH с интерфейсом Ethernet со скоростью передачи данных 13,824 Мбит/с, терминальный абонентский блок "Гудвин Таруса-С9ETH" с интерфейсом Ethernet со скоростью передачи данных 1,152 Мбит/с.



Состояние и перспективы развития Интернета в России

10-12 сентября 2007 г. в подмосковном пансионате "Ватутинки" состоялась VIII международная конференция " Состояние и перспективы развития Интернета в России". Подготовку конференции осуществляло общественно-государственное объединение "Ассоциация документальной электросвязи" (АДЭ).

Одним из важнейших условий создания в России информационного общества и интеграции страны в глобальное информационное пространство является развитие сети Интернет, как средства предоставления широкого спектра инфокоммуникационных услуг.

Участие в конференции представителей крупнейших международных организаций подтверждает, что развитие инфокоммуникационных технологий, в том числе сети Интернет в нашей стране достигло значительного уровня. Сегодня для этого делается немало — на всей территории России организуются пункты коллективного доступа в отделениях почтовой связи, в том числе в рамках универсального обслуживания; российские школы подключаются к сети Интернет в рамках приоритетного национального проекта "Образование". В 2007 г. количество пользователей сети Интернет в России достигло 30 млн.

Вместе с тем, очевидно, что решение таких важных вопросов, как интернационализация доменных имен, информационная безопасность, идентификация и анонимность в сети возможно только на международном уровне.

Темы конференции

Идентификация и анонимность в Интернете. Должен ли Интернет оставаться анонимным, и что за этим последует? На заседании анализировалось сегодняшнее положение дел в области идентификации пользователей и технических средств, перспективы дальнейшего развития Интернета как основы глобального информационного общества, вопросы информационной безопасности. Обсуждалось влияние фактора анонимности на возникновение и распространение угроз информационной безопасности.

Международные, национальные проекты и программы поддержки развития Интернета. Обсуждались национальные и международные инициативы и программы по поддержке развития Интернета, обеспечивающие расширение инфраструктуры IP-коммуникаций и IP-сервисов, разнообразие контента и приложений, надежность и безопасность использования.

Международное управление использованием Интернета. Данная тема является одним из важнейших вопросов, поднятых в ходе Всемирной встречи на высшем уровне по вопросам информационного общества. Согласно Тунисской программе для информационного общества управление использованием Интернета охватывает как технические вопросы, так и вопросы государственной политики, и должно осуществляться при участии всех заинтересованных сторон и соответствующих межправительственных и международных организаций.

Опыт работы телекоммуникационных компаний в условиях изменения нормативно-правовой базы. В формате круглого стола анализировались ключевые моменты изменения нормативно-правовой базы и перспективы ее дальнейшего совершенствования.

Развитие инфраструктуры IP-коммуникаций. IP-сервисы сегодня и завтра. Сегодня практически не осталось физических сред и технологий передачи данных, не связанных с переносом IP-пакетов. IP-технологии прочно утвердились как в сетях доступа, так и в транзитных сетях. На заседании обсуждались важные изменения в развитии инфраструктуры IP-коммуникаций, произошедшие за год, а также наметившиеся тенденции и проблемы, требующие срочного решения. Происходит разделение операторского бизнеса на сетевую (транспортную) и сервисную (предоставление различных услуг) компоненты. До недавнего времени единственной услугой в операторском бизнесе была услуга "доступа в Интернет" ("широкополосный доступ"), сводящая роль оператора лишь к передаче IP-пакетов. Появление термина IP-сервисы означает попытку операторов связи изменить ситуацию и играть более важную роль на поле, где сегодня господствуют Интернет-компании.

IP-технологии в сетевых инфраструктурах. Использование сетей подвижной радиотелефонной связи 3G/HSPA/LTE. Рассматривались вопросы эффективного использования потенциала существующей кабельной инфраструктуры для оказания современных инфокоммуникационных услуг. Обсуждалась стратегия использования инфраструктур, обеспечивающих ее конкурентоспособность, а также роль и значение сетей связи третьего поколения в широкополосном доступе к Интернету и предоставлении мультимедийных сервисов.

Интернет и цифровое телевидение. Первая волна развития IPTV, вызвавшая чрезвычайно сильный интерес и энтузиазм игроков телекоммуникационного и медийного рынков, в последние два-три года схлынула, предоставив заинтересованным лицам и организациям возможность проанализировать итоги этого начального роста, сделать выводы на будущее и скорректировать планы. Каковы эти итоги, в чем состоят проблемные зоны IPTV и возможные точки роста следующей волны его развития? Что нового в технологиях IPTV и в его бизнес-моделях? Являются ли видеоконтентные Интернет-сервисы (например, YouTube) угрозой для IPTV или они дополняют друг друга?

Интернет-сервисы и контент: модели бизнеса. Представители ведущих компаний-разработчиков контента и Интернет-сервисов обсудили действующие и перспективные модели ведения бизнеса, включая контекстную и медийную рекламу, премиум-сервисы, вопросы взаимодействия с Интернет-сервис-провайдерами.

Проекты АДЭ. Подтверждение соответствия по треюбованиям базового уровня информационной безопасности операторов связи. Сервисная инфраструктура общего пользования. Создание пилотной зоны UNUM в России.

В конференции принимали участие представители федеральных органов исполнительной власти, российские и зарубежные операторы связи, интернет-сервис-провайдеры, производители оборудования, представители интернет-компаний, пользователи IP-коммуникаций и IP-сервисов. Выступили ведущие российские специалисты, а также ведущие эксперты ISOC, IETF, ICANN. Во время конференции работала экспозиция, демонстрирующая достижения в использовании IP-коммуникаций и IP-сервисов для повышения эффективности деятельности организаций и улучшения условий жизни граждан.

В рамках конференции состоялось традиционное вручение почетных дипломов за достижения в области развития российских инфокоммуникаций.