МОБИЛЬНЫЕ ТЕЛЕКОММУНИКАЦИИ № 6/2011

# МОБИЛЬНЫЕ ТЕЛЕКОММУНИКАЦИИ

№6
август
2011

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

## В ожидании MVNO

## Новая стратегия Orange Business Services

ISSN 1562-4293

Подписные индексы: 79177 по каталогу «Роспечать», 27902 по каталогу «Пресса России»

Bakutel

17-я Азербайджанская Международная Выставка и Конференция
**“ТЕЛЕКОММУНИКАЦИИ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ”**

## 23-26 Ноября 2011
## Баку, Азербайджан

Генеральный спонсор
**Microsoft**

Присоединяйтесь к нам: facebook
http://www.facebook.com/BakuTel

Поддержка
Министерство Связи и Информационных Технологий Азербайджанской Республики

Организаторы
ITE, Iteca CASPIAN
Тел.: +994 12 447 47 74
Факс: +994 12 447 89 98
E-mail: telecoms@iteca.az

Место проведения
BAKU EXPO CENTER

**www.bakutel.az**

ufi Approved Event

# СЕДЬМОЙ ФОРУМ ИНВЕСТИЦИИ В ЦИФРУ. ПРАВОВЫЕ АСПЕКТЫ

## 19 ОКТЯБРЯ 2011 г.

**Гостиница "ПРЕЗИДЕНТ-ОТЕЛЬ" Управления делами Президента РФ**
г. Москва, ул. Б. Якиманка, 24

### 11.00-13.00 ПЛЕНАРНОЕ ЗАСЕДАНИЕ

**Участники:** представители Минкомсвязи, Роскомнадзора, Правительственной комиссии по развитию телерадиовещания, АКТР, ведущие эксперты отрасли.

**Вопросы для обсуждения:**

- Реализация ФЦП «Развитие телерадиовещания в Российской Федерации на 2009-2015 годы». Перспективы на 2015-2020гг.;
- Принципы и реальные сроки формирования 2-го и 3-го мультиплексов;
- Порядок распределения обязательных общедоступных каналов в сетях операторов многопрограммного телевидения. Цели государственного регулирования, проблемы реализации в аналоговых сетях;
- Исполнение и практическое применение правил лицензирования телеканалов для операторов многопрограммного телевидения.

### 14.00-15.30 Секция 1.

Актуальные вопросы лицензирования и взаимодействия игроков телекоммуникационного рынка.

### 16.00-17.30 Секция 2.

Использование интеллектуальной собственности. Развитие инвестиций в цифровое вещание.

**17.30** Подведение итогов Форума. Окончание мероприятия.

Внимание, количество мест ограничено!
Регистрация на Форум:
**www.midexpo.ru/idforum**

За дополнительной информацией обращайтесь:
тел.: +7 (495) 737-74-79

Реклама

Организаторы форума: АКТР, MIDexpo МЕЖДУНАРОДНЫЕ ВЫСТАВКИ И ЯРМАРКИ
Стратегический партнер: SALANS
Генеральный информационный партнер: ТЕЛЕСПУТНИК
Генеральный интернет-партнер: COMNEWS
Отраслевой медиа-партнер:

## РЕГИСТРАЦИОННАЯ ФОРМА

Пожалуйста, заполните заявку и вышлите её на электронный адрес Организаторам Форума [yana@midexpo.ru] или по факсу: +7 (495) 737-68-45

### Сведения о Компании

Название:
Адрес:
Тел/Факс: E-mail:

### Первый участник

ФИО:
Должность:

### Второй участник

ФИО:
Должность:

### СТОИМОСТЬ УЧАСТИЯ

В стоимость участия входит: информационные материалы Форума, кофе-брейки, обед.

| Цена | |
|---|---|
| Для 1 участника | **18 000** руб. |
| Для 1 участника в группах из 2-х и более человек от одной организации **(СКИДКА 5%)** | **17 100** руб. |
| **ДПЯ УЧАСТНИКОВ ВЫСТАВКИ CSTB’2011** | |
| Для 1 участника **(СКИДКА 5%)** | **17 100** руб. |
| Для 1 участника в группах из 2-х и более человек от одной организации **(СКИДКА 10%)** | **16 200** руб. |
| **ДЛЯ КОМПАНИЙ-ЧЛЕНОВ АКТР** | |
| Для 1 участника **(СКИДКА 10%)** | **16 200** руб. |

Все цены указаны без учета НДС 18%.
Пожалуйста, укажите источник, откуда Вы узнали о Форуме:

Организатор: «Мидэкспо – выставки и ярмарки», тел.: (495) 737-74-79, факс: (495) 737-68-45, регистрация на сайте: **www.midexpo.ru/idforum**

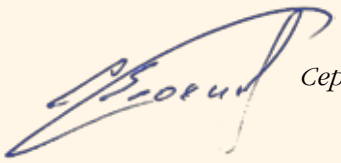
# ЖАРКОЕ ЛЕТО

Лето выдалось богатым на события, связанные с обеспечением информационной безопасности. В дополнение к утечкам персональных данных из информационных систем организаций и вирусным атакам, которые уже стали привычными, произошел скандал, связанный со слежкой Apple за перемещениями пользователей телефонов iPhone. Еще одним нашумевшим случаем стала утечка в поисковые системы личных SMS-сообщений абонентов «МегаФона», которые были отправлены через сайт компании. А буквально через несколько дней выяснилось, что в поисковиках доступна информация о покупателях и об их заказах в некоторых интернет-магазинах.

Регулирующие органы начали расследование этих инцидентов. Компании — участники скандалов перекладывают вину друг на друга, стремясь компенсировать имиджевые потери. Между тем существует законодательный механизм для предотвращения подобных проблем: завершая весеннюю сессию, депутаты Госдумы приняли очередные поправки к Федеральному закону «О персональных данных». Однако в экспертных кругах поправки были признаны нецелесообразными, так как, по мнению ряда авторитетных специалистов, их применение приведет к неоправданному росту расходов компаний на информационную безопасность, но при этом не обеспечит сохранности данных. Эти доводы были изложены в открытом письме президенту РФ с просьбой отложить подписание обновленного закона.

Важность защиты персональных данных очевидна, но мало кто из нас верит, что утечки в Интернет информации о том, где и когда мы бываем, кому и что пишем, что и где покупаем, можно прекратить раз и навсегда. Наш социум постепенно становится по-настоящему информационным обществом, и все больше различных информационных систем становятся неотъемлемой частью нашей жизни, а потому мы вынуждены все чаще предоставлять свои данные разнообразным сервисам.

«Открытие» личной информации — неизбежная плата за прогресс в сфере информатизации. Можно провести аналогию с автомобильным транспортом: пока автомобили не получили широкого распространения, не было большого числа жертв ДТП и необходимости в правилах дорожного движения. С течением времени, вероятно, законодательная база будет совершенствоваться, компании научатся лучше обращаться с пользовательскими данными, а сами пользователи станут осторожнее при размещении своих данных. На вопрос о том, что делать сейчас простым пользователям, абонентам и покупателям, однозначного ответа нет. Остается вспомнить старую добрую истину: спасение утопающих — дело рук самих утопающих.



*Сергей Ерохин, издатель*


# тема номера:
## Информационная БЕЗОПАСНОСТЬ



МОБИЛЬНЫЕ ТЕЛЕКОММУНИКАЦИИ
6 август 2011


Босс — издается совместно с журналом «БОСС»

№ 6 (108)/2011
Издается с 1999 года

**Издатель**
Сергей Ерохин (erokhin@profi-press.ru)
**Научный редактор**
Александр Семенов (semyonov@profi-press.ru)
**Ответственный редактор**
Маргарита Пасечник (pasechnik@profi-press.ru)
**Ответственный редактор интернет-портала**
Леонтий Букштейн (leo@profi-press.ru)
**Обозреватели:**
Сергей Данилин, Павел Катков
**Электронный адрес редакции**
mobile@profi-press.ru
**Дизайн и верстка**
Сергей Павленко





Учредитель
ЗАО «Профи-Пресс»

**Президент**
Ю. А. Кузьмин (kuzmin@profi-press.ru)

**Служба распространения**
Татьяна Михайлова (secretar@profi-press.ru)

**Адрес для переписки:**
Россия, 125993, Москва, ГСП-3, Волоколамское ш., д. 2

Тел./факс: (499) 753-05-51, 753-05-52
E-mail: mobile@profi-press.ru
URL: www.mobilecomm.ru

Издание зарегистрировано в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций ПИ № 77-14698

Научное издание

Печать офсетная. Формат 60x90/8. Печ. л. 7. Уч.-изд. л. 8,5.
Изд. № 598. Тираж 5000 экз. Цена свободная.
Отпечатано в типографии ЗАО «ФАБРИКА ОФСЕТНОЙ ПЕЧАТИ»
тел./факс: (495) 745-08-20
ISSN 1562-4293

# ORANGE BUSINESS SERVICES:
## новая стратегия развития

**Orange Business Services — торговая марка, объединившая в 2006 году под одним именем все работающие на корпоративном рынке компании Группы France Telecom. В России этот бренд занимает традиционно сильное положение на телекоммуникационном рынке. В интервью издателю журнала Сергею Ерохину генеральный директор Orange Business Services в России и СНГ Кристоф Жоанбланк рассказал о новой стратегии развития компании, своем отношении к консолидации телекоммуникационного рынка в России и перспективах конкуренции с универсальными операторами.**

**— Г-н Жоанбланк, в январе 2011 года исполнился год с момента вашего назначения на пост генерального директора. Каких результатов удалось достигнуть за это время?**

— Одной из основных задач первого года моей работы на посту генерального директора стала стабилизация финансового положения после кризиса. Я считаю, что задачу нам удалось выполнить полностью.

Кроме того, необходимо отметить, что в 2010 году во всей Группе France Telecom произошли достаточно большие изменения: пришел новый генеральный директор, и мы совместно начали разрабатывать новую стратегию, которая получила название Conquests 2015 (Завоевания 2015). Все региональные и функциональные подразделения Группы France Telecom участвовали в разработке этой стратегии. В общей сложности разработка стратегии заняла около шести месяцев, и в конце прошлого года мы презентовали ее всем сотрудникам компании.

**— Насколько успешным был 2010 год для вашей компании?**

— Этот год был очень успешным для всей Группы France Telecom. В первую очередь, мы выполнили обещание, данное акционерам, free cash flow составил €8 млрд.

Для российского филиала прошедший год был также достаточно успешным. Это был третий год подряд, когда мы смогли показать хорошие результаты и внести свой вклад в консолидированные финансовые показатели Группы France Telecom.

В прошлом году нам удалось завершить много серьезных проектов. В частности, нам удалось реализовать проекты с Росбанком, Сбербанком и некоторыми другими финансовыми учреждениями. Сейчас наша база корпоративных клиентов насчитывает более 4500 юридических лиц.

Что касается сетевой инфраструктуры, то мы продолжили расширение своей магистральной сети. В 2010 мы запустили сегмент «Москва — Ростов-на-Дону», подготовили свою сеть к переходу на IPv6. Также мы открыли новый контакт-центр в Нижнем Новгороде и новый центр обработки данных в Москве.

Подводя итог, могу сказать, что 2010 год был для нас успешным как в финансовом плане, так и в операционной деятельности.

**— Как вы оцениваете долю компании Orange Business Services на телекоммуникационном рынке России?**

— Абсолютные цифры, определяющие долю рынка, назвать сложно, так как не все операторы связи публикуют свою отчетность. Но, например, о предоставлении услуги IP-VPN я могу сказать точно, что наша компания — один из двух крупнейших операторов в стране. Что касается предоставления голосовой фиксированной связи, то в этом сегменте наша доля меньше: мы занимаем несколько процен-

тов рынка, и этот показатель очень сильно зависит от региона. Orange Business Services является одним из восьми операторов в России, которые имеют общенациональные лицензии на МГ/МН-связь.

**— На ваш взгляд, каковы преимущества компании перед конкурентами?**

— Во-первых, у нас развитая транспортная сеть. Она построена на оптоволокне, так же как и «последние мили». Причем мы — единственный крупный западный оператор связи, присутствующий в России, который имеет свою собственную магистральную сеть и обслуживающий персонал. Остальные западные игроки, как правило, арендуют сеть у российских операторов.

Во-вторых, у нас очень хороший потенциал для внедрения инноваций благодаря принадлежности к Группе France Telecom — Orange. Мы можем брать западные разработки и локализовать их для российского рынка. Это дает нам преимущество в скорости вывода на рынок новых продуктов.

В-третьих, у нас очень высококачественная клиентская база. Orange Business Services является одной из самых сильных телекоммуникационных компаний в мире по работе с транснациональными клиентами. Причем не только с западными компаниями, которые выходят на российский рынок, но и с крупными российскими компаниями, начинающими работать на международном рынке. Последнее время этот процесс идет все более активно.

Хочу отметить, что большую часть выручки Orange генерируют именно российские компании. По моим оценкам, эта пропорция 40:60 — доля выручки от международных компаний, работающих в России, составляет 40%, а российские компании приносят 60% доходов.

**— У вас есть успешные примеры российских компаний — клиентов Orange Business Services, работающих на российском и зарубежных рынках и продолжающих пользоваться вашими услугами связи?**

— Подобных компаний-клиентов у нас много. В основном это нефтегазовые и финансовые компании. По соглашениям конфиденциальности мы не можем назвать всех заказчиков, но в качестве примера могу привести крупного туристического оператора «Пегас Туристик», с которым мы начали сотрудничать в России, а теперь предоставляем услуги связи его зарубежным подразделениям.

*«Мы не будем покупать мелкого российского оператора связи только потому, что он продается»*

**— За последние годы телекоммуникационный рынок России сильно изменился. Прошла целая серия сделок по слиянию и поглощению. Рынок консолидируется вокруг нескольких крупных игроков. Как вы относитесь к этому процессу?**

Действительно, российский телекоммуникационный рынок переживает сейчас волну слияний и поглощений. В первую очередь это те покупки, которые делает «большая тройка», а после слияния «Связьинвеста» и «Ростелекома» можно будет говорить о «большой четверке».

Что касается наших планов, то мы не планируем конкурировать с «большой четверкой» в этом направлении. Мы не будем покупать мелкого российского оператора связи только потому, что он продается. По нашим оценкам, это не будет способствовать достижению поставленных перед нами целей. Мы хотим дифференцироваться в глазах заказчиков за счет предложения более качественных и инновационных сервисов — например, облачных технологий, качественного видео и т.д. Наша задача — оставаться в секторе фиксированной связи для сегмента B2B и все больше развивать сектор ИТ-услуг. Поэтому если мы и будем рассматривать какие-то приобретения, то это будут компании, оказывающие ИТ-услуги: небольшие системные интеграторы, компании, предоставляющие услуги контакт-центров, или ЦОДы. Этот вариант консолидации возможен.

Кроме того, мы считаем, что когда на рынке идет волна слияний и поглощений, то приобретающим компаниям всегда потребуется время на то, чтобы осуществить качественную интеграцию и консолидацию приобретенных активов. Мы думаем, что для нас это «окно возможностей», которое нужно использовать для завершения трансформации нашей компании и развития относительно нового для нас сектора ИТ-услуг.

**— Какие стратегические направления компания выбрала для своего развития?**

— Первое наше приоритетное направление, как и указано в стратегии Conquests 2015, — это качество обслуживания наших заказчиков, соответственно качество наших сервисов также должно быть на высоте. Второе — мы будем продолжать развивать нашу сеть. Третья составляющая нашего успеха — это

наши сотрудники. Любая успешная компания — это прежде всего компания, в которой работают люди, с удовольствием приходящие на работу и получающие удовольствие от того, что они делают. И, конечно, мы будем продолжать выводить на рынок новые услуги.

Если говорить о портфеле услуг, мы планируем выпускать больше ИТ-сервисов, трансформируясь из оператора, предоставляющего традиционные услуги связи, в интегратора телекоммуникационных решений. В продуктовом портфеле будет появляться все больше услуг на стыке ИТ и телекоммуникаций — например, облачных сервисов, видео-решений, решений по управлению ИКТ-инфраструктурой заказчика и т.п.

***«Мы планируем выпускать больше ИТ-сервисов, трансформируясь из оператора, предоставляющего традиционные услуги связи, в интегратора телекоммуникационных решений»***

Многие услуги мы планируем предоставлять по принципу as a Services, который подразумевает отсутствие капитальных вложений со стороны клиента и оплату за фактическое пользование услугой.

**— Вы имеете в виду облачные услуги?**

— Да, мы говорим о развитии направления облачных сервисов. Orange Business Services к 2015 году на глобальном уровне планирует добиться дохода €500 млн от облачных услуг. И Orange Россия, конечно, будет принимать участие в достижении этой цели. Для усиления наших позиций на рынке Cloud Computing мы сформировали несколько «облачных партнерств».

В сентябре прошлого года было объявлено о создании глобального бизнес-альянса, который получил название Flexible 4 Bussiness, между компаниями Orange Business Services, Cisco, EMC и VMware. Цель данного союза — предоставить корпоративным заказчикам весь комплекс услуг в сфере облачных вычислений. Orange Business Services выполняет роль провайдера/интегратора облачных сервисов для всех проектов этого альянса и помогает клиентам внедрять облачные решения, в том числе строить «частные облака», используя продукты партнеров. В следующем году мы планируем запустить наше первое «публичное облако».

Мы планируем также развивать решения по безопасности и решения, которые у нас условно называются «рабочие места будущего». Первое подобное решение появится осенью этого года и будет называться Business Together, совместное с Microsoft. Это облачное решение — Unified Communication as a Service (UC as a Service).

Все перечисленные решения в основном ориентированы на крупные компании. Для компаний малого и среднего бизнеса численностью до 250 человек Orange предлагает продукт Easy Office.

Easy Office — это коробочное решение, позволяющее просто и без дополнительных расходов на оборудование (мини-АТС, Ethernet-коммуникатор) подключиться к сети Интернет и организовать телефонную связь в офисе.

**— Что имеется в виду под термином «безопасность как услуга»?**

— В Orange существует целый ряд услуг по безопасности. Среди них, например, Internet Umbrella — это услуга эффективной круглосуточной защиты сети клиента от DDoS-атак на уровне оператора, способная блокировать атаку до входа в клиентскую сеть и позволяющая функционировать ресурсам сети клиента даже в условиях активно ведущейся атаки. Клиент в качестве сервиса получает возможность использовать наши аппаратные ресурсы, а также техническую поддержку опытных специалистов, которые обеспечивают надежную защиту информации в клиентской сети.

В ближайшем будущем мы выпустим более комплексное решение — Security as Service. Также мы планируем коммерческое развертывание услуги «резервное копирование как услуга» (Backup as a Service), когда пользователь сможет осуществлять резервное копирование своих данных на наши аппаратные ресурсы и платить только по факту получения услуги.

**— Чем отличаются условия работы компании в России от условий в других странах мира?**

— Бизнес Orange в России сфокусирован исключительно на сегменте B2B, предоставлении услуг фиксированной связи. Такая ситуация уникальна для Группы France Telecom, так как в большинстве европейских стран (Франции, Испании, Польше и т.д.) Orange работает во всех сегментах: мобильном, фиксированном, а также B2B (корпоративный сегмент) и B2C (потребительский сегмент).

Конечно, способы ведения бизнеса в России менее формальны, чем в большинстве других стран. Но при этом принципы нашей работы нисколько не отличаются от международных. Пока у нас получается применять здесь те же бизнес-процессы и процедуры, что и в других странах. Мы применяем глобальные методы работы в национальной специфике российского телекоммуникационного рынка, и у нас это успешно получается. Хочу отметить, что France Telecom обслуживает своих клиентов в 220 странах, и в России мы предлагаем нашим клиентам те же самые услуги, что и клиентам в других государствах.

**— Orange Business Services, наверное, единственный крупный телекоммуникационный оператор в России, который не имеет своего подразделения мобильного бизнеса. Все остальные конкуренты превратились в универсальных операторов, которые могут предложить своим корпоративным клиентам услуги как фиксированной, так и мобильной связи. Как этот факт может повлиять на развитие бизнеса в будущем?**

— Как я уже отметил, услуги мобильной связи в России мы не предоставляем — так сложилось исторически. Сейчас мы не видим причин вкладывать огромные средства в строительство собственной мобильной сети в стране, которая уже достаточно насыщена сотовой связью.

*«Сейчас мы не видим причин вкладывать огромные средства в строительство собственной мобильной сети в стране, которая уже достаточно насыщена сотовой связью»*

Стратегия Orange Business Services в России формировалась без учета мобильного сегмента. Конечно, у нас есть соглашения с ведущими операторами сотовой связи, по которым наши клиенты могут получать конвергентные услуги. Но основывать свою стратегию развития на этом мы не стали. Наша задача — капитализировать уже существующие у компании активы. Это фиксированная связь, ориентированная на требования корпоративных клиентов, и внедрение на российском рынке инновационных ИТ-сервисов.

**— Какие цели и задачи ставит перед собой компания на следующий год?**

— До конца этого года мы должны выполнить первую часть стратегии Conquests 2015 и продолжать увеличивать выручку. Достичь этого мы планируем с помощью, во-первых, завоевания новых корпоративных клиентов и увеличения доходов от существующих клиентов. Это наше стратегическое направление будет поддерживаться вторым направлением — развитием ИТ-сервисов. И наконец третье направление — это увеличение нашего присутствия в сегменте малого и среднего бизнеса. Мы считаем, что в настоящее время услуги ШПД можно развивать только здесь. Именно поэтому два года назад было принято стратегическое решение начать инвестиции в этот сегмент клиентской базы. Нельзя сказать, что мы сейчас входим в число крупнейших игроков в России, но в апреле мы подключили к услуге Easy Office 500-го клиента, до конца этого года мы планируем подключить более тысячи и дальше выйти на уровень несколько десятков тысяч клиентов.

**— Вы планируете сосредоточиться на московском или региональных рынках ШПД?**

— Мы планируем развивать продажи услуги Easy Office в 11 крупнейших городах России. Сегодня мы присутствуем уже в девяти из них, и до конца года мы откроем еще два и начнем в них работать.

**— Большое спасибо за интересную беседу!** ■

# СПУТНИКОВЫЙ ШПД В Ка-ДИАПАЗОНЕ

***Александр КОМАРИЦКИЙ,***
*генеральный директор ИСТАР*

На геостационарной орбите становится тесно, и Россия, следуя международной тенденции, спешит занять позиции в новом частотном диапазоне Ка, который еще не задействован на отечественных спутниках. Это отрадно, как и то, что эта задача поддерживается инициативами комиссии по модернизации и технологическому развитию при президенте России по созданию в стране сети спутникового широкополосного доступа (СШПД) под рабочим названием РСС-ВСД. Так же, как в США и в Европе, основная ставка делается на индивидуального пользователя, который с помощью этой сети сможет подключиться к Интернету в любом уголке нашей страны. Эта важная социальная задача может решить проблему цифрового неравенства, стимулировать развитие малого и среднего бизнеса в регионах и, что немаловажно, может стимулировать развитие отечественных технологий космической связи.

Мы строим в России современную рыночную экономику, поэтому даже к социально значимым проектам необходимо подходить по-хозяйски, с анализом рисков и перспектив. Вложены большие средства в строительство спутников, предстоят большие инвестиции в дорогостоящее оборудование наземной инфраструктуры, модернизируется законодательство для обеспечения упрощенного применения терминалов Ка-диапазона. Все эти затраты должны быть обеспечены надежным маркетинговым планом, гарантирующим долгосрочные и достаточные доходы от эксплуатации сети. С учетом инновационности технологии и длительности проекта (около 15 лет) этот маркетинговый план должен быть максимально диверсифицирован и иметь несколько вариантов стратегий развития, обеспечивая возможность маневра в случае неправильной оценки объема или изменения конъюнктуры спроса. Только первая тройка спутников «Экспресс» — АМ4, АМ5 и АМ6, которые уже готовятся к запуску на орбиту, привнесут на рынок более 2,4 ГГц полосы, что на порядок превышает емкость действующих операторов VSAT. А в перспективе запланированы еще два мощных спутника, с еще большей пропускной способностью. Под такой всплеск предложения необходимо готовить и соответствующий рынок сбыта.

Прежде чем мы перейдем к анализу возможных маркетинговых стратегий, хотелось бы несколько слов сказать о технологической специфике спутниковых сетей Ка-диапазона. Как правило, спутники Ка-диапазона имеют многолучевую структуру, что требует использования единой каналообразующей платформы. Это принципиальное отличие от спутников предыдущего поколения, где в одном транспондере могло работать множество операторов с различными VSAT-платформами, арендуя себе необходимую выделенную полосу. Следует также учитывать достаточно большое влияние атмосферных затуханий на сигналы, передаваемые в этом диапазоне частот. Современные VSAT-платформы способны динамически менять параметры каналов, удерживая терминалы на связи в любую погоду, однако это обеспечивается за счет снижения пропускной способности, что накладывает соответствующие ограничения на применение этой технологии при передаче трафика с высокими требованиями к QoS, например в телевизионном вещании.

## Частные пользователи

Основным потребителем услуг в проекте РСС-ВСД планируется индивидуальный пользователь. Пред-

полагается, что таких пользователей будет около 2 млн. Неизвестно, на базе каких маркетинговых исследований была получена эта цифра, но она вызывает большое недоверие. Самое простое — обратиться к опыту внедрения подобной услуги в США, в стране с высоким уровнем развития малого и среднего бизнеса, разбросанного по всей территории государства. Такие предприниматели имеют необходимость в подключении к Интернету как дома, так и на работе, а также имеют достаточный доход. Даже невзирая на мощную финансовую поддержку американского государства в виде дотаций на приобретение терминалов и субсидирование затрат на пользование услугами в труднодоступных регионах, двум американским операторам СШПД сообща удалось подключить чуть более 1 млн пользователей. Так как государственных субсидий для такой услуги в России пока не предвидится, а развитие малого и среднего бизнеса у нас пока находится на очень низком уровне, потенциал проникновения СШПД на российском рынке индивидуальных пользователей может оказаться на порядок ниже, чем в Северной Америке. Нельзя не учитывать и условия, в которых предстоит развиваться российскому проекту: сегодня безлимитные тарифы сетей 3G уже захватили рынки крупных городов, а в течение 15 лет предполагаемой эксплуатации сети СШПД мобильные операторы охватят большинство населенных пунктов, где есть платежеспособный спрос. Уже сегодня обсуждается применение мобильной связи взамен таксофонной сети и пунктов коллективного доступа, созданных в рамках проекта Универсальной услуги, а это также конкуренция для проекта СШПД.

Нет сомнений, что спрос со стороны индивидуальных потребителей будет и он обеспечит значительную долю доходов проекта. Для стимуляции этого спроса потребуются соответствующие меры со стороны государства — это и субсидии для пользователей, проживающих в малонаселенных регионах нашей страны, и налоговые льготы, например возврат НДС при приобретении терминалов частными пользователями или снижение налогооблагаемой базы для предпринимателей и семей с детьми школьного возраста, использующих СШПД, и т.д. Но в любом случае частные пользователи не смогут обеспечить полной загрузки сети и ее рентабельность, то есть необходимы дополнительные каналы сбыта.

## Электронное государство

Спутниковая сеть ШПД Ка-диапазона может стать единым стандартом подключения государственных структур к общероссийской сети электронного правительства, там, где использование наземных каналов невозможно или нерентабельно. Общая для всех государственных структур сеть спутниковой связи обеспечит глобальное покрытие всех региональных представительств власти, значительно упростит процесс их подключения и администрирование. С помощью СШПД могут быть внедрены самые современные технологии, включая электронный документооборот, порталы в Интернете, видео-конференц-связь, удаленные приемные для населения (в том числе и мобильные), дистанционное обучение госчиновников и т.д. Для безопасной передачи информации могут быть использованы соответствующие методы шифрования.

Широкополосное подключение к сети всех госучреждений — это основа перехода к современным технологиям электронного государства, а наличие единого, простого и гарантированного метода подключения позволит в кратчайшие сроки связать все структуры в единую сеть. Следует учесть и колоссальную экономию бюджетных средств, когда разношерстные и часто малоэффективные спутниковые сети различных ведомств заменит единая, стандартная и безопасная инфраструктура связи.

## Специальное применение

Во многих странах мира спутники гражданского назначения и действующие на них VSAT-платформы активно используются и в проектах специального назначения, и это уже является нормой. Преимущества Ка-диапазона для специального применения очевидны ввиду высокой защищенности данного диапазона от преднамеренных помех благодаря узким лучам в обоих направлениях. Современные же технологии шифрования позволят защитить не только передаваемую информацию, но и внутренние команды управления сетью, что делает невозможным не только перехват трафика или станций, но и получение информации об активности станций сети. Возможность работы средств связи спецпотребителей как с военными, так и с гражданскими спутниками значительно расширяет имеющиеся ресурсы, позволяя силовым ведомствам оперативно перейти к самым современным технологиям.

Спутники Ка-диапазона идеально подходят для их использования в вооруженных силах, МВД, силах быстрого реагирования и т.д. Компактный терминал с высокой

пропускной способностью и низким энергопотреблением может находиться в ранце, может быть установлен на транспорте или даже использоваться в движении на земле и в воздухе.

Силовые структуры России могут стать значительным потребителем услуг создаваемой сети СШПД как в повседневной жизни, так и в чрезвычайных ситуациях. Текущие реформы министерств обороны и внутренних дел должны дать толчок к модернизации средств связи этих ведомств. Единственный путь сократить текущее технологическое отставание — это доработка имеющихся современных решений гражданского назначения для их специального применения. Такая технологическая конвергенция позволит в самые короткие сроки модернизировать отечественные средства специальной связи, что значительно повысит безопасность нашего государства в целом.

## Коммерческие проекты

Существует целый ряд коммерческих применений, где спутниковые терминалы СШПД окажутся незаменимыми. Это и резервирование наземных каналов, и широкополосный доступ для проведения сеансов видео-конференц-связи, и доставка тяжелого контента большому числу потребителей и многое другое. СШПД может позволить мобильным операторам значительно поднять пропускную способность имеющихся каналов к их базовым станциям, для обеспечения работы повсеместно внедряемого доступа в Интернет через сети 3Gи LTE.

Еще одна потенциальная ниша — это телевизионные репортажные станции нового поколения, IPSNG. С помощью такой станции можно передавать репортаж с мест событий как в реальном масштабе времени (для непосредственного включения в эфир), так и просто загружать контент на сервер телекомпании для последующего монтажа и воспроизведения в эфире. Компактная и недорогая репортажная станция IPSNG с полностью автоматическим режимом входа в сеть, а также постоянной интерактивной связью со студией позволит значительно повысить оперативность репортажей с мест событий и глобальность охвата, что качественно повлияет на наполнение новостных программ этих телеканалов.

## Перспектива Ка-диапазона в России

Учитывая длительный срок эксплуатации современных спутников, при планировании стратегии желательно предвидеть 20-летнюю перспективу развития телекоммуникаций. В условиях современного темпа развития технологий любые долгосрочные прогнозы не имеют высокой достоверности, поэтому наличие диверсифицированного спектра применений, возможность модернизации аппаратных и программных платформ в процессе эксплуатации позволит адаптировать услуги СШПД под реальные потребности рынка в течение всего срока эксплуатации сети.

Так как модернизировать запущенный спутник уже невозможно, такая универсальность и адаптивность сети накладывает специфические требования к каналообразующему оборудованию — наземному сегменту. Чтобы охватить весь спектр применений, такое оборудование должно изначально иметь специфические технические параметры: высокую пропускную способность, многоуровневый QoS, возможность шифрования данных и каналов управления и т.д. Кроме того, должна иметься возможность доработки такой технологии под специальные требования государственных клиентов или под меняющийся спрос на рынке. Все это достижимо только тогда, когда у компании — оператора сети СШПД есть собственная технология либо неисключительная лицензия, обеспечивающая доступ к исходным кодам для их экспертизы на безопасность и дальнейшей доработки технологической платформы. Неслучайно все американские операторы сетей СШПД являются и собственниками спутников, и производителями технологий — это не только избавляет от технологической зависимости, но и гарантирует многогранность применения их услуг. В тех странах, где есть производители VSAT-систем, сети массового доступа,имеющие национальную значимость, строились исключительно на отечественном оборудовании, что отвечало потребностям технологической независимости страны, стимулировало внутренний спрос, способствовало укреплению и развитию отечественной технологической базы в области связи. Очень важно, чтобы в российском проекте РСС-ВСД были применены не только передовые технологии, но и современные бизнес-подходы, ориентированные на благо населения и государства в долгосрочной перспективе. Как и стратегический проект ГЛОНАСС, создаваемая сеть РСС-ВСД может стать еще одним шансом преодолеть технологическое отставание и обеспечить все категории пользователей в России современным широкополосным спутниковым доступом на базе передовых отечественных технологий. ■

## VSAT В АРЕНДУ. «ИСТАР» ДЕЛАЕТ СПУТНИКОВУЮ СВЯЗЬ ДОСТУПНОЙ

Компания ИСТАР, первая среди производителей оборудования спутниковой связи, предложила своим клиентам оборудование в аренду. Это предложение ориентировано на операторов связи, корпоративных и государственных заказчиков, которые теперь смогут быстро и без значительных капитальных затрат создать собственную сеть спутниковой связи. В аренду может быть предоставлено любое оборудование, производимое компанией ИСТАР — от простейших абонентских VSAT-терминалов, до полноценных Центральных станций.

«Предложение аренды оборудования адресовано исключительно российским пользователям и является нашей подготовкой к выходу отечественного VSAT-рынка из состояния стагнации, который начнется с запуска новых российских спутников связи, намеченного уже на этот год, — комментирует решение компании ее генеральный директор А.И. Комарицкий. — Решением акционеров вся прибыль общества за прошлый год была направлена на дальнейшее развитие нашего успешного проекта, и одной из новых инициатив менеджмента является новый продукт по финансированию клиентских проектов в России».

Возможность аренды оборудования открывает операторам и корпоративным клиентам небывалые возможности при реализации новых проектов:

• значительное сокращение капитальных затрат (CAPEX) проектов, повышение их рентабельности и снижение рисков;

• повышение готовности сетей за счет аренды дополнительного оборудования ЗИП без отвлечения средств оператора на капитальные затраты;

• предоставление клиентам услуг без взимания высоких первоначальных платежей за оборудование (входит в состав услуги);

• возможность исполнения краткосрочных клиентских заказов без риска вложений в оборудование, которое будет возвращено после исполнения такого проекта;

• снижение рисков в новых проектах, длительность которых непредсказуема;

• временное расширение/дублирование технической инфраструктуры оператора для выполнения работ по переводу сетей на новый спутник/частотный диапазон;

• внедрение/тестирование новых продуктов, изучение новых рынков сбыта.

В прошлом месяце компания ИСТАР предоставила одному из своих азиатских клиентов дополнительную Центральную станцию в краткосрочную аренду, что позволило успешно перевести всю сеть из одного частотного диапазона в другой (с заменой РЧ-оборудования) без существенных перерывов связи. Подобные вопросы будут вставать перед многими российскими операторами, которые начнут осваивать емкости новых отечественных спутников, и предложение ИСТАР нацелено на упрощение этой задачи.

Оборудование может быть предоставлено в аренду на срок от трех месяцев до пяти лет. Стоимость аренды маршрутизатора абонентского терминала составляет всего 840 руб. в месяц, а полнофункциональная Центральная станция сети обойдется в 33 400 руб. в месяц. К началу этой кампании ИСТАР специально произвел 4000 маршрутизаторов серии UHP-1000 и UHP-8000 и готов удовлетворить практически любой спрос на свое оборудование.

# АЛЕКСЕЙ КУЗЕНКОВ:

## «Сегмент спутниковой связи в России растет на 15% в год»

*Александр СЕМЕНОВ*

**Интервью заместителя генерального директора — генерального конструктора ОАО «Российские космические системы» Алексея Николаевича Кузенкова научному редактору журнала.**

**— Алексей Николаевич, расскажите о мировом рынке спутниковой связи.**

— Мировой рынок спутниковой связи разделяется на несколько сегментов. Это разработка и производство спутников связи, производство наземного оборудования, пусковые услуги и собственно услуги спутниковой связи.

Если говорить об объеме рынка спутниковой связи, то инвестиции в разработку, производство и запуск (космический сегмент) на период до 2018 года оцениваются приблизительно в $50 млрд, что составляет 57,5% от общего финансирования всех космических систем. При этом 82% затрат на военные спутники и 52% затрат на гражданские ИСЗ являются затратами на спутники связи. В этом сегменте работают такие известные компании, как Lockheed Martin и Boeing (США), Thales Alenia Space и EADS (Европа) и др.

В настоящий момент систем фиксированной и подвижной связи на геостационарной орбите около сотни. В них входит 375 телекоммуникационных космических аппаратов. При этом в разработке находятся еще около 240 систем.

Лидером по региональным системам является США. А лидером по

проектам систем спутниковой связи — Франция.

Совокупные доходы отрасли спутниковой связи в 2010 году составили около $160 млрд.

Сюда включены доходы от услуг спутниковой связи в размере $93 млрд, которые в свою очередь можно разбить на доходы от непосредственного вещания — $75,3 млрд, доходы от услуги фиксированной спутниковой службы — $14,5 млрд, доходы от услуги мобильной спутниковой связи — $2,2 млрд.

Кроме того, есть еще доходы от производства наземного оборудования — $50 млрд, доходы от производства спутников — $13,5 млрд, доходы от пусковых услуг — $4,5 млрд.

Как видно из структуры доходов, основную их долю на рынке спутниковой связи составляют услуги. Причем услуги непосредственного телевизионного и радиовещания.

**— Расскажите вкратце об основных игроках рынка и их доходах.**

— В свое время в Space News был опубликован рейтинг 25 крупных компаний фиксированной космической связи. Среди них две компании, годовые доходы которых превышают $2 млрд и которые контролируют 50% рынка фиксированной спутниковой связи. Это компании Intelsat и SES Global. Годовой доход Eutelsat превышает $1 млрд, остальные ниже. Российская компания ФГУП «Космическая связь» занимает шестое место в рейтинге.

Для сравнения, годовые доходы компаний, предоставляющих услуги непосредственного вещания: Direct TV Group — свыше $20 млрд, DICH Network — свыше $11 млрд, Sirius XM Radio — около $2,5 млрд.

**— Каковы основные тенденции рынка?**

— Основными тенденциями рынка сегодня являются рост пропускной способности систем связи и универсализация услуг.

Это обусловлено ростом общего объема потребляемого трафика. Поскольку ресурсы спутниковых систем связи в традиционных освоенных диапазонах частот C (4/6 ГГц), Ku (11/14 ГГц) в силу организационных и технических причин имеют существенные ограничения, то сегодня интенсивно осваиваются более высокие Ка-диапазоны (18/30 ГГц), позволяющие получить большую полосу пропускания радиосигнала. При этом для «экономии» радиочастотного ресурса и увеличения энергетических возможностей радиолинии на космическом аппарате применяют многолучевые антенные системы с как можно более узкими диаграммами направленности (до 0,35°). Применение таких технологий позволяет уже сегодня создавать высокоскоростные спутниковые системы около 100 Гбит/с, а лет через пять — семь это будут уже терабиты в секунду.

Следствием таких технологических «прорывов» являются новые потребительские свойства спутниковой связи: значительное снижение стоимости трафика, упрощение терминальных устройств. При этом гарантированная скорость абонентского доступа к информационным интернет-ресурсам сопоставима с возможностями иных земных систем (волоконно-оптических, беспроводных).

В результате формируется значительный спрос на персональные услуги спутниковой связи. Пользователь сможет получать все востребованные услуги: высокоскоростной доступ в Интернет, IP-телефонию, IP-телевидение и пр.

По имеющимся оценкам, рынок продаж спутникового оборудования широкополосного доступа в мире показывал рост, несмотря на кризис, и в 2010 году достиг объемов в 2,3 млн терминалов. Аналитики ожидают дальнейший рост на 10—12% в год.

По проведенным нами вместе с нашими партнерами оценкам, в России более 2 млн домохозяйств — потенциальных пользователей спутникового Интернета.

**— Расскажите о примерах современных систем.**

— Прообразами систем, о которых мы только что говорили, явились спутниковые системы, функционирующие на североамериканском континенте. Это такие системы, как Anik F2 (2004 год, TelesatCanada), Ka WildBlue-1 (2006 год, ViaSat Inc.), Ka SPACEWAY (2007 год, HNS). На американском рынке около миллиона пользователей широкополосного спутникового доступа. Между тем при всей насыщенности этого рынка услугами высокоскоростного доступа в Интернет американские операторы планируют запуск новых космических аппаратов с пропускной способностью свыше 100 Гбит/с. На 28 сентября запланирован пуск КА ViaSat-1, оператор ViaSat Inc., в 2012 году запланирован пуск КА Jupiter, оператор Hughes.

Не отстает и Европа. Европейский спутник Ка-диапазона Hylas-1 успешно выведен на орбиту в ноябре 2010 года. Ka-Sat — второй европейский спутник для широкополосного Интернета. Запущен на орбиту 27 декабря 2010 года. По расчетам его владельцев (компания Eutelsat Comm.), спутник обеспечит доступом в Интернет до 1 млн домовладений. Ka-Sat стал первым европейским спутником со сверхвысокой пропускной способностью — до 70 Гбит/с.

В разной стадии реализации находятся аналогичные проекты в интересах других регионов мира: Южной Америки, Северной Африки и Ближнего Востока.

Аналогичный проект в настоящее время реализуется и в Российской Федерации. Он был предложен генеральным директором — генеральным конструктором ОАО «Российские космические системы» Ю.М. Урличичем Комиссии при президенте Российской Федерации по модернизации и технологическому развитию экономики России. В настоящее время в рамках проекта планируется создание целевых космических аппаратов в Ка-диапазоне частот, а также использование ретрансляторов Ка-диапазона новых космических аппаратов «Экспресс АМ 5» и «Экспресс АМ 6».

**— В каких отраслях экономики наиболее популярна спутниковая связь?**

— Во многих. Точнее, во всех, где необходимо обеспечить инфокоммуникационное взаимодействие между распределенными на значительной территории объектами инфраструктуры, подразделениями, офисами. Особенно она актуальна для труднодоступных районов, которых в нашей стране немало. Это добывающие отрасли, энергетика, все виды транспорта, включая трубопроводный, банки с их многочисленной сетью офисов, сети автозаправочных станций, почтовая связь. В каких-то системах спутниковая связь организована резервной к существующим наземным сетям, а в каких-то — в качестве основной и зачастую единственной.

Спутниковая связь незаменима для мобильных объектов: автомобилей, самолетов, пароходов, железнодорожных локомотивов и вагонов, при транспортировке

особо ценных или опасных грузов. В развитых странах уже давно существует возможность доступа в Интернет пассажирам морских круизных лайнеров, скоростных поездов и самолетов, в том числе и возможность телефонных переговоров с борта самолета. Сегодня, применяя технологии спутниковой связи, такие услуги развиваются и российскими перевозчиками.

А в некоторых регионах Сибири, Дальнего Востока, Сахалина и Камчатки персональная подвижная спутниковая связь — это единственный вид связи, не говоря уж об обеспечении связью при освоении и научных исследованиях в Арктике и Антарктике.

Спутниковая связь используется в качестве канала доступа к научным образовательным ресурсам, в телемедицине.

Само собой разумеется, спутниковая связь широко используется в интересах обороны и безопасности.

**— А что вы можете сказать о российском рынке спутниковой связи?**

— Российский рынок спутниковой связи формируется в основном на ресурсах орбитальных группировок ФГУП «Космическая связь» в составе 11 спутников связи и ОАО «Газпром космические системы» — двух спутников «Ямал». Основные виды трафика — это распространение телевизионных и вещательных программ по зонам вещания, магистральные телефонные каналы и передача данных, обмен данными в корпоративных и выделенных сетях, непосредственное телевизионное и звуковое вещание, подвижная и фиксированная правительственная связь — в общей сложности около 300 транспондеров.

Оба владельца спутникового ресурса имеют планы увеличения своей орбитальной группировки. Буквально в ближайшее время будет запущен большой спутник связи «Экспресс-АМ4», в планах следующего года «Экспресс-АМ5» и «Экспресс-АМ6». Заключены контракты на создание еще нескольких космических аппаратов связи и непосредственного вещания типа «Экспресс» и «Ямал». К 2015 году предполагается удвоить возможности спутников связи, а еще через пять лет довести их пропускную способность до 1100 транспондеров. Объемы рынка космических аппаратов до 2018 года составят немногим меньше $1 млрд.

Вместе с тем в настоящее время спрос на спутниковую связь значительно превышает возможности существующих спутников связи. Спрос настолько велик, что потенциальные пользователи заранее «разбирают» ресурсы еще только строящихся и планируемых спутников связи и одновременно атакуют регулятора просьбами упростить разрешительную процедуру допуска к иностранным спутниковым системам связи. И, насколько известно, регулятор всерьез думает об этом.

К слову сказать, территория РФ находится в зонах обслуживания порядка 130 иностранных спутников связи и вещания. Это примерно треть всех телекоммуникационных спутников на геостационарной орбите.

Наибольшие показатели роста демонстрирует сегмент фиксированной спутниковой связи — около 15%, в основном за счет VSAT-сетей.

Несколько слов стоит сказать о сетях VSAT. Буквально эта аббревиатура Very Small Aperture Terminal, то есть терминал с маленькой антенной. Это малая спутниковая земная станция, она используется в спутниковой связи с начала 90-х годов. По международной классификации к VSAT относятся спутниковые станции с антеннами менее 2,5 м. Как правило, для VSAT применяется упрощенная процедура получения разрешений на частоты.

Потребителей российского рынка VSAT можно разделить на четыре сегмента: государственные учреждения; крупные корпорации с разветвленной сетью филиалов и представительств; средний и малый региональный бизнес; частные пользователи.

Сегодня в России около 30 значимых операторов VSAT-сетей, которые обслуживают около 50 тыс. VSAT-станций. 30% таких терминалов находится в Сибирском федеральном округе, примерно по 15% — в Дальневосточном и Центральном федеральных округах, 10% — в Уральском, и по 6—8% — в остальных федеральных округах.

Интересно, что серьезный толчок развитию этого вида связи в России был дан федеральной программой «Образование», в соответствии с которой с 2005 года все школы оснащались доступом в Интернет. Во многих удаленных поселениях это можно было сделать только с помощью VSAT-технологий. Благодаря этой программе их число выросло примерно в 4—4,5 раза.

Другой динамично развивающийся сектор использования спутниковой связи — это непосредственное телерадиовещание. В России уже около 10 млн абонентов спутникового непосредственного вещания. Пять компаний активно конкурируют в этом сегменте, борясь за клиентов. Однако пользователям уже мало обычного телевидения, приходит эпоха телевидения высокой четкости, и появ-

ляется 3D-изображение. Вещание в новых форматах требует совершенно иных ресурсов. Поэтому среди перспективных спутников запланированы два спутника непосредственного вещания.

К сожалению, в нашей стране не получила должного развития услуга непосредственного подвижного спутникового вещания. В российской орбитальной группировке нет пока космических аппаратов такого назначения. Соответственно, не развит и рынок терминального оборудования. И это парадоксально для нашей страны с ее географическими размерами. В мире услуги непосредственного подвижного вещания обеспечивают десять спутников.

Не создана в России и система персональной подвижной спутниковой связи. В настоящее время услуги в этом сегменте в полной мере представляет один оператор — ГлобалТел, использующий спутниковую группировку американской компании Globalstar. И хотя спрос на данную услугу из-за высокой стоимости трафика и абонентского оборудования невелик (около $1 тыс.), тем не менее операторы еще двух систем, Iridium и Thuraya, заявили о своих претензиях на российский рынок. В настоящее время идут подготовительные организационные технические мероприятия для начала предоставления услуг.

К общей грусти, отечественная спутниковая группировка «Гонец» не обладает пока достаточной орбитальной компонентой и требуемыми потребительскими качествами.

Вообще говоря, предоставление широкого спектра услуг для конечных пользователей — это общемировая тенденция. Именно в этом направлении и будет развиваться спутниковая связь: Россия пока немного отстает, но все же ожидания радужные.

**— Приведите, пожалуйста, несколько интересных примеров систем спутниковой связи.**

— Это непросто, поскольку каждая система по-своему интересна и уникальна.

Однако, на мой взгляд, интересны системы спутникового высокоскоростного доступа в Интернет, которые уже упоминались. Упомянутая перспективная система для России так и называется: Российская спутниковая система высокоскоростного доступа (РСС-ВСД).

Интересна японская система высокоскоростной связи «Кизуна». Интересна тем, что в отличие от спутников Ka-Sat, ViaSat-1, Hylas-1, Jupiter она использует обработку и маршрутизацию сигналов на борту. Несмотря на то что такое построение бортового ретранслятора связи значительно его усложняет, а значит удорожает, передовые компании активно разрабатывают эти технологии. Активность в данном направлении проявляет компания Cisco, которая, как анонсировалось, вместе с компанией Astrium приступила к изучению и тестированию приложений для маршрутизаторов космического базирования.

Среди негеостационарных систем интересна, безусловно, система персональной подвижной спутниковой связи Iridium. Уникальность ее в том, что она фактически является глобальной спутниковой системой, то есть обладает возможностью предоставить услугу связи в любой точке земного шара. Другие подобные системы имеют разного рода ограничения. К тому же это единственная система, имеющая межспутниковую связь, что позволяет иметь на земле фактически одну шлюзовую станцию спутниковой связи. Ну а абонентские терминалы этой и подобных систем могут работать как через спутник, так и в сотовых GSM-сетях.

Большой интерес благодаря своему предназначению и технической реализации вызывает перспективная российская спутниковая система «Арктика». Это многоцелевая система, которая предназначена для обеспечения связью террито-

рии нашей страны, включая территории в высоких широтах. Кстати, в том числе и высокоскоростной связью, связью с мобильными объектами и непосредственным телерадиовещанием.

**— Скажите несколько слов о новых технологиях спутниковой связи.**

— Чтобы удовлетворить возрастающий информационный спрос, передавать все большие потоки данных, требуются, как мы уже говорили, широкие полосы частот, и это вынуждает осваивать более высокие частотные диапазоны, выше 30 ГГц, и даже оптические диапазоны, выше 300 ГГц. Однако в силу своих физических свойств радиоволны в этих диапазонах испытывают значительное затухание и рассеивание. Платой за это является повышение мощности передающих средств космической станции, то есть требуется высокая энерговооруженность спутника. Американская компания Loral, например, производит спутники с 30-киловаттными энергоустановками. 12—15 кВт для современных спутников — обыденность. Для сравнения, при создании первых спутников связи 1,5 кВт мощности считалось запредельной величиной. Это стало возможным благодаря научно-техническим достижениям в области создания аккумуляторных, солнечных батарей.

Новые технические возможности порождают новые идеи. Например, очень интересный проект спутниковой системы связи для работы в мобильных сетях реализует в Северной Америке компания SkyTerra. Назначение — работа в мобильных сетях 4G (LTE) Северной Америки на основе технологии Ancillary Terrestrial Component (ATC), запатентованной MSV. Во время перегрузки мобильных сетей пользователи автоматически будут без перерыва связи переключаться на спутник.

На основе новых технологий модернизируются космические аппараты низкоорбитальных систем спутниковой связи Globalstar, Iridium. У Iridium до 1 Мбит/с увеличивается пропускная способность межспутниковых каналов связи. В этих сетях появляются иные большие возможности для пользователей, чем только голосовая связь.

Одновременно появляются новые интересные проекты широкополосной спутниковой связи на основе низкоорбитальных группировок космических систем. Например, проект O3B (the Other 3 Billion), предложенный Google и ViaSat Inc для предоставления высокоскоростного доступа в Интернет населению стран, расположенных вдоль экватора.

Канадская компания Microsat Systems Canada Inc. недавно предложила аналогичный проект CommStellation, в основе которого предполагается группировка из 94 малоразмерных, до 50 кг, космических аппаратов.

Следует сказать, что создание спутниковых телекоммуникационных систем на базе малоразмерных космических аппаратов (мини — до 500 кг, микро — до 50 кг, нано — 1—10 кг) — это отдельная технологическая ветвь. Современная микросхемотехника позволяет создавать приборы и устройства с малыми габаритами и весом. И сегодня все ведущие компании — производители спутников вкладывают значительные средства и усилия в поиски эффективного применения этих возможностей. Вполне возможно, что за такими спутниками будущее. Они достаточно дешевы в производстве и выводе на орбиту, они могут быть разработаны, модернизированы и созданы в достаточно короткий срок, от года до двух лет. Для сравнения, на разработку и создание средних и больших спутников требуется от пяти до десяти лет. Апологеты малых спутников говорят, что космические аппараты, создаваемые в течение пяти — десяти лет и сохраняющие в неизменном виде все заложенные технические и технологические решения на весь срок активного существования — до 20 лет, будут пытаться решать проблемы завтрашнего дня с помощью вчерашних технологий. В этом смысле малые аппараты будут соответствовать требованиям времени, а может и опережать.

Но пока большие аппараты все-таки более эффективны и экономически выгодны.

**— А теперь расскажите немного о проблемах, естественно в России.**

— Основная проблема для операторов спутниковой связи — это ограниченность имеющегося спутникового ресурса.

Проблема для компаний — владельцев космических аппаратов, то есть владельцев космического ресурса — это длительные сроки окупаемости космического аппарата на орбите, высокие риски для инвесторов. А следовательно, трудности получения бюджетных или внебюджетных инвестиций для создания новых спутников связи.

Для разработчиков и производителей космических аппаратов, кроме финансовых ограничений, это отсутствие рынка заказчиков, с одной стороны, и внятной генерации перспективных потребностей от бизнеса, с другой стороны. ■

# АКТУАЛЬНЫЕ ПРОБЛЕМЫ правового регулирования отрасли связи

***Владимир ГОРБАЧЕВ,***
*заместитель председателя Комитета Государственной думы по информационной политике, информационным технологиям и связи*

**Правовое регулирование — важнейший инструмент реализации государственной политики в телекоммуникационной отрасли России.**

В связи с этим, а также принимая во внимание, что связь является одной из самых динамично развивающихся отраслей российской экономики, находится на переднем крае процессов модернизации, технического и технологического обновления, использует инновационные решения, Комитет Государственной думы РФ по информационной политике, информационным технологиям и связи ведет активную законопроектную работу.

Зачастую действующее законодательство не может быть применено к новым отношениям, возникающим в сфере услуг связи, а в ряде случаев тормозит развитие отрасли в целом. Поэтому вопросы совершенствования правового регулирования стремительно развивающегося отечественного телекоммуникационного рынка находятся в центре внимания российских парламентариев.

Остановимся подробнее на законопроектах, затрагивающих сферу информационных технологий и связи, которые были приняты в период весенней сессии 2011 года и находятся на рассмотрении Государственной думы РФ.

28 января 2011 года Госдума приняла в третьем чтении проект федерального закона, предусматривающего сокращение срока принятия федеральным органом исполнительной власти в области связи решения о присвоении радиочастот или радиочастотных каналов для радиоэлектронных средств гражданского назначения на основании заявления граждан РФ или российских юридических лиц с 120 до 35 дней.

Федеральный закон «О внесении изменений в статью 24 ФЗ “О связи”», подписанный президентом РФ 23 февраля 2011 года, также вводит сроки для уведомления заявителя: информация о принятии соответствующего решения размещается на официальном сайте федерального органа исполнительной власти в области связи в сети Интернет в течение пяти рабочих дней. Кроме того, разрешение на использование радиочастот или радиочастотных каналов должно быть подготовлено в течение 20 рабочих дней со дня принятия решения.

Предлагаемые изменения статьи 24 Федерального закона «О связи» будут способствовать ускорению процесса принятия решения о присвоении радиочастоты или радиочастотного канала и устранению административных барьеров.

Кроме того, поправки уточняют терминологию. Так, вводится единое наименование экспертизы — проводимая радиочастотной службой экспертиза возможности использования заявленных радиоэлектронных средств и их электромагнитной совместимости с действующими и планируемыми для использования радиоэлектронными средствами (экспертиза электромагнитной совместимости).

Закон вводит упрощенную процедуру доступа к радиочастотному спектру правопреемника реорганизованного юридического лица.

Чтобы обеспечить возможность непрерывного оказания услуг связи, документ предлагает переоформлять разрешения на использование радиочастотного спектра на правопреемника без изменений условий, установленных при присвоении радиочастот или радио-

частотных каналов реорганизованному юридическому лицу.

Уточняется, что до окончания процедуры переоформления правопреемник вправе использовать радиочастотный спектр в соответствии с ранее выданными документами.

В то же время, в случае реорганизации юридического лица правопреемник в течение 45 дней со дня внесения соответствующих изменений в единый государственный реестр юридических лиц обязан подать заявление о переоформлении решения о выделении полос радиочастот — в государственную комиссию по радиочастотам и разрешения на использование радиочастот или радиочастотных каналов — в федеральный орган исполнительной власти в области связи.

В работе над данным законом, помимо ответственного комитета Госдумы, приняли участие представители Министерства связи и массовых коммуникаций РФ, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также операторов связи.

Комитет по информационной политике, информационным технологиям и связи тщательным образом рассмотрел все поступившие поправки, учел замечания, изложенные в официальном отзыве Правительства РФ, заключении Правового управления Аппарата Государственной думы, а также позицию Государственно-правового управления президента РФ.

В итоге комитет рекомендовал к принятию во втором чтении десять поправок, которые позволят устранить пробелы и коллизии в сфере отношений, связанных с выделением полос радиочастот и присвоением (назначением) радиочастот или радиочастотных каналов.

Рассматриваемый федеральный закон, безусловно, является актуальным и практически значимым. Его принятие было направлено на повышение эффективности распределения и использования такого экономически важного общенационального ресурса, как радиочастотный спектр. Применение его положений позволит государству получить более прогрессивные рычаги управления спектром при рыночных и технологических изменениях, удовлетворить наибольшее количество заявок.


***Владимир Горбачев и Сергей Железняк во время расширенного заседания Комитета Государственной думы РФ по информационной политике, информационным технологиям и связи***

Три законопроекта готовятся Комитетом Государственной думы РФ по информационной политике, информационным технологиям и связи к рассмотрению во втором чтении.

Техническим регламентом «Об электромагнитной совместимости», который был принят в первом чтении 2 июля 2010 года, регулируются отношения, связанные с деятельностью по разработке, изготовлению, ввозу, выпуску в обращение и вводу в эксплуатацию на территории Российской Федерации технических средств, применяемых в условиях электромагнитных помех.

Проект Федерального закона «О внесении изменений в Федеральный закон “О связи”» разрабатывался в целях совершенствования процедуры лицензирования деятельности в области оказания услуг связи.

Поправки вносятся в ряд статей Федерального закона «О связи».

В частности, предлагается отменить требование для соискателя на получение лицензии о представлении документов, заверенных исключительно органами, осуществляющими ведение единого государственного реестра юридических лиц — подразделениями Федеральной налоговой службы. Это позволит сократить срок сбора необходимых для получение лицензии бумаг.

Также вносятся изменения, упрощающие процедуру переофор-

мления лицензии в случае реорганизации юридического лица. Это исключит возможность остановки работы оператора связи при невыполнении им сугубо формальных требований. Сегодня в том случае, если документы на переоформление лицензии не поданы в течение 30 дней с момента реорганизации, деятельность оператора прекращается, что наносит ущерб прежде всего пользователям услуг связи.

Кроме того, поправки устанавливают, что в случае изменения некоторых реквизитов юридического лица или индивидуального предпринимателя переоформление лицензии не потребуется. Будут упорядочены процедурные вопросы переоформления лицензий и внесения изменений и дополнений в лицензии, что позволит операторам связи бесперебойно оказывать услуги связи.

Необходимо подчеркнуть актуальность и практическую значимость законопроекта. Его принятие позволит улучшить условия для развития конкуренции на рынке услуг связи, снизить административные барьеры и инвестиционные риски, ускорить развитие телекоммуникационной отрасли.

В первом чтении законопроект был принят 7 декабря 2010 года. На него получен положительный отзыв Правительства РФ. Рассмотрение законопроекта во втором чтении запланировано на период осенней сессии 2011 года.

На осеннюю сессию в график работы Государственной думы включен и законопроект «О внесении изменений в статью 19 Федерального закона “О связи”». Им уточняются требования к порядку присоединения и взаимодействия сетей связи.

В первом чтении законопроект был принят 26 января 2011 года. Однако к доработанному тексту с учетом поправок имеются серьезные замечания, поэтому было принято решение о создании рабочей группы по подготовке текста законопроекта ко второму чтению, в которую войдут представители Министерства связи и массовых коммуникаций, Федерального агентства связи, телекоммуникационных компаний, члены Экспертного совета при Комитете по информационной политике, информационным технологиям и связи.

На этапе подготовки Комитетом Государственной думы по информационной политике, информационным технологиям и связи к первому чтению находится законопроект, направленный на пресечение незаконного использования похищенных сотовых телефонов.

***«Хищение мобильных средств связи остается в России одним из самых распространенных преступлений. Телефоны воруют сотнями тысяч»***

Хищение мобильных средств связи остается в России одним из самых распространенных преступлений. Телефоны воруют сотнями тысяч. Нередко кражи телефонов становятся частью тяжких и особо тяжких преступлений. Положение усугубляется возможностью легкого сбыта похищенных телефонов и их беспрепятственным использованием в сетях операторов подвижной связи после кражи.

Проблема, таким образом, является актуальной и социально значимой и требует решения на законодательном уровне.

Проектом федерального закона «О внесении изменений в ФЗ “О связи”» предусматривается возможность для абонента по его желанию без оплаты производить регистрацию мобильных телефонов у оператора связи в порядке, устанавливаемом Правительством Российской Федерации. При этом имеется в виду, что будут определены удобные формы регистрации, в том числе это можно будет сделать при покупке средства связи.

В случае кражи зарегистрированного абонентского терминала оператор связи по заявлению абонента должен будет прекратить пропуск трафика от и к этому терминалу, как в своей сети, так и сообщить о факте утери терминала операторам всех сетей подвижной связи, действующим на территории России.

Блокирование работы украденных телефонов в итоге сделает бизнес кражи телефонов неблагодарным делом.

Актуальными остаются вопросы социальных гарантий доступности услуг связи для населения. В частности, депутаты Государственной думы считают, что цены на роуминг завышены и не соответствуют нынешней ситуации в телекоммуникационной отрасли России. Поэтому появилась законодательная инициатива, направленная на отмену национального роуминга. Это поправки в статью 54 Федерального закона «О связи», предусматривающие отмену платы за входящие звонки для абонентов сотовой связи во внутрисетевом роуминге в пределах России. Законопроект готовится к рассмотрению нижней палатой парламента в первом чтении.

Для того чтобы законы работали, законодателям необходимо учитывать мнение тех, кто будет подчиняться этим законам. Только в этом случае вступивший в силу документ не будет оторван от реальной жизни. Это особенно актуально в век интенсивного развития технологий и телекоммуникаций. Поэтому каждый отраслевой законопроект на этапах разработки и процедуры принятия в Государственной думе РФ получает экспертную оценку операторов связи.

Конструктивный диалог между депутатами Госдумы и операторами связи в рамках мероприятий, проводимых Комитетом по информационной политике, информационным технологиям и связи: парламентских слушаний, совещаний, расширенных заседаний комитета а также заседаний Экспертного совета при комитете, помогает принимать законы, учитывающие интересы абонентов и способствующие эффективному развитию телекоммуникационного рынка.

Для работы над некоторыми проектами федеральных законов создаются рабочие группы с участием представителей государственных органов, телекоммуникационных компаний, ассоциаций, научно-исследовательских и общественных организаций.

7 апреля 2011 года в Государственной думе РФ состоялось очередное заседание Секции по информационным технологиям и связи Экспертного совета при Комитете ГД по информационной политике, информационным технологиям и связи.

Члены Экспертного совета и приглашенные специалисты (среди которых представители Аппарата Правительства России, Минкомсвязи, Россвязи, Роскомнадзора, ФАС России, Минэкономразвития России, ФГУП «Почта России», негосударственных операторов почтовой связи) обсудили новую редакцию Федерального закона «О почтовой связи», а также вопросы необходимости внесения изменений в отдельные законодательные акты и развития конкуренции на рынке услуг почтовой связи.

***«Как показало обсуждение, одним из наиболее сложных вопросов, который призван решить законопроект, является обеспечение условий эффективной и добросовестной конкуренции на рынке услуг почтовой связи»***

Свое видение того, как должно осуществляться законодательное регулирование почтовой связи в России, представили докладчики из Министерства связи и массовых коммуникаций РФ, Федерального агентства связи, Федеральной антимонопольной службы, ФГУП «Почта России», Национальной ассоциации дистанционной торговли.

Дело в том, что действующий Федеральный закон «О почтовой связи» был принят в 1999 году. С того времени серьезные изменения претерпел рынок услуг почтовой связи — его структура, состав участников, условия конкуренции.

Участники заседания обсудили новую редакцию Федерального закона «О почтовой связи», подготовленную с целью обеспечения эффективного развития отрасли. Основным разработчиком законопроекта выступило Министерство связи и массовых коммуникаций РФ. Деятельное участие в работе над текстом проекта приняли также и другие министерства и ведомства, в числе которых Министерство финансов РФ, Федеральное агентство связи, Федеральная служба по тарифам, Федеральная антимонопольная служба.

Несмотря на то что проделана большая работа, представляется, что текст законопроекта еще не готов к внесению в Государственную думу. Развитие инфраструктуры почтовой связи, повышение качества оказания услуг населению, обеспечение условий для развития добросовестной конкуренции сегодня являются приоритетными задачами. Для решения этих задач необходимо законодательное регулирование, отвечающее требованиям времени. Во время заседания докладчики изложили основные концептуальные замечания, которые позволят продолжить работу над законопроектом.

Как показало обсуждение, одним из наиболее сложных вопросов, который призван решить законопроект, является обеспечение условий эффективной и добросовестной конкуренции на рынке услуг почтовой связи.

В то же время представляется, что только постепенная либерализация позволит обеспечить инфраструктурную целостность сети общедоступной почтовой связи на всей территории страны и сохранить доступность услуг почтовой связи для населения. С правовой точки зрения наиболее эффективным механизмом, обеспечивающим условия для добросовестной конкуренции, является недискриминационный доступ. В зависимости от отрасли недискримина-

ционный доступ осуществляется в отношении сетей, инфраструктуры и услуг. В сфере электросвязи недискриминационный доступ введен в законодательство в форме правовых условий присоединения сетей связи. Аналогичная правовая конструкция в сфере почтовой связи может стать существенным вкладом в совершенствование отраслевого законодательства.

На основании вышеизложенного участники заседания разработали рекомендации Министерству связи и массовых коммуникаций и Правительству РФ. В частности, было предложено: рассмотреть возможность уточнения перечня универсальных услуг почтовой связи в целях максимально полного удовлетворения потребностей граждан России в почтовых услугах; продолжить работу по дальнейшей либерализации рынка услуг почтовой связи, активизировать в этих целях консультации с различными субъектами рынка почтовой связи, включая федеральную организацию почтовой связи, профессиональные союзы работников почтовой связи, союзы и ассоциации негосударственных операторов почтовой связи; ускорить разработку и внесение в Государственную думу законопроекта, регулирующего вопросы преобразования ФГУП «Почта России» в акционерное общество, и др.

28 июня 2011 года состоялось расширенное заседание Комитета Государственной думы РФ по информационной политике, информационным технологиям и связи. В нем приняли участие председатель комитета Сергей Железняк, депутаты — члены комитета, представители крупнейших телекоммуникационных компаний России.

Участники встречи обсудили инновационные решения на телекоммуникационном рынке, вопросы развития национальной системы телекоммуникаций, социальной значимости телекоммуникационных реформ.

Представители компаний связи дали оценку регулирующему воздействию законодательного процесса на бизнес и высказали предложения по дальнейшему совершенствованию отраслевого законодательства.

***«Среди факторов, мешающих развитию инфраструктуры связи и вызывающих многочисленные нарекания участников телекоммуникационного рынка — избыточное государственное регулирование деловой активности»***

Среди факторов, мешающих развитию инфраструктуры связи и вызывающих многочисленные нарекания участников телекоммуникационного рынка — избыточное государственное регулирование деловой активности.

Проблемы, с которыми сталкиваются в своей работе предприятия отрасли, касаются также правовых гарантий недискриминационного доступа к инфраструктуре связи, технологической нейтральности, гармонизации отраслевого и смежных законодательств, формирования регуляторной среды для обеспечения ускоренного инфраструктурного развития, законодательного оформления совместного использования операторами радиочастот, обмена ими, госрегулирования защиты пользователей мобильной связи от мошенничества и др. Оперативное решение этих проблем, в том числе на законодательно-правовом уровне, будет стимулировать развитие конкурентного телекоммуникационного рынка.

При этом депутаты прежде всего руководствуются интересами людей, которые пользуются услугами связи. Если законодательный орган предпримет необходимые меры для организации эффективной деятельности участников телекоммуникационного рынка, то это приведет к улучшению качества и расширению спектра услуг, снижению тарифов, что в конечном итоге положительно скажется на абонентах.

По результатам расширенного заседания Комитета Государственной думы РФ по информационной политике, информационным технологиям и связи были приняты решения о создании рабочих групп с участием операторов связи по актуальным проблемам отраслевого законодательства. Всего будут сформированы четыре рабочих группы: «По законодательному обеспечению переносимости телефонных номеров в сетях фиксированной и подвижной радиотелефонной связи», «По разработке нормативно-правовой базы в целях реализации государственной программы Российской Федерации “Информационное общество (2011—2020 годы)”», «По анализу правовых аспектов и подготовке законодательных предложений, направленных на обеспечение информационной безопасности SMS-сообщений» и «По подготовке ко второму чтению законопроекта, уточняющего требования к порядку присоединения и взаимодействия сетей связи». ■

# БОРЬБА С ЭКСТРЕМИЗМОМ В ИНТЕРНЕТЕ: ПОИСК «ВИНОВАТОГО»?

***Оксана ГОНЧАРЕНКО,***
*канд. полит. наук,*
*ведущий эксперт Центра политической конъюнктуры*

Борьба с распространением экстремизма все активнее переходит в медийное пространство. 2 июня президент России Дмитрий Медведев подписал ряд поручений, одно из которых предполагает установление пределов ответственности СМИ за размещение комментариев читателей и высказываний, нарушающих российское законодательство. Перспектива нормативных изменений стала предметом дискуссий политологов, экспертов в области права и представителей телекоммуникационных компаний, работу которых напрямую затрагивает президентская инициатива.

Глава государства поручил руководству Минкомсвязи подготовить поправки к законодательству о СМИ, устанавливающие пределы ответственности редакций интернет-изданий за размещение комментариев читателей и высказываний тех или иных лиц, нарушающих, в частности, законодательство о противодействии экстремистской деятельности. Крайняя мера, предусмотренная действующими нормами, — прекращение работы нарушителей: согласно статье 8 Закона «О противодействии экстремистской деятельности», СМИ, уличенное в распространении экстремистских материалов, может быть закрыто.

Полпред президента в Уральском федеральном округе Николай Винниченко продолжил мысль президента РФ о необходимости выработки правовых механизмов для противодействия распространению в сети Интернет материалов, призывающих к насилию, способствующих обострению межнациональных и межконфессиональных отношений и разжиганию розни, обратив внимание на роль провайдеров — операторов связи. В настоящее время их ответственность за размещаемый контент законодательством не предусмотрена. По мнению Винниченко, «оставлять это так нельзя, нужно, чтобы провайдеры мониторили этот вопрос и в случае необходимости несли ответственность». О конкретных формах такой ответственности говорить преждевременно, полпред лишь внес информационный вопрос в политическую повестку дня и в дальнейшем намерен собрать предложения компаний-провайдеров и общественности для анализа.

Бизнес-структуры, предоставляющие населению услуги связи (в частности, доступ во Всемирную паутину) и информацию в Сети (контент-провайдеры), традиционно стремятся дистанцироваться от содержания материалов, распространяемых по полученным от них каналам и через страницы интернет-ресурсов, настаивая на своей посреднической роли. «Ответственность за контент должно нести то лицо, которое разместило контент или дало указание о его размещении, оператор связи не должен быть наделен функциями цензуры», — так прокомментировали свою позицию представители «ВымпелКома», который входит в «большую тройку» сотовых операторов. Подобного мнения придерживаются и другие игроки рынка, что вполне объяснимо: на данном этапе компании, даже крупные, не готовы к серьезным затратам, которых потребовала бы реализация предложенного полпредом президента сценария (установка специальных фильтров для отслеживания противоправной информации и пр.). Ответственность в данном случае возлагается на пользователя, который в случае нахождения экстремистских материалов может сообщить об этом администрации соответствующего интернет-ресурса (последняя в этом случае обяза-

на удалить такие материалы) либо использовать их в иных целях, за что может стать фигурантом уголовного дела.

Указанный порядок действует в настоящее время, но отслеживать данные подобным образом затруднительно. Работа интернет-ресурса может быть прекращена в том случае, если он признан экстремистским (по содержанию материалов) по решению суда, но, как показывает практика, за время разбирательства или вскоре после него могут возникнуть и другие сайты аналогичной направленности. Кроме того, часть ресурсов базируется за рубежом, что представляет отдельную проблему. Об этом, в частности, говорил премьер-министр РФ Владимр Путин 20 апреля в Госдуме, отвечая на вопрос о возможности введения цензуры в Интернете (премьер признал, что «не считает возможным что-либо ограничивать»). Наказания, выносимые авторам сетевых дневников, как правило, получают широкий резонанс, однако не всегда признаются справедливыми активными пользователями Интернета. Преобладает скорее мнение о стремлении властных структур закручивать гайки и ограничивать свободу слова, что не способствует снижению числа провокационных высказываний и иных материалов. Показательный пример — число «защитников» блогера Саввы Терентьева, который был приговорен к году лишения свободы условно за размещение в интернет-дневнике призыва к тому, чтобы сжигать милиционеров на площадях.

Сегодня в полной мере эффективных способов борьбы с распространением экстремизма в Интернете не существует. Дискуссия о стороне, которая несет большую ответственность (пользователь либо ресурс, провайдер), продолжается, при этом максимальная обобщенность понятия «экстремизм» в действующем законодательстве лишь усугубляет ситуацию. С учетом актуальности проблемы обеспечения безопасности неудивительно, что неформальное обсуждение проблемы ответственности СМИ за комментарии читателей имеет политическую подоплеку, связанную с конфликтом интересов разных сегментов элиты. Так, либерально ориентированные эксперты и политики через лояльные информационные ресурсы высказываются о возможности ущемления гарантированного Конституцией права граждан на свободу слова путем «чрезмерного» усиления правоохранителей, которое может привести к злоупотреблению соответствующими полномочиями. В данном случае вопрос об экстремизме зачастую сводится к политике Центра в отношении регионов Северного Кавказа, рассматриваемых как источник террористической угрозы и «черная дыра», в которой коррупционным образом «осваиваются» масштабные финансовые средства. Близкие к силовикам лидеры мнений, напротив, указывают на недостаточность существующих инструментов для борьбы с экстремистской угрозой и зачастую используют достигнутые успехи в деле борьбы с терроризмом как инструмент повышения собственной значимости и неформального статуса в системе органов госвласти. И та и другая «крайние» позиции нецелесообразны с точки зрения приоритетов государственной политики, связанных с обеспечением стабильности и снижением угроз обострения межнациональных противоречий в преддверии парламентских и президентских выборов.

Оценивая перспективу принятия новых норм, устанавливающих ответственность СМИ за публично высказываемые пользователями информресурсов позиции, можно прогнозировать, что в среднесрочной перспективе приоритет получат превентивные меры. Так, можно ожидать ужесточения наказания за преступления, связанные с разжиганием межнациональной розни и призывами к беспорядкам, а также за действия, признанные экстремистскими по решению суда. Введение цензуры в интернет-пространстве в течение ближайшего года-двух маловероятно. Реализация предложения полпреда президента в УрФО об ответственности провайдеров за содержание размещаемых материалов будет затруднена не столько несовершенством законодательства, сколько лоббистской «контригрой», которая может быть развернута представителями работающих в телекоммуникационной сфере крупных бизнес-структур. ■

По данным ВЦИОМ, основные претензии россиян к СМИ связаны не с отсутствием свободы слова, а с отсутствием или недостаточностью цензуры. В ее необходимости убеждены 58% граждан, указывающих на перенасыщенность наших СМИ насилием, пошлостью, дезинформацией и бескультурьем. Однако цензурировать политическую информацию предлагает абсолютное меньшинство. По мнению людей, цензура должна быть направлена против следующих явлений: «показывают много насилия, разврата, пошлости» (40%), «надо избегать клеветы и дезинформации, обеспечивать граждан достоверной информацией» (22%), «избегать глупости, повышать через СМИ культуру, образование граждан» (11%), «СМИ разлагают детей и молодежь» (9%).

# В ОЖИДАНИИ MVNO

***Владимир ФРЕЙНКМАН,***
***Юрий СЕНЧЕНКО,***
*ООО «НТЦ ПРОТЕЙ»*

**На момент написания этой статьи в России насчитывается 67 потенциальных виртуальных операторов сотовой связи. Потенциальных потому, что, обладая лицензиями на осуществление этого вида деятельности, начать оказывать услуги абонентам операторы не имеют возможности в силу отсутствия номерной емкости. Когда именно завершится процесс выделения номеров, предсказать сложно, поэтому за неимением информации к размышлению в виде фактических результатов авторам остается присоединиться к рассуждениям о перспективах развития MVNO и попытаться выделить несколько, на их взгляд, интересных моментов.**

В Европе, где виртуальные операторы функционируют на протяжении уже более десяти лет, имели место проекты как успешные, так и не очень, поэтому однозначно спрогнозировать исход аналогичных отечественных начинаний только на основе имеющегося опыта, скорее всего, не получится. По сравнению с развивавшимся европейским рынком, на котором зарождались первые MVNO, ситуация в России сегодня усугубляется тем, что проникновение сотовой связи давно перевалило за 100%, что сразу ставит под сомнение успех такой категории MVNO, как «игроки с тарифами», к числу которых в первую очередь относятся дискаунтеры. Так как на текущий момент развитие операторов «вширь» закончилось, предоставление емкости практически полностью загруженной сети операторам, играющим на понижение, представляется не совсем оправданной политикой с позиции акционеров сотовых компаний. С учетом третьего пункта «требований к оказанию услуг подвижной радиотелефонной связи при использовании бизнес-модели виртуальных сетей», который закрепляет необходимость согласования виртуалами схемы взаимодействия с владельцем инфраструктуры, появление MVNO-дискаунтеров будет сильно затруднено. Участники рынка традиционно придерживаются полярных позиций по вопросу конкурентного доступа к сетевым ресурсам, однако авторы, ограниченные форматом статьи, оставляют поиск истины на долю ФАС.

Задача MVNO — «игроков с тарифами» заключается в занятии какого-либо сегмента рынка, характеризуемого определенным уровнем расходов на связь. Например, можно попытаться привлечь абонентов, находящихся в режиме экстремальной экономии, на тарифные планы «без излишеств». Либо, наоборот, сформировать предложение, интересное абонентам, рассчитывающим иметь много услуг за много денег. Проблема, однако, состоит в том, что MNO, эксплуатирующие OSS/BSS-системы уже достаточно долгое время и имеющие значительные по своим возможностям отделы маркетинга, способны без посторонней помощи покрыть рынок тарифами, обеспечивающими эффективное сегментирование абонентской базы.

Труды MVNO, манипулирующих тарифными планами, по всей видимости, могут увенчаться успехом в двух случаях. Первый случай имеет место, если у виртуала очень гибкая и функциональная биллинговая система, а также штат маркетологов, способный породить такие тарифы, которые, будучи неудобными для реализации «большим» оператором, были бы достаточно простыми, чтобы можно было доступно изложить их преимущества абонентам, то есть, проще говоря, продать.

Это в первую очередь касается MVNO, которых условно можно назвать «виртуозами биллинга», так как ничем другим, кроме как комбинациями услуг и тарифов, эти операторы не отличаются от MNO.

Часть таких MVNO предоставляет также услуги фиксированной телефонии и доступа в Интернет. Лицензия на мобильную связь, таким образом, превращает их в универсальных операторов, что за счет присущего FMC-компаниям конвергентного эффекта могло бы обеспечить им конкурентное преимущество, но только года три-четыре назад. Сегодня же, как известно, «большая тройка» уже образована этими самыми универсальными операторами, сформированными в результате нескольких крупных поглощений последних лет.

Второй случай успешного запуска MVNO, не предоставляющего абонентам каких-либо дополнительных услуг по сравнению с классическими операторами, как правило, обусловлен тем, что такой оператор использует для привлечения абонентов силу бренда, не имеющего к связи никакого отношения. К примеру, количество болельщиков некоторых футбольных клубов превышает миллион человек, и, при определенном подходе, весь этот миллион может составить абонентскую базу виртуального оператора. Ключевая роль бренда в организации прибыльного MVNO практически не ставится под сомнение, и многие аналитики уверенно предрекают успех компаний такого типа в РФ.

Вообще, описанный случай полного совпадения предоставляемых виртуалом и классическим оператором услуг является предельным и в природе не существует: бренд всегда привязан к какому-то бизнесу (если это, конечно, не организация типа «Гринпис», хотя и тут есть варианты), и этот бизнес оказывает абонентам услуги. То есть брендовые MVNO будут также использовать конвергентный эффект, только в предыдущем примере аббревиатура FMC будет расшифровываться не как Fixed-Mobile Convergence, а как Football-Mobile Convergence, когда абонент сотовой сети получает бесплатные билеты на футбол.

По большому счету, «игроки с тарифами» и «бренды» являются наиболее простыми воплощениями MVNO. Более интересными с точки зрения организации представляются виртуальные операторы, работающие по рекламной модели, операторы — поставщики дополнительных услуг, а также операторы туристических SIM-карт. Конкурентным преимуществом таких MVNO является их специализация на определенных видах деятельности, в которых «большому» оператору сложно проявить сопоставимую эффективность.

Операторы, работающие по рекламной модели, используют такие сервисы, как sponsored call, sponsored SMS/ MMS, а также, в некоторых случаях, sponsored Internet (когда реклама встраивается в содержимое Web-страниц или происходит переадресация на ресурс рекламодателя) для частичной или полной компенсации стоимости услуг связи. Эффективная работа с рекламодателями и привлечение соответствующей абонентской базы является нетривиальной задачей даже для крупного оператора, поэтому перспективы специализирующихся на работе с рекламой MVNO видятся авторам в достаточной степени обоснованными.

Аналогичные рассуждения относятся и к виртуальным операторам, предоставляющим дополнительные услуги, например доступ к библиотекам видео- или аудиоконтента. Что касается операторов туристических SIM-карт, то успешность этого вида бизнеса уже доказана на практике — действующие MVNO, базирующиеся преимущественно в Прибалтике, регулярно отчитываются о росте абонентской базы. На данном направлении, вероятно, могут быть сильны обладающие сотовыми активами зарубежные инвесторы.

Опыт реализации компанией «НТЦ ПРОТЕЙ» нескольких проектов по построению инфраструктуры MVNO (к сожалению, за рубежом) позволяет сделать вывод о том, что несмотря на разницу в бизнес-моделях все типы виртуалов, кроме разве что «брендов», объединяет приоритетность работы в режиме full-MVNO, то есть с использованием собственных MSC, HLR и биллинга, в отличие от «облегченной» версии MVNO, при которой задействуются мощности соответствующих подсистем присоединяющего оператора.

В первую очередь это относится к эксплуатации биллинга и организации маршрутизации. Наличие отдельного биллинга, позволяющего управлять тарифами без оглядки на MNO, представляется критическим условием успеха компании, направленной на сегментирование абонентов и динамично реагирующей на изменение ситуации на рынке. При этом возможности биллинга не имеют значения в отсутствие соответствующего тарификационного функционала системы коммутации, которая, таким образом, также должна быть максимально независимой от инфраструктуры MNO.

Гибкие возможности тарификации и маршрутизации играют существенную роль и в деятельности операторов туристических SIM-карт, для которых модель full-MVNO более удобна при организа-

ции взаимодействия с роуминговыми партнерами. Для рекламных и контентных операторов возможность запускать VAS-платформы и формировать системы бонусов без необходимости реконфигурации оборудования MNO также видится важным фактором успеха.

Особняком в представленной классификации стоит группа виртуальных операторов, создаваемых специально под обслуживание госструктур и крупных компаний. Вопрос работы таких операторов в режиме full-MVNO, то есть в режиме, максимально независимом от присоединяющего оператора, стоит в этом случае даже более остро по целому ряду причин.

Во-первых, огромный штат сотрудников крупных компаний (вспомним, к примеру, РЖД), объединенных в разнородные структурные единицы, будет постоянным источником требований по организации сервисов и управлению абонентами, таких как настройка голосовых и SMS-уведомлений, конфигурация закрытых групп нумерации, применение политики обслуживания в зависимости от подразделения, изменение профиля абонента и доступных ему услуг при изменении должности, закрытие учетных записей уволенных работников и многое-многое другое. В режиме «облегченного» MVNO реализация непрерывного потока задач будет замедляться издержками по согласованию работ с сотрудниками владельца инфраструктуры, а иногда и намеренно саботироваться последними.

Во-вторых, крупные компании, работая в режиме full-MVNO, минимизируют количество информации, оседающей в хранилищах оператора — владельца инфраструктуры. В свете недавних случаев раскрытия секретных данных этот вопрос становится все более актуальным. Причем раскрытие персональных данных абонентов «брендового» виртуального оператора по понятным причинам не идет ни в какое сравнение с раскрытием информации оборонной компании или силовиков. Теоретически, по настоянию виртуального оператора MNO может выполнить перенастройку своего оборудования и запретить сохранять те или иные виды информационного обмена для группы абонентов, но это, во-первых, сложно для самого оператора, а во-вторых, не дает полной уверенности в невозможности утечки. Работа на выделенных сетевых элементах в данной ситуации представляется наиболее разумным решением, к примеру, использование «своего» SMSC и защищенного сайта, с которого можно отправить сообщения, гарантирует, что MNO не будет хранить SMS-переписку и она не будет в дальнейшем просмотрена конкурентами. Понятно, что организация дополнительных средств защиты информации от перехвата в максимально независимой от MNO сети осуществляется проще, и степень защиты в этом случае получается выше.

Третьей причиной преимущества максимально независимой схемы функционирования является то, что MNO свойственно обновлять и наращивать существующее оборудование. Но, как известно практически каждому специалисту, хотя бы раз сталкивавшемуся с заменой/расширением систем с широким функционалом, такие проекты не проходят без полномасштабного согласования со всеми заинтересованными подразделениями (биллинг, коммутация, коммерсанты и т.п.), в число которых будут тем чаще входить структуры MVNO, чем выше будет степень его интеграции с невиртуалом. С учетом существенного отличия абонентской базы обоих участников симбиоза весьма вероятно, что требования к обновляемой системе также будут разниться, многократно усложняя задачу модернизации оборудования. Фактически, в указанной ситуации закупкой будут заниматься два оператора вместо одного, и число согласований, необходимых для выбора удовлетворяющей потребностям обоих новой системы может также удвоиться. При этом сотрудничество MNO — публичной компании и виртуального оператора, представляющего интересы компании с госучастием, часть акций которой при этом, возможно, контролируется миноритариями, потенциально может стать почвой для конфликта интересов и на управленческом уровне. Увеличение количества сторон, влияющих на политику компании, представляет собой дополнительный риск для MNO, и необходимость учитывать этот риск, скорее всего, породит дополнительные издержки.

За последние несколько лет обсуждений перспектив запуска MVNO в России приведенная в этой небольшой статье аргументация в той или иной форме уже выносилась на суд читателей. Не претендуя на оригинальность, авторы надеются, что вопрос с распределением номерной емкости в ближайшем будущем благополучно разрешится, и участники рынка реализуют свои амбиции ко всеобщей выгоде и на благо абонентов, прервав поток теоретических выкладок отчетами об успешных результатах деятельности компаний. ■

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

## виртуальных инфраструктур в телекоме

***Олег ГЛЕБОВ,***
*специалист департамента маркетинга компании «Информзащита»*

**В российских телекоммуникационных компаниях, которые вплотную подходят к эре облачных технологий, виртуализация применяется давно и успешно. Наибольший рост ее использования был отмечен в кризисный период. Такой подход помог достичь необходимого уровня экономии и перераспределения существующих мощностей.**

По оценкам специалистов, до 80% ресурсов компаний до виртуализации вообще не использовались. Одним из первых примеров успешного использования виртуализации в телекомах стала технология виртуальных АТС. В виде покупаемой услуги предлагалось развертывание виртуальной машины с АТС либо на собственном сервере компании, либо в дата-центре оператора. Данный продукт положительно зарекомендовал себя как простая в настройке и установке замена массивным стационарным АТС.

Первым же примером комплексного использования виртуализации стала аренда инфраструктуры. С конца 2000 года была распространена модель, когда бизнес телекоммуникационной компании основывался на мощностях более крупного оператора. Достаточно вспомнить компанию «Корбина телеком», которая арендовала инфраструктуру у «ВымпелКома» и выступала в виде мобильного оператора виртуальных сетей.

Отдельно стоит сказать о собственных виртуальных фермах серверов телекоммуникационной компании. Простота и удобство масштабирования мощностей и сетей быстро позволили объединить распределенные сегменты филиальной сети в единую среду. Данное направление развития компании становится сегодня успешным плацдармом при переходе к облачной модели. С одной стороны, компания имеет возможность еще более централизовать управление собственной сетью через приватное облако. С другой — это становится бизнес-кейсом для клиентов, которые готовы покупать доступ к публичным облакам, услугам облачного ПО или облачных средств обеспечения безопасности.

Вопросы обеспечения информационной безопасности сегодня уже неотделимы от построения виртуальной среды. Если на начальном этапе внедрения такой технологии до 80% проектов не привлекали даже специалистов по информационной безопасности, то теперь обеспечение безопасности носит обязательный характер, и средства ее обеспечения, появляющиеся на рынке, привлекают большое внимание пользователей. Не стоит забывать, что задачи защиты являются важным фактором при переходе компаний на виртуальные инфраструктуры. Финансовые затраты компаний на обеспечение безопасности, отказоустойчивости и катастроф устойчивости можно оценить. Поддержка текущей ИБ-инфраструктуры и ее модернизация со временем, обучение специалистов и их заработная плата, а также аренда дополнительных

площадей, например, для территориально разнесенного резервного копирования — все это выливается в колоссальные затраты.

Виртуализация приходит на помощь компаниям, готовым все это арендовать у телекомоператора, который давно использует аналогичные средства для собственных нужд. Внедренная виртуальная инфраструктура для телекома дает большую компетенцию и настроенные средства обеспечения безопасности, что позволяет предлагать аналогичные проекты в виде услуги для клиентов. По оценкам аналитиков, для крупной компании внедрение и построение собственной ИБ-инфраструктуры может быть сравнимо по цене с 18—20-летним сроком аренды аналогичной по уровню безопасности среды у оператора.

Не стоит расценивать виртуальные среды как полный аналог физических сред. Переняв все аспекты защиты от реальных инфраструктур, виртуальные привносят целый спектр очень специфических задач по обеспечению защиты. Если говорить о комплексном подходе в вопросе оценки безопасности такой среды, то можно выделить целый ряд очевидных уязвимостей:

- уязвимость аутентификации ресурсов и пользователей;
- SQL-инъекции;
- небезопасное хранение данных;
- cross site scripting;
- уязвимость контроля доступа;
- эскалация привилегий;
- отказ в обслуживании DDoS (внутренний и внешний);
- блокировка подлинного пользователя системами обеспечения ИБ;
- шифрование хранилища данных;
- сетевое проникновение;
- перехват сессии;
- безопасность передачи данных.

Перечисленные уязвимости влекут за собой реализуемые на их основе атаки на виртуальную инфраструктуру. Достаточно перечислить самые распространенные виды атак, которые уже имеют место в реальности. Возможность кражи или подмены данных в процессе обеспечения резервного копирования, так как передача информации происходит в виртуальной сети и в незашифрованном виде. Аналогичный метод атаки может быть применен и просто в отношении курсирующего в виртуальной сети трафика с данными.

Довольно сложно представить себе ситуацию кражи всей операционной системы с реального компьютера, количество файлов которой достаточно велико. В виртуальной среде это всего лишь один большой файл-образ, который может быть выкачан полностью со всеми данными и настройками. Одним из наиболее частых методов атаки является подключение к работающей инфраструктуре виртуальной машины с уже внедренным в нее вредоносным кодом (вирусом или руткитом). Большинство средств обеспечения безопасности не смогут выявить такую атаку «на лету». К моменту обнаружения атаки может быть заражено значительное количество виртуальных машин в сети.

Опасность атаки также может быть связана со штатными работами сети, поскольку в момент вынужденного восстановления виртуальной машины может создаться уязвимая точка. Процесс восстановления связан с подключением клона выведенной из строя виртуальной машины, но клон обычно отстает от прародителя на несколько месяцев. Естественно, что в такой ситуации клон не имеет всех обновлений безопасности, которые вышли с момента его создания. У злоумышленников появляется возможность выявления такой дыры в защите с применением средств стандартного анализа перебором известных уязвимостей из базы. Воспользовавшись одной из таких уязвимостей, хакер может получить доступ не только к виртуальной машине, но и ко всей сети, и скомпрометировать ее. Нередко в виде атакуемой цели выступает даже не сама виртуальная среда, а внешние хранилища данных SAN/NAS, в которых размещены сетевые папки пользователей. Так как хранение на них производится без использования шифрования или других средств контроля, то возможно заражение файлов. Это повлечет за собой вероятность дальнейшего распространения атаки уже на саму сеть и виртуальные машины.

Слабым звеном в безопасности любой виртуальной среды является отсутствие тесной связи между виртуальными машинами и политиками безопасности. Несложно представить себе такую ситуацию, когда в сеть подключается виртуальная машина со всеми обновлениями безопасности, но при этом без соответствующих политик. Данная уязвимость очень часто происходит в момент миграции виртуальной машины из одной сети в другую или между физическими серверами. Перенос происходит лишь ОС и данных, при этом политики безопасности не переносятся. Это может повлечь за собой появление слабого звена в сетевой защите.

Самыми опасными и деструктивными атаками можно назвать те, которые направлены на перехват контроля или вывод из строя гипервизора сервера. При этом такая атака может быть реализована как из

отдельной подконтрольной гипервизору виртуальной машины, так и напрямую из внешней среды, и даже на физическом уровне. Проблематика тесного и неразрывного общения в рамках одной виртуальной среды также выделяет возможность реализации атаки одной виртуальной машины из другой посредством общих папок или непосредственно через сеть передачи данных. Выявления таких атак затруднено, в том числе и в связи с тем, что нелегитимный трафик не покидает пределов физического сервера. Поэтому классические средства сетевой безопасности будут бессильны что-либо выявить и заблокировать.

Реализуемые атаки позволяют выделить основные задачи обеспечения информационной безопасности виртуальной среды: контроль доступа к гипервизору, разграничение каналов обмена данными между виртуальными машинами, базовая авторизация пользователей и аутентификация ресурсов. Важным фактором является мониторинг информации при ее передаче и хранении, а также контроль инициализации элементов инфраструктуры. Администраторам безопасности необходимо иметь эффективные средства управления конфигурациями виртуальных машин, средств виртуализации и виртуальных сетевых адаптеров. Таким образом, необходимо не только правильно настраивать элементы в сети, но и контролировать процесс дальнейшего изменения настроек. Обеспечение защиты от направленных атак против гипервизора на физическом и сетевом уровнях должно дополнить картину комплексного подхода к информационной безопасности со стороны компании.

Практические аспекты реализации безопасности виртуальных сред подразумевают целый ряд мер. Основной момент защиты — это блокировка угроз и атак на уровне виртуальных сетей, которые являются основой построения инфраструктуры. Для этих целей должны использоваться специализированные средства, разработанные под специфику виртуальных адаптеров и каналов передачи, ведь зачастую трафик между отдельными точками даже не покидает пределов одной физической машины. Важным моментом в подходе к защите виртуальной среды является обеспечение защиты каждого виртуального объекта на уровне не менее чем физического сервера, но с учетом дополнительных угроз и специфики виртуализации.

Безопасность всей виртуальной инфраструктуры также неразрывно связана с непрерывным отслеживанием состояния виртуальных машин, их обновлением и контролем процесса обновления. В любой момент времени системный администратор инфраструктуры и администратор безопасности должны иметь средства проверки состояния любой из виртуальных машин. При работе в виртуальной среде компании необходимо вносить изменения в глобальные политики доступа и безопасности так, чтобы использовались и учитывались аспекты виртуализации.

Опыт обеспечения безопасности виртуальных сред показывает, что есть список методов и рекомендаций, которыми следует прежде всего воспользоваться архитекторам информационной безопасности. Эти меры направлены на обеспечение максимальной безопасности без использования чрезмерных средств защиты, что позволяет компенсировать затраты на конечный проект по ИБ.

В первую очередь нужно обеспечить усиленную аутентификацию администраторов инфраструктуры и администраторов информационной безопасности. Стоит заметить, что приоритетным должно быть разделение этих ролей между несколькими сотрудниками. Для защиты средств управления (гипервизора) необходимо иметь сертифицированные решения защиты от НСД. Необходимо также уделять внимание защите от НСД самих ESX-серверов как единой точки отказа всей среды.

Разграничение пользователей необходимо строить на мандатном управлении доступа к виртуальной среде. Защита виртуальных машин должна обеспечиваться средствами контроля целостности конфигурации и доверенной загрузки. Для защиты конфиденциальной информации важно разграничение и контроль доступа администраторов к данным виртуальных машин.

Важно обеспечивать автоматическую и постоянную регистрацию событий, связанных с информационной безопасностью, для последующего аудита или расследований инцидентов. Следующим аспектом становится контроль целостности и доверенная загрузка самих ESX-серверов, что позволит избежать модификации или заражения.

Сами средства защиты должны иметь элементы контроля целостности и защиты от НСД. Данный фактор очень важен, ведь зачастую даже правильно настроенные системы защиты могут быть сами атакованы различными средствами. Основой предлагаемой модели защиты становятся обязательные средства централизованного управления всеми элементами управления, защиты и администрирования и их постоянный мониторинг. ■

# ФОРУМ ПО СПУТНИКОВОЙ НАВИГАЦИИ

*Леонтий БУКШТЕЙН*

В Москве прошел юбилейный, V Международный форум по спутниковой навигации. Открывая форум, вице-премьер Правительства РФ Сергей Иванов заявил, что «сегодня Россия способна в полном объеме обеспечить свой навигационный суверенитет и гарантировать, что навигационный сигнал системы ГЛОНАСС будет предоставляться бесплатно и на всей территории земного шара». Он также подчеркнул необходимость «коммерциализации системы на основе государственно-частного партнерства со значительным преобладанием доли частного капитала». Вслед за вице-премьером перед участниками форума выступил председатель Комитета Государственной думы по информационной политике, информационным технологиям и связи Сергей Железняк, огласивший приветственное слово председателя Госдумы Бориса Грызлова.

На пленарном заседании с докладами выступили российские и зарубежные эксперты: Анатолий Шилов, заместитель руководителя Федерального космического агентства; Валерий Субботин, первый заместитель генерального директора — генерального конструктора ОАО «Российские космические системы»; Александр Гурко, генеральный директор ОАО «НИС», Федерального сетевого оператора; Рэй Клор, старший советник по вопросам ГНСС Государственного департамента США; Валерий Бабаков, главный конструктор навигационной аппаратуры потребителей ПВО «Алмаз Антей» и др.

Главной темой форума и, в частности, пресс-конференции по итогам пленарного заседания стала коммерциализация ГЛОНАСС в России и за рубежом. По словам Анатолия Шилова, «реализация программы развития ГЛОНАСС идет по плану и является абсолютно прозрачной для потребителей». Сейчас завершается разработка концепции программы на период до 2020 года, направленной на создание «массовой аппаратуры».

Говоря о динамике производства потребительских устройств ГЛОНАСС, Александр Гурко заявил, что в 2011 году будет произведено 500 тыс. модулей ГЛОНАСС, это превысит объем выпуска 2010 года в пять раз, а объем 2009 года — более чем в 16 раз. Как сообщил Евгений Шмелев, вице-президент по техническому развитию ОАО «АВТОВАЗ», завод уже начал серийное производство автомобилей «Лада-Калина» и «Лада-Приора» со встроенными ГЛОНАСС-навигаторами.

При этом Валерий Бабаков считает необходимым создание «механизмов борьбы с демпингом и защиты отечественных производителей навигационной аппаратуры».

Все докладчики отметили большие перспективы развития ГЛОНАСС как в регионах России, так и за рубежом. В частности, в рамках программы формирования сети региональных партнеров НИС-ГЛОНАСС, о которой ОАО «НИС» объявило в начале 2011 года, уже отобрано 30 из 150 поданных заявок на сотрудничество.

Говоря о международном сотрудничестве, Александр Гурко назвал Индию, Латинскую Америку, Ближний Восток и страны СНГ «приоритетными рынками с точки зрения коммерциализации ГЛОНАСС». По его словам, некоторые мировые разработчики навигационного оборудования уже объявили о своих планах на разработку устройств, поддерживающих ГЛОНАСС.

Как сказал Рэй Клор, США хотят развивать международное сотрудничество с Россией: «Америка поощряет всемирное использование системы GPS, а российская система ГЛОНАСС сейчас также активно развивается, и мы хотим продолжать нашу кооперацию».

В свою очередь, Анатолий Шилов отметил, что двумя ключевыми направлениями работы с зарубежными партнерами является, во-первых, увеличение числа наземных спутниковых станций ГЛОНАСС по всему миру в целях повышения точности сигнала и, во-вторых, предоставление навигационных услуг странам, не имеющим собственных спутниковых систем.

По оценкам исполнительного вице-президента NAVTEQ Map Клиффа Фокса, «ГЛОНАСС имеет

хорошие возможности развития за рубежом, особенно в Индии».

После пленарного заседания состоялась церемония вручения премии Ассоциации «ГЛОНАСС/ГНСС Форум» в области навигации по двум номинациям: «За вклад в создание и развитие системы ГЛОНАСС» и «За внедрение технологий на базе системы ГЛОНАСС».

Одновременно с форумом прошла специализированная международная выставка «Навитех-Экспо-2011», на которой ведущие российские и зарубежные компании представили свои достижения в области разработки и производства навигационного оборудования и периферийных систем.

В последний день работы форума наш корреспондент побеседовал с директором по развитию бизнеса компании NAVTEQ, выступившей, кстати, серебряным спонсором форума, Павлом Козловым:

**— Если анализировать последние два очень непростых года, что можно сказать об отрасли, в которой работает компания?**

— Мы ведь говорим о локации, и мы видим, что решения становятся шире, дистанции — больше. У людей растут потребности в анализе данных, которые привязаны к карте. Все сильнее проявляется необходимость получать данные с карты. Поэтому и развиваются разнообразные сервисы, в том числе и картографические. Какие тенденции мы видим? Прежде всего, рост технологий и преобразование самих карт. Они превращаются из плоских «дорога — город» в трехмерные модели. И на форуме говорили о том, что у нас есть методики, которые позволяют делать такие карты. И это не наши фантазии — такие требование выдвигают клиенты, пользователи, партнеры по бизнесу. Еще одна тенденция — это проникновение локации, навигации в различные классы мобильных устройств. Опция востребована, пользователи требуют, чтобы такой сервис «на борту» коммуникатора и мобильного телефона обязательно был. Третья тенденция, которую мы замечаем, это то, что и потребители, и правительство начинают видеть роль навигации в экологии — так называемый «зеленый эффект». Мы проводили исследование, которое показало, что использование навигации может помочь сэкономить до 15% расходов на топливо для автомобильного транспорта. Это благодаря тому, что сокращается холостой пробег машин, практически исключается поиск нужного здания в городе путем плутания по неизвестным улицам и закоулкам. А на междугородной трассе — благодаря выбору оптимального маршрута. В перспективе, с появлением электромобилей, пробег которых от одной зарядки аккумуляторов еще не так велик, навигатор — условие правильного расчета пробега, безостановочного движения, рационального выбора маршрутов с учетом заправок. Еще одна тенденция — это появление на рынке систем низкого ценового уровня, что позволяет ставить их на недорогие автомобили и сделать навигацию еще доступней для рядового пользователя. Все это вкупе порождает большую заинтересованность операторов мобильной связи, и у нас есть ряд сделок в Европе и в России, показывающих, что рынок на подъеме. Я это говорю не по личным ощущениям — мы проводим исследования среди потребителей и судим о тенденциях на основании полученных результатов.


**— То есть вы целиком подвластны вкусам и желаниям потребителей?**

— Я бы так не сказал. Все чаще, особенно в высокотехнологичных сегментах, мы видим, что потребитель даже не представляет, что мы ему можем предложить. Но когда мы предлагаем новинку, он, потребитель, чаще всего хватается за нее с большим удовольствием. У нас есть целое подразделение, разрабатывающее инновационные проекты. Мы уверены, что потребителям результаты его работы понравятся.


*Сергей Иванов*

**— Как вы оцениваете ГЛОНАСС-форум?**

— Это уже пятый форум по спутниковой навигации, в котором мы принимаем участие. Конечно, налицо тенденции к развитию. Руководство страны проявляет большой интерес к данной теме, это видно и по представительству органов законодательной и исполнительной власти. Да и от нашей компании впервые был исполнительный вице-президент, второй человек в компании, человек, который управляет картографической деятельностью компании по всему миру — Клифф Фокс. Он привез, что называется, новость дня: компания приняла решение в 2012 году привезти в Россию четыре автомобиля по сбору данных для картографирования и навигации в РФ. Такую работу компания начала с Северной Америки, затем была Европа, и то, что теперь наступил черед России, говорит о том, что она у нас в списках первоочередных приоритетов. Сам проект с использованием этих машин очень недешев и в стране с развивающейся рыночной экономикой будет реализован впервые. Интерес к будущим результатам его реализации есть и у государства, и у коммерческих компаний.

**— В чем его специфика?**

— Он позволяет автоматизировать сбор данных. Причем речь идет не только о дорогах непосредственно, но и обо всех объектах инфраструктуры вдоль этих дорог на расстоянии 200—300 м от них. Это открывает новые и зачастую неожиданные рынки для картографии, потому что речь идет об обогащении детализации, углублении отображения атрибутов. Компанию теперь можно назвать складом геолокационной навигационной продукции: берем обыкновенную карту и, используя информационные технологии, делаем ее цифровым продуктом.

**— Какой будет нагрузка на каждый из четырех комплексов?**

— Сейчас у нас в базе 2 млн 400 тыс. км дорог России. Вот так можно просчитать проектную нагрузку. Эти машины проедут и просканируют все основные городские улицы и дороги.

**— Какой вы видите перспективу работы по локации с использованием спутниковой навигации?**

— У нас на сегодня верифицировано, то есть пройдено нашими специалистами, 750 тыс. км дорог. Эту работу нужно завершить, на нее уйдет еще несколько лет. Второе — это борьба с пробками путем предоставления необходимой информации для водителей. Такой продукт, выпущенный нами, уже доступен для пользователей. Мы разрабатываем виртуальные 3D-развязки, что при наличии развязок на разных уровнях совершенно необходимо водителям. Много еще предстоит поработать с адресной базой данных, чтобы гражданин страны с навигатором мог доехать по нашим картам до любого города, поселка, деревни. Тут еще есть над чем работать. А в перспективе будем переводить «плоские» электронные карты в объемные.

Еще одна новая работа, которая уже ведется в США, это картографирование помещений. Сейчас много высотных зданий, бизнес-центров, культурно-развлекательных комплексов, разобраться в которых новому посетителю очень непросто. И чтобы добраться до нужного помещения, бутика, офиса, нужна внутренняя навигация. Тут, конечно, есть проблема проникновения сигнала со спутника, но она решаемая. В Барселоне в этом году мы уже показывали такую систему, и она работала устойчиво, реагируя на перемещения мобильного телефона начиная с 20 см.

Вообще же наша задача — создавать тот фундамент, на котором можно будет строить новые услуги и сервисы. ■

# Cisco Cius — первая экосистема приложений корпоративного класса для планшетных компьютеров

**Во время очередной конференции CiscoLive! в Лас-Вегасе (Невада, США) был представлен первый планшет корпоративного класса Cisco Cius и экосистема приложений для него. Из Лас-Вегаса сообщает наш специальный корреспондент Александр Семенов.**

По мнению разработчиков, Cisco Cius изменит представление заказчиков о мобильности и рабочем месте. В Лас-Вегасе компания Cisco анонсировала AppHQ — прикладную экосистему, специально созданную для планшетных компьютеров Cisco CiusTM. Это открывает новые возможности для разработки, использования и быстрого внедрения планшетных приложений на предприятии. Cisco Cius, единственный на сегодня беспроводной планшетный компьютер, специально созданный для корпоративных пользователей, работает под управлением операционной системы Android и поддерживает функции передачи голоса и видео, совместной работы и виртуализации лучше любого другого планшетника, доступного ныне на рынке.

Cisco Cius представляет собой оптимизированный планшетный компьютер с функциями безопасности корпоративного класса, используемый как естественное расширение корпоративной сети. Устройство предоставляет пользователям мобильность, централизованное управление, возможность создания виртуального контента и вычислительные функции вместе с полным набором приложений для совместной работы.

AppHQ предлагает разработчикам инструментальные средства и ресурсы для создания, тестирования и вывода приложений для Cisco Cius на рынок, а ИТ-менеджерам позволяет определять, какие именно приложения могут использоваться на корпоративных устройствах. Кроме того, компании могут создавать своеобразные «витрины», где сотрудники могут находить, выкладывать и добывать приложения, дополняющие их личную деловую среду.

Компании CDW, Nervecentre Software, Verizon, госпитали Ноттингемского университета, здравоохранительная организация Palomar Pomerado Health, университет Wisconsin-Whitewater — вот лишь некоторые из заказчиков, чьи сотрудники используют Cisco Cius. На специальной презентации в Лас-Вегасе они поделились с представителями СМИ своими впечатлениями от нового планшета.

Cisco AppHQ — надежный источник корпоративных приложений — представляет собой отлично защищенную облачную «витрину», где конечные пользователи и ИТ-менеджеры могут найти функции и возможности, недоступные другим онлайновым магазинам приложений.

Перечислим некоторые из этих возможностей.

• Тестирование и оценка. ИТ-менеджеры хотят знать, какие из приложений, установленных в корпоративной среде, действительно нужны предприятию. Cisco AppHQ предоставляет ИТ-менеджерам и конечным пользователям «доверенный источник» приложений, гарантируя, что каждое приложение AppHQ прошло строгий контроль компании Cisco и разработано либо специалистами Cisco, либо партнерами по разработке приложений для ОС Android, либо пользователями самого предприятия. Процесс оценки включает тестирование на совместимость приложений и типовых конфигураций аппаратного устройства.

• Store-within-a-Store (магазин в магазине). В среде AppHQ предприятие получает от Cisco на правах хостинга отлично защищенный частный магазин приложений. Заказчик может настроить его на свои требования, включая использование правил корпоративного брендинга, логотипов, иконок и цветовых гамм. Кроме того, «магазин в магазине» создает платформу, позволяющую эффективно внедрять приложения на предприятии. К примеру, финансовая организа-

ция может выбрать приложения для управления кадрами или начисления зарплаты и автоматически установить их на устройствах лишь тех пользователей, кому данные приложения нужны для выполнения служебных обязанностей.

• Новые возможности ИТ-менеджеров. AppHQ Manager™ позволяет ИТ-отделу разрешать либо запрещать доступ к магазинам приложений тем или иным сотрудникам в зависимости от их должностей и используемых устройств.

Кроме того, ИТ-отдел может предоставлять или блокировать доступ к приложениям для устройств определенного типа, принадлежности или категории.

Эти уникальные возможности позволяют ИТ-отделам устанавливать оптимальное соотношение между свободой действий сотрудника, корпоративными правилами и экономичностью.

### Дополнительные сведения о Cisco AppHQ и Cisco Cius

В экосистему AppHQ будут входить отобранные компанией Cisco лучшие в отрасли корпоративные и пользовательские приложения, тесно интегрированные с решениями Cisco для совместной работы. Кроме того, в экосистему войдут проверенные приложения B2B и B2C от партнеров разработчиков. Cisco будет постоянно пополнять среду AppHQ новыми приложениями с учетом требований заказчиков. Кроме того, ИТ-менеджеры смогут выбирать любое из 200 тыс. приложений на рынке Android Marketplace.

Удобный пользовательский интерфейс Cisco AppHQ позволяет легко находить и устанавливать приложения, а также давать оценки их работе с комментариями. С помощью этого интерфейса пользователь может найти информацию о приложении (автор, дата публикации и т.д.), установить его и классифицировать по таким признакам, как частота обращений, новизна и т.п. Планшетный компьютер Cisco Cius предоставляет интегрированный доступ к полному ассортименту приложений Cisco® для совместной работы, таких как приложения для конференций Cisco WebEx®, социальные приложения Cisco Quad™, системы обмена сообщениями Cisco Jabber® и Cisco TelePresence™.

Устройство Cisco Cius должно стать доступным для заказа во всех странах с 31 июля 2011 года. Его стоимость не должна превышать $750. При этом Cisco делает специальное предложение Triple V, в рамках которого Cisco Cius можно будет приобрести по цене ниже $700. Базовый доступ к среде Cisco AppHQ будет по умолчанию поддерживаться на всех устройствах Cisco Cius.

Вместе с Cisco Cius заказчики получают гарантии корпоративного класса и единую точку для обращения за технической поддержкой. В случае необходимости отказавшие компоненты можно будет заменить в течение одних суток. Кроме того, сервисный отдел Cisco предлагает предприятиям годовую, двухлетнюю или трехлетнюю гарантию в зависимости от пожеланий заказчика.

По словам старшего вице-президента компании Cisco Барри О'Салливана (Barry O'Sullivan, возглавляет подразделение коммуникаций и совместной работы), «Cisco — лучший в мире поставщик решений telepresence и оконечных устройств для телефонной связи. Планшетный компьютер Cisco Cius и экосистема AppHQ укрепляют лидерство Cisco в области сетевой совместной работы, делая такую работу более мобильной, безопасной и управляемой».

«Мы стали первой системой здравоохранения, разработавшей собственные приложения для Cisco Cius, — заявил Орландо Портале (Orlando Portale), главный директор по инновациям в системе здравоохранения Palomar Pomerado Health. — Мы хотели повысить мотивацию медицинских работников и качество обслуживания пациентов с помощью более качественного средства совместной

работы, предоставляющего врачам доступ к данным в реальном времени независимо от местоположения. В результате врачи получили возможность своевременно принимать необходимые решения. Наше приложение MIAA (Medication Information, Anytime, Anywhere — медицинская информация в любом месте в любое время) не только собирает по требованию данные об историях болезни из разных источников, но и позволяет врачам консультировать друг друга по электронной почте и каналам видеоконференц-связи. При этом на экраны пользовательских устройств выводится одна и та же информация о пациенте. Мы выбрали Cisco Cius, потому что это устройство сочетает гибкость платформы Android с информационной безопасностью и виртуализацией корпоративного класса. Кроме того, это решение поддерживает важные функции совместной работы, в том числе видео высокого разрешения».

Майк Смит (Mike Smith, вице-президент компании Verizon, отвечающий за корпоративные коммуникации, сети и мобильность) считает, что «возможность ускоренного принятия решений в распределенном режиме с помощью мобильных унифицированных коммуникаций и совместной работы становится реальной с появлением "умных" сетей 4G LTE, облачных вычислений и новых корпоративных устройств, таких как Cisco Cius. Наши продавцы и заказчики получат все преимущества облачных корпоративных приложений, позволяющих выполнять служебные обязанности практически в любом месте, использовать функции совместной работы и быстрее обслуживать клиентов».

«Одна из главных задач нашего вуза, — отмечает главный ИТ-директор университета Wisconsin-Whitewater Елена Покот (Elena Pokot), — подготовка студентов к работе в сложной, разнообразной, непрерывно меняющейся среде XXI века. Оснащение преподавателей и студентов планшетными компьютерами Cisco Cius, поддерживающими видео высокого разрешения и интегрированными с Cisco WebEx, позволило нам повысить качество коммуникаций, снизить зависимость пользователей от местоположения и перейти к принципу "виртуального присутствия". Использование этих возможностей для подготовки студентов позволяет существенно улучшить процессы совместной работы. Это особенно важно для развития коммуникативных навыков студента, который получает возможность пользоваться языком мимики и жестов и проводить визуальную оценку своих собеседников».

«Супервайзеры колл-центров, — говорит менеджер по новым технологиям из компании CDW Кен Сайдер (Ken Snyder), — должны быть в любой момент доступны для операторов и в любой момент быть готовы предоставить оператору самую свежую информацию о производительности и работе колл-центра. При этом по характеру своей работы супервайзер не может быть привязан к рабочему столу. Наша компания разработала приложение для Cisco Cius, расширяющее возможности мобильной информационной панели CDW Mobile Wall Board и поднимающее эффективность и производительность нашего колл-центра на качественно новый уровень. Это приложение предоставляет всем супервайзерам колл-центра мгновенный доступ к оперативным данным и ключевым индикаторам производительности, что позволяет быстро принимать решения и исправлять ситуацию, повышать скорость реакции операторов и пользоваться удобным коммуникационным устройством, поддерживающим все необходимые функции, включая видеосвязь и учет присутствия».

«VMware и Cisco делают все возможное для разработки полномасштабных решений, ориентированных на конечного пользователя, — отметил вице-президент компании VMware по вопросам пользовательских вычислений Витторио Виаренго (Vittorio Viarengo). — Эти решения расширяют возможности работы (в том числе совместной), позволяя сотрудникам находиться где угодно — в офисе, дома, в дороге. Решения VMware View™ и Cisco Cius предоставляют компаниям любого размера лучшее в своем классе виртуальное рабочее пространство, включающее гибкие, хорошо защищенные виртуальные настольные системы с унифицированными коммуникациями, предназначенные для поддержки многофункционального мультимедийного контента и универсального доступа к корпоративным приложениям и данным».

«Новые планшетные компьютеры, такие как Cisco Cius, служат ярким примером распространения пользовательских технологий на предприятиях, — подчеркнул вице-президент, генеральный менеджер отдела пользовательских услуг компании Citrix Сумит Дхаван (Sumit Dhawan). — Citrix тесно сотрудничает с Cisco, совмещая системы виртуализации и мобильной совместной работы Citrix Receiver с планшетными компьютерами Cisco Cius, чтобы предоставить конечным пользователям и ИТ-специалистам все преимущества этого нового уникального устройства». ■

# IP-SUMMER 2011:

## обзор наиболее значимых интернет-правовых событий этого лета

***Павел КАТКОВ,***
*директор юридического департамента «Система Масс-медиа» (АФК «Система»), член Ассоциации юристов России*

**Лето, казалось бы, обещало принести некоторое затишье, которого, однако, не случилось: правовая публичная активность в июне — августе не уступает более «оживленным» временам года. Насыщенность событий такова, что буду вынужден писать обо всем коротко, благо заинтересованные люди всегда могут уточнить детали.**

Важным прецедентом стало, например, применение со стороны МВД меры, предусмотренной статьей 13 Федерального закона «О полиции», на основании которой ведомство вправе вносить обязательные для исполнения руководителями и должностными лицами организаций представления об устранении причин и условий, способствующих реализации угроз безопасности граждан и общественной безопасности, совершению преступлений и административных правонарушений. Блокировка (точнее, временное приостановление делегирования) интернет-сайтов не является чем-то новым: достаточно вспомнить известное постановление органов прокуратуры относительно сайта torrents.ru. И тем не менее прецедент показательный: впервые в России подобное административное решение претворяется в жизнь в подобном — массовом и последовательном порядке.

Не меньший интерес вызывает поведение социальной сети «ВКонтакте», а именно случай с предоставлением IP-адресов пользователей в связи с иском компании Gala Records. Нет, сам факт предоставления не является редкостью. Интересно другое: как подобная позиция сочетается с заявлениями многих интернет-площадок о «свободе Интернета», «заботе о пользователях» и других подобных вещах. Если это позиция вида «до первого иска» то, похоже, дела правообладателей не так уж и плохи.

Забавно наблюдать за судьбой открытых лицензий, а особенно за той трактовкой, которую им дают некоторые «эксперты». Особый интерес лично у меня вызывает мнение, что без creative commons невозможно свободное распространение аудиовизуального контента — что, конечно же, неправда. Я уже высказывался по этому вопросу в прошлых номерах рубрики и вынужден повторить: правообладатель имел и, надеюсь, будет и дальше иметь право распоряжаться своим произведением, в том числе предоставлять его в безвозмездное пользование по своему усмотрению. Повторить — и предостеречь, ибо не в первый раз возникает ощущение, что идеи свободных лицензий используются для лоббирования откровенно «пропиратских» законодательных интересов.

Возвращаясь к контролю за сетью в целом, надо отметить, что новостей об этом все больше. Можно говорить разное о свободе или несвободе сети, но с фактами не поспоришь. Вот и «Яндекс» подписался на piFilter для распознавания так называемого «нежелательного» контента. То есть фильтровать контент, как делает, например, американский Google при помощи content ID, все-таки возможно. И как это вяжется с заявлениями российских интернет-гигантов

(см. материалы круглых столов ВОРУ.НЕТ! за 2010 год) о том, что они просто «не имеют технической возможности» отследить пиратский контент?

Теперь об интеллектуальных судах. Вопрос обсуждается уже два года, планировалось, что данный судебный орган будет базироваться в «Сколково», но пока ничего не происходит: во всяком случае Правительство РФ дало отрицательный отзыв на законопроект об их создании. Между тем президент России настаивает на реализации инициативы, что в очередной раз говорит о повышенном внимании государства к результатам интеллектуального труда в разрезе технического прогресса. Здесь, правда, есть риск, что данный суд будет исключительно научным — однако, если при его создании будет учтен зарубежный опыт, этого не произойдет. Странно, правда, слышать о его необычном статусе: уровень первой инстанции арбитражных судов с системой обжалования внутри их же. Смысл в этом случае как-то теряется: если суд первой инстанции будет сформирован из профессионалов, специализирующихся на интеллектуальном праве, то ситуация, при которой их решения сможет отменить судья общего профиля, кажется абсурдной.

К созданию интеллектуальных судов нас, кстати, призывают и США. В докладе Рона Кирка (2011 Special 301 Report, Ambassador Ronald Kirk Office of the United States Trade Representative) наша страна в очередной раз оказывается в «почетном» списке «пропиратских» государств. В ежегодном докладе о положении дел с защитой прав интеллектуальной собственности (ПРИС) список вообще живописный: Алжир, Аргентина, Венесуэла, Израиль, Индия, Индонезия, Канада, Китай, Пакистан, Таиланд, Чили, и еще 29 стран, в числе которых Белоруссия, Таджикистан, Туркмения, Узбекистан и Украина, в так называемом «надзорном» статусе.

А у нас все по-прежнему. 2 августа в Министерстве экономического развития прошли открытые слушания, касающиеся поправок в части 1—4 Гражданского кодекса РФ, на которых мы опять слышим, мягко говоря, смелые идеи о приравнивании результатов интеллектуального труда к информационным объектам, послаблениях в защите интеллектуальных прав. На мой взгляд, никакой технический прогресс не может попирать право, ограничивать или разрушать его. Надеюсь, ведомство, контролирующее поправки, также услышит данный тезис и сочтет его более разумным, чем общеизвестное пропиратское лобби, давно и, к сожалению, успешно существующее в нашей стране.

И поможет им в этом судебный взгляд на проблему — ведь именно суд является арбитром в неурегулированных (а потому судебно-спорных) вопросах. 13 июля Федеральный арбитражный суд Московского округа поставил точку в споре между «Всемирными Русскими Студиями» (RWS, входит в холдинг «Система Масс-медиа») и интернет-магазином «Видео.ру», представленным группой ответчиков, каждый из которых признан ответственным за незаконное распространение аудиовизуального произведения RWS*. Юридическая общественность пристально следила за ходом этого дела с начала 2010 года, и понятно почему: впервые в России иск о незаконном использовании аудиовизуального произведения в сети Интернет вчинен на сумму 24 (двадцать четыре) миллиона рублей, впервые в таком деле правообладатель судится сразу с тремя ответчиками, каждый из которых может свалить вину на другого, впервые правообладатель комплексно применяет имеющийся у него правовой инструментарий, включая арест домена нарушителя, впервые дело имеет такое широкое освещение в прессе, и главное — суд признает правоту правообладателя и признает ответственными всех троих ответчиков, один из которых владел доменом, второй управлял им, а третий агрегировал нелегальный аудиовизуальный контент, предоставляя его для незаконного распространения. Крайне, принципиально важно, что в линии защиты была попытка использовать аргументы интернет-посредника, и суд отклонил их. Важно, потому что именно безответственное отношение и уклонение от ответственности интернет-посредников, таких как P2P и социальные сети, фактически зарабатывающих на нелегальном контенте, незаконное размещение которого они поощряют. Отрасль давно нуждалась в прецеденте, который мог бы «перевесить» дело ВГТРК — «ВКонтакте», и этот прецедент создан. Остается поздравить команду, работавшую над делом, и выразить надежду, что оно станет лишь первым значимым событием в упорядочивании Интернета.

Именно упорядочивании, ибо справедливо было сказано, что многие новые вещи пытались *изменить* мир, но в итоге — они в этот мир *вписались*.

Хорошего всем лета! ■



*Для связи с автором пишите на pavel.a.katkov@gmail.com с пометкой «Интернет и закон»*

* Постановление ФАС МО №КГ-А40/6477-11 от 13 июля 2011 года

# МАРИО ИВАНОВ: «Россия — очень важный для нас рынок»

**О работе и перспективах развития крупнейшего мирового спутникового оператора в России «Интелсат» рассказал его коммерческий директор Марио Иванов (Mario Iwanow) в своем интервью издателю журнала «Мобильные телекоммуникации» Сергею Ерохину.**

**— Марио, каких показателей достигла ваша компания к концу 2010 года? Вы довольны этими результатами?**

— Для компании «Интелсат» 2010 год был благоприятным: с рекордными доходами в $2,5 млрд, рекордным портфелем заключенных контрактов на $9,8 млрд и почти с $1 млрд капитальных инвестиций в нашу спутниковую группировку.

**— Насколько успешна работа «Интелсат» в России?**

— Россия — очень важный для нас рынок. На российском рынке существует большой спрос на услуги спутниковой связи, и наши клиенты — мобильные операторы, нефтяные и газовые компании и банки — являются лидерами на соответствующих рынках. Их успех — залог нашего успеха.

**— Какие вы ставите перед собой задачи на 2011 год?**

— Мы видим, что рынки услуг спутниковой связи в России и Азии развиваются достаточно быстро. Компания «Интелсат» способствует развитию данной области в этих регионах в рамках нашей программы инвестирования во флот. В январе начнет работу спутник Intelsat 17, а позднее в этом году запланирован запуск Intelsat 18. Мы также готовим запуск большого количества спутников в 2012 году, что обеспечит новые спутниковые емкости в этих регионах. Мобильность нашей спутниковой группировки также позволяет нам передислоцировать активы для соответствия спросу на рынке.

**— Какие вы можете сделать прогнозы, касающиеся стоимости спутникового ресурса?**

— Мы прогнозируем, что стоимость спутниковых ресурсов либо останется на нынешнем уровне, либо возрастет. Дефицит спутниковой емкости весьма велик. Например, в настоящее время мы обсуждаем предварительные обязательства, касающиеся емкостей спутников, которые мы еще только планируем запустить.

**— «Интелсат» — глобальная компания, которая работает как на территории России, так и в других странах. Есть какие-нибудь особенности работы компании в России?**

— Россия — очень надежный рынок, и у нас здесь очень хорошие партнеры. Растет спрос на рынке спутникового телевидения, а также имеется отличный потенциал роста в области мобильной связи. Для обслуживания всех этих рынков на большой территории требуется оператор, который может предложить большой ассортимент спутниковых емкостей, и ресурсы наших спутников смогут удовлетворить потребности таких клиентов.

**— Вы наверняка знаете, что в России сегодня разрабатывается проект предоставления высокоскоростного спутникового доступа в Интернет. Планирует ли ваша компания участвовать в этом проекте? Насколько, на ваш взгляд, реалистично построить такую систему с учетом требований по ограничению стоимости абонентских терминалов и скоростей доступа?**

— Реализация в России большого проекта широкополосного доступа через спутник очень благоприятна для отрасли спутниковой связи. Мы надеемся, что наши старания не будут напрасными, и мы обеспечим

население улучшенным доступом к широкополосным услугам.

О возможности применения Ка-диапазона много говорили, ведь емкость Ка-диапазонных спутников позволяет провайдерам потребительского широкополосного доступа предоставлять услуги с большой пропускной способностью и низкой стоимостью. Но для нас не имеет значения используемый спектр частот. Что касается услуг предоставления широкополосного доступа в Интернет через системы спутниковой связи, мы уверены, что Ка-диапазон — это прекрасный компромисс между пропускной способностью и доступностью услуг, который удовлетворит все потребности наших клиентов. Мы способны адаптировать наше оборудование в зависимости от потребностей клиентов в частотных ресурсах.

Для компании «Интелсат» мы выбираем спутниковые проекты, соответствующие нашим оперативным целям по обеспечению надежности услуг в пределах нашего спутникового флота. Наши основные клиенты — это провайдеры, у которых строгие требования к надежности и доступности. Наша работа — создать оптимальные условия, чтобы они могли предоставлять высококачественное обслуживание населению. Мы обеспечиваем Россию спутниковой связью уже десятки лет и стремимся к участию в инновационных проектах, если это имеет смысл для компании «Интелсат» и наших клиентов. ■

## «ГЛОБАЛСТАР» ОБЪЯВЛЯЕТ ОБ УСПЕШНОМ ПРОВЕДЕНИИ ЗАПУСКА ВТОРОЙ ШЕСТЕРКИ СПУТНИКОВ

Компания «Глобалстар, Инк.» объявила об успешном проведении запуска шести спутников второго поколения системы «Глобалстар» с космодрома Байконур в Казахстане с использованием ракеты-носителя «Союз».

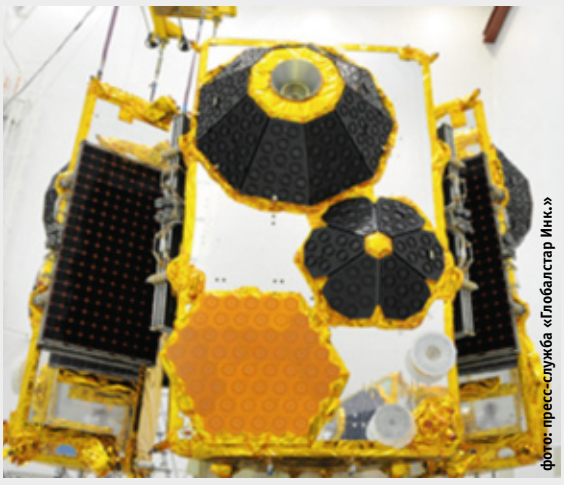


фото: пресс-служба «Глобалстар Инк.»

Компания Arianespace, осуществлявшая запуск, подтвердила, что верхняя ступень вывела на орбиту высотой 920 км шесть спутников. «Глобалстар» сообщил, что все шесть спутников отделились от разгонного блока «Фрегат» и от выводного устройства. «Глобалстар» начал тестирование запущенных спутников, работа всех спутников в настоящее время проходит нормально.

«Сегодня мы с огромным удовольствием объявляем об успешно проведенном запуске шести спутников и о развертывании спутников второго поколения. Теперь мы с нетерпением ждем предоставления услуг с использованием новой группировки, — сказал президент “Глобалстар” Энтони Наварра. — Еще шесть спутников благополучно выведены на орбиту, и мы снова поздравляем и благодарим всех сотрудников “Глобалстар”, говорим спасибо компании Arianespace, осуществившей запуск спутников, а также компании-производителю Thales Alenia Space за проделанную работу».

«Глобалстар» подписал контракт с Thales Alenia Space на проведение проектирования, производство и поставку спутников нового поколения в 2006 году. Всего Arianespace произведет четыре запуска по шесть спутников в каждом.

Группировка спутников второго поколения «Глобалстар» предназначена для обеспечения работы продуктов и услуг телефонии, дуплексной и симплексной передачи данных, включая линейку продуктов СПОТ. Проектный ресурс спутников составляет 15 лет, это в два раза больше, чем у спутников «Глобалстар» первого поколения. Планируется, что спутники второго поколения будут работать как минимум до 2025 года включительно

После осуществления еще двух запусков и развертывания всей группировки второго поколения «Глобалстар» планирует вновь предоставлять услуги мобильной телефонии самого высокого качества и передачу данных с использованием портативных спутниковых телефонов коммерческим и правительственным абонентам в более чем 120 странах.

# INTEL В РОССИИ:
## 20 лет побед и свершений

***Александр СЕМЕНОВ***

**15 июня корпорация Intel отметила 20-летие работы в России и других странах СНГ. Торжества прошли в Московской школе управления «Сколково». В рамках мероприятия состоялась конференция, на которой с докладами выступили руководители корпорации. Во второй части конференции гости посетили четыре сессии: высокопроизводительные вычисления и центры обработки данных; ИТ на предприятии; решения Intel для мобильных платформ; программное обеспечение и вычислительные платформы. На выставке, развернутой в холлах Сколковского «диска», продукцию на базе решений Intel представили более 20 компаний-партнеров.**


Конференцию, посвященную 20-летнему юбилею российского отделения Intel, открыл Камиль Исаев, директор по исследованиям и разработкам (SSG) в России и СНГ. Он обратил внимание гостей на достижения российских коллег в области исследований и разработок. Затем Камиль Исаев представил Дмитрия Конаша, регионального директора Intel в странах СНГ, и Уильяма Сэведжа (Bill Savage), вице-президента Intel Software and Services Group (SSG) и директора отдела продуктов для разработчиков (Developer Products Division).

Дмитрий Конаш рассказал об истории Intel в России, начиная с первого офиса корпорации, открытого в Москве в 1991 году. Сегодня Intel в нашей стране — это не только крупнейший в Европе центр исследований и разработок, который размещен в офисах Москвы, Санкт-Петербурга, Нижнего Новгорода, Новосибирска, с отделениями по продажам и маркетингу в Киеве и Алматы. Корпорация стала неотъемлемой частью ИТ-индустрии и экономики, активным участником социальных процессов в этих странах, уважаемым работодателем.

Уильям Сэведж остановился на структуре центров разработок Intel в России, подчеркнул, что в них представлены разные группы: программного обеспечения и сервисов (SSG), архитектур (Intel Architecture Group, IA), технологий и производства (Technology and Manufacturing, TMG), а также исследовательские лаборатории (Intel Labs). Основными разработками является создание компиляторов, вычислительных библиотек и инструментов для программ (Intel Parallel Studio, Intel Cluster Tools, Media SDK и MeeGo SDK), симуляторов, новых микроархитектур.

Один из наиболее содержательных докладов под названием «Лидерство в эпоху вычислений» (Leading in the Age of Computing) сделал Томас Килрой (Thomas Kilroy), старший вице-президент Intel и генеральный менеджер департамента маркетинга и продаж (Sales and Marketing Group, SMG).

Он начал с того, что сегодня информационные технологии окружают человека повсюду. Люди все

активнее общаются друг с другом в социальных сетях, используют электронную почту, создают контенты и обмениваются ими. 53% опрошенных из числа работающих граждан США считают, что компьютеры и различные мобильные устройства делают жизнь намного лучше. Г-н Килрой привел интересную статистику: сколько часов ежемесячно пользователи проводят в социальных сетях. По этому параметру Россия лидирует (10 час.), за ней идет Израиль (9 час.), Турция (8 час.), Великобритания (7,8 час.), Филиппины (6 час.), Канада (5,8 час.), Индонезия, Финляндия, Испания, Пуэрто-Рико (примерно по 5 час.).

Объем данных, обмениваемых с помощью мобильных устройств, ежегодно удваивается. Вычислительные модули становятся компонентами встраиваемых систем там, где ранее не использовались (реклама, сборочное производство, автомобилестроение и т.д.). Количество «умных» клиентских устройств, по прогнозам аналитиков, до 2014 года будет расти со скоростью 22% в год и в 2014 году вырастет до 15 млрд (в 2011 году их будет около 8 млрд). Количество скачиваемых мобильных приложений будет расти в среднем на 34% в год и к 2014 году приблизится к 40 трлн, в 2011 году их будет около 15 трлн. Как подчеркнул г-н Килрой, для обеспечения успешной работы устройств и приложений должно расти и количество серверов архитектуры x86, оно будет расти на 14% в год и к 2014 году достигнет 27 млн. Количество данных, пересылаемых через Интернет, растет колоссальными темпами: в 2009 году их объем составил 150 эксабайт, а в 2010 году он вырос до 245 эксабайт.

Intel продолжает воплощать в жизнь закон Мура, делая процессоры все более производительными и энергоэффективными. Это было бы невозможно, если бы компания Intel не была технологическим лидером отрасли. Г-н Килрой напомнил, что в 2003 году компания внедрила технологию напряженного кремния в технологический процесс 90 нм, в 2007-ом — металлический затвор с диэлектриком High-K (техпроцесс 45 нм), в 2011-ом — трехмерные транзисторы Tri-Gate (техпроцесс 22 нм). Эти инновации стали залогом успеха Intel на современном рынке. Г-н Килрой особо подчеркнул, что технологический процесс 22 нм — настоящий революционный прорыв в производстве: он позволяет на 37% повысить производительность при низком напряжении и на 50% снизить энергопотребление.

Очень важно, что все современные операционные системы, приложения и поддержка экосистемы оптимизированы для работы на архитектуре Intel. Благодаря этому обеспечивается широкая поддержка ПО на настольных ПК, ноутбуках, нетбуках, планшетах, смартфонах, серверах, умном ТВ и многих других устройствах. Кроме того, во всех перечисленных устройствах с успехом работают процессоры Intel, такая ситуация называется компьютерным континуумом.

Чтобы оставаться лидерами рынка, надо постоянно предлагать ему новые и новые инновации. Г-н Килрой представил новый сегмент мобильного рынка — «ультрабуки», отличительными чертами которых являются ультратонкие (толщиной менее 2 см) и ультрабезопасные устройства с очень быстрым откликом. «Ультрабуки» сочетают в себе производительность ноутбуков с характеристиками планшетов. Они будут использовать чипы Sandy Bridge, а затем и Ivy Bridge (с 2012 года). Еще одним преимуществом «ультрабуков» станет длительное время работы от батарей (до 8 час., то есть полный рабочий день). Новые устройства будут продаваться по цене менее $1000. Ожидается, что к концу 2012 года они займут до 40% рынка мобильных компьютеров. Г-н Килрой продемонстрировал один из таких «ультрабуков» от Lenovo толщиной всего 14,9 мм.

Далее г-н Килрой подчеркнул, что без обширной экосистемы партнеров корпорация Intel не смогла бы достигнуть успехов в своей деятельности. Сейчас Intel особое значение придает развитию программного обеспечения, поэтому на сцену был приглашен Павел Фролов, генеральный директор LinuxCenter в России.

Он рассказал, как его компания поставляет в России свободное ПО и помогает людям стать независимыми, экономя на лицензиях. LinuxCenter отвечает за создание русской версии MeeGo. Г-н Фролов отметил, что компания Intel начала активно работать на рынке свободного ПО, и это очень радует. В российской версии MeeGo обеспечена поддержка социальных сетей. Павел Фролов продемонстрировал планшет компании 3Q с поддержкой MeeGo и подчеркнул, что это пока единственный планшет в России, который предназначен не только для потребления, но и для создания контента. По его мнению, этот планшет будет с успехом использоваться в системе образования и целом ряде других отраслей.

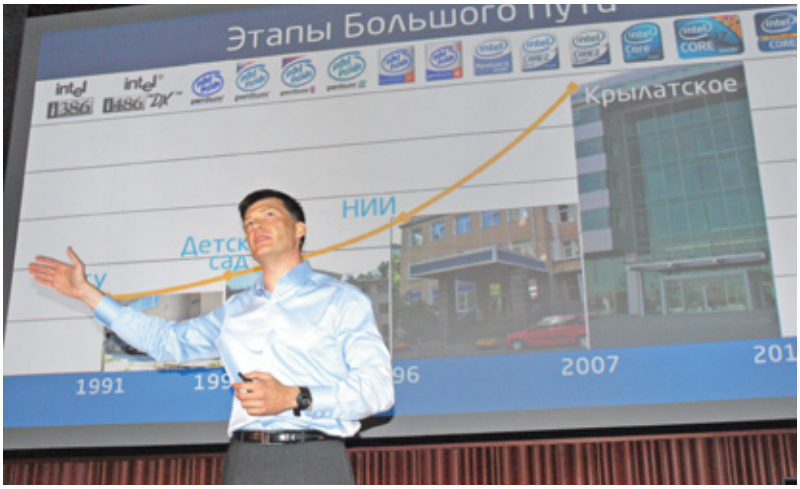
В заключение Томас Килрой отметил, что Россия становится одним из глобальных лидеров в ИТ-сфере. РФ занимает шестое место в мире по величине ВВП, обладает колоссальными энергетически-

ми ресурсами, глубокими культурными традициями и образованием мирового уровня. Объемы инвестиций в России и других странах СНГ в 2010—2014 годах, согласно прогнозам, покажут наибольший процентный прирост среди всех европейских рынков. В России он составит более 70%, тогда как в Турции — 55%, в Румынии — 42%, в Польше — 38%, в Венгрии — 35%, в Швеции, Германии и Франции не более 20%.

В России продажи ПК через торговые сети растут существенно быстрее, чем на развитых европейских рынках. Стремительно растет и количество компаний, разрабатывающих ПО (прогноз: в два раза с 2009 по 2015 год). Весь этот комплекс обстоятельств способствует выходу России на лидирующие позиции, и Intel готова всячески помогать этому процессу. Поэтому есть уверенность в том, что корпорацию в России ждут еще 20 прекрасных лет.

Кирк Скауген (Kirk Skaugen), вице-президент, генеральный менеджер Intel Architecture Group, Data Center Group, рассказал о том, каким Intel видит стратегическое развитие облачных вычислений, и представил соответствующие стандарты и технологии следующего поколения, которые сделают центры обработки данных безопаснее, эффективнее и проще. Также Кирк поделился передовым опытом внедрения проектов по созданию «публичных облаков», которые обеспечивают пользователям гибкость и возможность выбора.

Важность облачных систем значительно выросла в последнее время и к 2015 году составит более 2,5 млрд подключенных пользователей, будет обрабатывать более 1000 эксабайт интернет-трафика и насчитывать 15 млрд устройств




с доступом к облачным сервисам. Поэтому преобразование центров обработки данных для поддержки такого объема подключенных устройств может быть достаточно сложным. Кирк подчеркнул важность облачных решений: открытых, совместимых, управляемых, безопасных, построенных в соответствии со стандартами, для решения задач, стоящих перед ИТ-индустрией, и получения значительных преимуществ, которые могут привнести «облака».

Значительный рост количества портативных электронных устройств, а также их производительности изменил наше представление о мобильных компьютерах еще в начале 90-х. Появление миллионов устройств, подключенных к Интернету, социальные сети и общение в режиме реального времени, многофункциональные мобильные девайсы подвинули нас от традиционной абстрактной модели использования данных к контекстной модели, когда информация, контент, созданные пользователями, взаимосвязаны и взаимодействуют друг с другом. Однако взаимодействие данных, наряду с огромным количеством приложений и различных источников информации, приводят к проблемам, связанным с безопасностью передачи данных.

В своем выступлении Стив Павловски (Steve Pawlowski), старший заслуженный инженер-исследователь Intel Architecture Group, генеральный менеджер Cross-IAG Architecture and Pathfinding, представил тенденции и достижения, необходимые для обработки данных, программного обеспечения, беспроводных сетей и безопасности, которые все вместе смогут улучшить работу мобильных компьютеров, чтобы, с одной стороны, сделать нашу жизнь проще, а с другой — решать не только основные задачи пользователей, но и глобальные проблемы человечества.

Будущее мобильных вычислений как новая эра в компьютерных вычислениях, потребности пользователей сегодня и завтра — далеко не все темы, которые были затронуты в выступлении.

Очень интересным было и выступление Леонида Соколинского, декана факультета вычислительной математики и информатики и руководителя Лаборатории суперкомпьютерного моделирования Южно-Уральского государствен-

ного университета. Он рассказал об инновационной образовательной программе «Персональный виртуальный компьютер» на базе облачных вычислений, практическое использование которой для обучения и подготовки специалистов инженерно-технических направлений начато в ЮУрГУ. Проект реализуется компанией РСК СКИФ при участии специалистов ЮУрГУ и корпорации Intel, выступившей в качестве инициатора. Это первый в России и СНГ пример полномасштабного внедрения платформы на базе облачных вычислений в процесс обучения студентов.

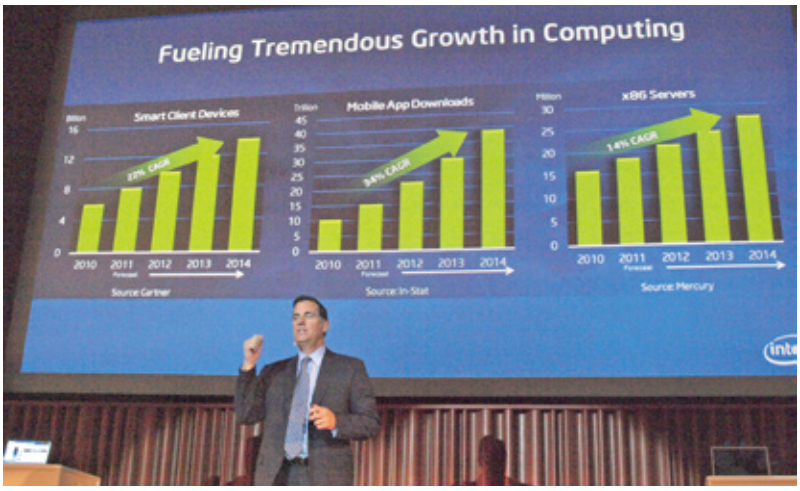
Технические сессии были посвящены наиболее актуальным темам.

## Центры обработки данных, высокопроизводительные и облачные вычисления

Участникам сессии был предложен обзор технологий корпорации Intel, которые помогают решать наиболее сложные задачи в области высокопроизводительных вычислений: ключевые технические данные о процессорах Intel® Xeon® для высокопроизводительных вычислений, процессорах Intel® Many Integrated Core Architecture (Intel® MIC Architecture), доступных сегодня программных инструментах и библиотеках корпорации Intel. Было уделено внимание будущему гетерогенных программных инструментов для процессоров Intel Xeon и Intel® MIC Architecture. Презентации сопровождались сообщениями лидирующих промышленных потребителей и университетов-партнеров об успешном использовании высокопроизводительных вычислений от компании Intel в решении широкого спектра задач, начиная от предсказания погоды и заканчивая металлургией.

## ИТ на предприятии

Что, по мнению корпорации Intel и отраслевых ИТ-экспертов, ожидает нас в будущем? В каком направлении корпорация Intel будет развивать индустрию ИТ-технологий в ближайшие 20 лет? Сессия была посвящена общим вопросам использования клиентских устройств в корпорации Intel и путях оптимизации. Было рассказано о проблемах и функциональных возможностях, которые необходимы ИТ-организациям для внедрения клиентских устройств, и о том, как подготовиться к будущим изменениям, установив необходимые требования и приоритеты при внедрении защищенных и масштабируемых решений.




## Решения Intel для мобильных платформ

Трек был посвящен тонкостям системного проектирования и техническим деталям, которые необходимо знать в ходе разработки новых аппаратных устройств и программных приложений на базе Intel® Atom™. Эксперты Intel поделились данными об исследовании рынка и рассказали о том, на какой технической базе создаются нетбук, планшет и другие мобильные устройства. Вниманию слушателей были представлены программы для поддержки разработчиков и инструменты разработки ПО, а также новая операционная система MeeGo и центр продаж приложений Intel AppUp.

## Программное обеспечение и вычислительные платформы

На сессии обсуждалась стратегия разработки ПО компании Intel для ее различных аппаратных платформ. Был представлен обзор программных продуктов, позволяющих аппаратным платформам удовлетворять запросы всего рынка вычислительных систем. В частности, эксперты рассказали о следующих платформах и программных продуктах компании Intel:

- применение продукта Intel Parallel Studio XE;
- обзор Intel HD Graphics и программных методов для наилучшего использования GPU;
- обзор продукта Intel MediaSDK;
- обзор инструментов Intel Cluster tools.

Более подробно о мероприятии смотрите на www.intel.ru/20years ■

# АЛЕКСЕЙ ЛУКАЦКИЙ:

## «Рынок информационной безопасности бурлит»

***Александр СЕМЕНОВ***

**Алексей Лукацкий, эксперт компании Cisco в области информационной безопасности, ответил на вопросы научного редактора нашего журнала.**

**— Чем интересен нынешний момент на рынке информационной безопасности в мире и в России: идет нормальная эволюция или все бурлит?**

— Все бурлит, во всяком случае в России, где в процессе принятия находится закон о персональных данных, точнее поправки к нему. Если эти поправки будут приняты, то картина рынка информационной безопасности кардинально изменится: все либеральные инициативы последних лет будут упразднены, и право регулировать рынок закрепится за ФСТЭК и ФСБ.

Вопрос о персональных данных реально важен для 7 млн российских операторов, среди которых и юридические лица, и индивидуальные предприниматели. Если в прежнем варианте закона не было четко определено, что операторы должны делать для обеспечения информационной безопасности, и они должны были лишь защищать персональные данные (как — не уточнялось), то в нынешней редакции закона прописаны конкретные меры. Обеспечение безопасности персональных данных в самом жестком своем варианте становится обязательным для всех без исключения. Проблема, однако, в том, что многие участники рынка физически не смогут выполнять этот закон. Фермерское хозяйство с двумя-тремя компьютерами, например, никогда не сможет приобрести сертифицированные средства защиты и выполнить целый ряд других мер организационного и технического характера.

Принятие поправок к закону должно сильно подхлестнуть рынок информационной безопасности, но не факт, что это благотворно повлияет на число утечек персональных данных.

Так что баталии вокруг этого закона — главное событие на рынке информационной безопасности сегодня. Главное, но не единственное: есть еще законодательство, связанное с государственными услугами. Портал таких услуг уже работает, и ими должны пользоваться самые разные организации, а это свыше 10 тыс. узлов или сайтов, требующих реализации тех или иных мер защиты. Это тоже достаточно важный драйвер развития рынка информационной безопасности.

Если смотреть шире, то принятая в конце прошлого года государственная программа «Информационное общество 2012—2020» подразумевает решение большого количества задач по обеспечению информационной безопасности. Например, создание крупных информационных систем в масштабах государства, кадастров разного типа, реестров, больших баз данных невозможно без обеспечения информационной безопасности. Невозможна и эффективная работа дистанционного обучения и телемедицины.

Словом, можно сказать, что информационной безопасности сегодня уделяется особое внимание, этот рынок будет расти и развиваться.

**— Не могли бы вы сказать несколько слов о письме, которое написали российские эксперты в области информационной безопасности президенту РФ в связи с законом, о котором шла речь.**

— Суть его в том, что внесенные поправки нарушают систему подготовки документов для принятия государственных актов в России. Буквально за два дня до отправки поправок на второе чтение на сайте Госдумы был размещен совсем другой текст этих поправок, в выработке и согласовании которых и я принимал участие, поскольку вхожу в различные рабочие группы, обсуждающие поправки в действующее законодательство с целью его гармонизации с европейской практикой. Согласование всех формулировок длилось около полутора лет, была проведена серьезнейшая работа, и вдруг совершенно неожиданно выработанный совместными усилиями текст был изменен. Согласно новой версии законопроекта, все правила по обеспечению информационной безопасности определяют не сами операторы персональных данных, а регуляторы — ФСТЭК и ФСБ.

Эта поправка коренным образом меняет сложившуюся в России ситуацию. В предыдущей версии закона операторам предоставлялось право самостоятельно выбирать меры по защите, в нынешней же редакции это право отсутствует.

Поправка также полностью уничтожает понятие отраслевого стандарта. До сих пор их было несколько: стандарт Банка России, стандарты Минкомсвязи и Минздравсоцразвития, стандарт по защите персональных данных Национальной ассоциации участников фондового рынка, стандарт Национальной ассоциации негосударственных пенсионных фондов и т.д. Предложенная поправка делает бессмысленной всю проделанную работу, аннулируя все эти стандарты.

Более того, эта поправка противоречит европейской конвенции и директиве по защите персональных данных, согласно которым оператор самостоятельно выбирает способ защиты персональных данных, исходя из наличия конкретных угроз, технологии обработки персональных данных, размера возможного ущерба и т.п. В случае утечки информации оператор, естественно, должен нести ответственность перед субъектом. В предложенном же варианте поправок о субъекте и речи нет. Меры по защите информации прописаны жестко, а ответственности за утечку информации как не было, так и нет. Предусмотрено наказание не за нарушение духа закона, а за нарушение его буквы, то есть за применение несертифицированных решений.

Добавлю, что этот законопроект не применим к таким новым технологиям, как облачные вычисления, виртуализация, аутсорсинг, мобильный доступ и т.п. Все эти технологии окажутся практически вне закона. Для них не всегда существуют сертифицированные средства защиты, а значит, нет возможности выполнить требования закона и подзаконных актов.

**— Какие наиболее интересные технологические решения в области информационной безопасности вы можете выделить?**

— Есть несколько основных направлений: защита виртуализации, защита облачных вычислений, защита мобильного доступа (в широком смысле — в плане подключения с любых мобильных устройств). Четвертое направление — активное внедрение социальных сетей и других технологий Web 2.0 (твиттеры, блоги и т.п.) в работу компаний. Это новая тенденция, и она существенно влияет на возможные утечки информации.

В мире уже есть эффективные решения для защиты информации в каждом из перечисленных случаев. В России их внедрение наталкивается на законодательные препоны, которые относятся к этим новым технологиям «с подозрением».

В случае облачных вычислений проблема не столько технологическая, сколько юридическая и психологическая. Главное при использовании облаков — доверие. Можно ли доверять критически важные для бизнеса данные партнеру? А если да, то как обеспечить их сохранность? Чем гарантирована ответственность бизнес-партнера? В России облачные вычисления

сталкиваются еще с одной проблемой — низким качеством интернет-каналов за пределами крупных городов. В каком-то смысле это дает нам дополнительный запас времени: когда страна подтянется в плане качества связи, улучшится и законодательство в области информационной безопасности, в том числе по защите персональных данных.

**— Расскажите об интересных решениях компании Cisco, касающихся каждого из этих направлений.**

— Начнем с защиты мобильного доступа. Несколько лет назад мы поняли, что постепенно мобильные устройства вытеснят все остальные не только из личной жизни, но даже из бизнеса. Если вы посмотрите вокруг, то заметите, что сейчас у пользователей в руках планшетов и смартфонов больше, чем ноутбуков.

Учитывая эту тенденцию, несколько лет назад наша компания разработала решение Cisco AnyConnect — унифицированный защищенный мобильный клиент, позволяющий обеспечить защищенный доступ к корпоративным ресурсам с любого устройства, будь то обычный ноутбук, iPad, iPhone, смартфон webOS, Palm, Symbian, Windows Mobile. Функционал Cisco AnyConnect предельно широк: это и построение VPN с данных платформ, и контроль защищенности данного мобильного устройства на предмет наличия уязвимостей, и возможность прозрачного перенаправления трафика через облако ScanSafe, чтобы проверить, не заражены ли данные, уходящие или поступающие на устройство. Cisco AnyConnect обеспечивает и полный контроль доступа в Интернет на любые сайты. Мобильные пользователи обычно не находятся под защитой корпоративных средств защиты, поэтому их нельзя контролировать и защищать, но Cisco AnyConnect достаточно эффективно решает и эту задачу.


Клиент AnyConnect обеспечивает также доступ к проводным и беспроводным сетям, аутентификацию в процессе доступа к корпоративным ресурсам и эффективную защиту медиатрафика при работе через Skype или корпоративные средства связи.

Данное направление активно развивается и будет развиваться в дальнейшем, поскольку, по прогнозам подразделения Cisco IBSG (Internet Business Solutions Group), количество подключенных к Интернету устройств будет стремительно расти, и к 2015 году их количество достигнет 25 млрд.

Для защиты виртуализированных сред компания выпустила межсетевой экран Cisco Virtual Security Gateway, который контролирует трафик между виртуальными машинами и блокирует попытки несанкционированного доступа к гипервизору. Защита облачных вычислений реализуется во всех решениях Cisco. При этом компания предлагает еще и самостоятельный облачный сервис по защите web-доступа, что наиболее актуально для защиты новых офисов и особенно мобильных пользователей.

Большим успехом Cisco стала разработка совместно с российской компанией «С-Терра СиЭсПи» и запуск локального производства сертифицированного VPN-модуля NME-RVPN, который интегрируется в маршрутизаторы Cisco ISR G2 и может обеспечить требуемый законодательством уровень криптографической защиты различных видов тайн и конфиденциальной информации, включая и защиту персональных данных.

**— А какие новые угрозы появляются на рынке информационной безопасности?**

— Основная проблема сегодня — это интернет-угрозы, поскольку все уходит в Интернет: облака, социальные сети, блоги

и т.д. Именно через Web-сайты вредоносные программы проникают в компьютеры и мобильные устройства пользователей. По нашей статистике, 87% всех угроз осуществляется через Web-сайты, причем владельцы 79% сайтов даже не представляют, что их сайты взломаны. Один из последних примеров — сайт одной отечественной метеорологической службы. Можете себе представить, сколько пользователей его посещают?! Этот сайт регулярно «ломают», заражая компьютеры посетителей. По нашим оценкам, девять из десяти сайтов в Интернете уязвимы к атакам, поэтому сегодня заражение через Web с дальнейшим распространением вредоносного ПО — самая актуальная тема.

Традиционные методы борьбы с такими угрозами уже не эффективны, поскольку они ориентированы на так называемые черные или белые списки. При этом все забывают о том, что адрес сайта — это всего лишь URL в строке браузера, а за этим адресом раскрывается огромное количество изображений, полученных с разных сайтов, скриптов и флэш-объектов, которые динамически подгружаются в процессе формирования страницы. Разрешая доступ к одному сайту, мы автоматически разрешаем доступ к множеству других сайтов. Именно так вредоносные программы и проникают в компьютеры пользователей.

Два года назад мы в Cisco запустили процедуру создания «Бостонской матрицы киберпреступников». В ее правом верхнем углу находятся «звезды», то есть те приложения, которые приносят злоумышленникам основной доход. В ближайшие два года, по нашему мнению, доминировать будут два направления: использование проблемных сторон Web-сайтов (о чем мы уже говорили) и трояны, которые будут красть персональные и идентификационные данные пользователей. Кстати, трояны проникают в компьютеры пользователей через зараженные сайты. Дальше злоумышленники могут продавать индивидуальные данные пользователей для проникновения в информационные системы, с этим связанные.

В нижней правой части нашего квадрата «дойные коровы» — угрозы, которые не требуют от злоумышленника серьезных усилий, но приносят ему много денег. Это спам и мошенничество, связанное с накручивание кликов на баннерах в Интернете. Эти угрозы не связаны напрямую с информационной безопасностью, но ведь и с мошенничеством надо по мере сил бороться...

В левом верхнем углу нашего квадрата — потенциальные угрозы. Здесь расположены угрозы мобильным устройствам и жульничество в IP-телефонии. Пока эти виды жульничества не очень распространены, но набирают силу. Часто они связаны с тем, что пользователи недостаточно внимательно настраивают параметры IP-телефонии, оставляя «дыры» для доступа злоумышленников.

Мошенничество, связанное с мобильными устройствами, будет очень популярно в ближайшее время в связи с большой распространенностью мобильных устройств. Не так давно появился первый банковский троянец для Blackbery, Android и Symbian, раньше этого не было. Этот вирус, изначально созданный для платформы Windows, постоянно эволюционирует, похищая у пользователей реквизиты для их доступа к банкам.

Важно отметить и то, что поменялась мотивация злоумышленников. Если раньше они стремились к известности, то сегодня все ориентировано на получение прибыли. Поменялся также ландшафт угроз. Прежде целью преступников были публичность и известность, теперь атаки проводятся тихо и незаметно. Некоторое время назад вирусы писались вручную, сегодня они создаются автоматически. Объектом атак все чаще становятся конкретные приложения, в частности банковские или технологические. Раньше целью атак была массовость, сегодня — фокус на конкретном заказчике или группе заказчиков. Как показывают наши исследования, финансовая отдача от фокусной атаки выше.

Один из недавних ярких примеров — атаки на атомную электростанцию в Бушере (Иран). Интересно, что вредоносное ПО было обнаружено только через год после его внедрения. Бороться с такими фокусированными атаками очень сложно. Традиционные антивирусные методы не срабатывают.

Еще одна тенденция нового времени — переход к «кибервойнам», но для конечных пользователей они не очень важны, так как не затрагивают их интересы.

Даже самые простые вирусные атаки становятся сложными и мутирующими, каждый экземпляр атаки может отличаться от другого. Домены меняются ежедневно, даже ежечасно. Контент мутирует и маскируется под легальный трафик. 80% спама исходит от инфицированных клиентов. 70% «зомби» используют динамические IP-адреса. Угрозы из легальных доменов растут на сотни процентов в год. Спам составляет более 180 млрд сообщений в день. ■

# ОБЛАЧНЫЙ OFFICE

***Сергей ДАНИЛИН,***
*обозреватель*

**Сегодня можно с уверенностью сказать, что Россия стоит на пороге «облачной» революции. Системные интеграторы и операторы связи России делают все, чтобы решить проблему недостатка мощностей передающих каналов коммуникаций и ЦОД, которые являются ключевыми элементами в развитии облачных вычислений в России.**

Одной из главных тенденций последнего десятилетия ИТ-рынка стало развитие сервисных продуктов, а именно cloud computing — облачных вычислений, «облаках» — стандартных сервисах, которые поставляются через Интернет и учитываются по мере потребления.

О нынешнем состоянии облачных вычислений в России высказался вице-президент «Газпромбанка» по ИТ Алексей Широких: «Если сопоставлять российский рынок облачных вычислений с тем, что происходит в Америке, Европе и Азии, то налицо некоторое запаздывание — не столько в плане технологий, сколько в области понимания того, как следует размещать информацию в публичном облаке. К тому же наши законы несколько “непредсказуемы”, и продвижение облачных вычислений в России будет сдерживаться не столько технологическим и инфраструктурным факторами, сколько вопросами, связанными с “легализацией” облаков. Для привыкания к облакам потребуется определенный период адаптации, и эта адаптация в большей степени связана с человеческим фактором, чем с технологиями».

Тем временем в «облачной» среде бизнес-приложений произошел значимый прорыв. Компания Microsoft 28 июня официально запустила Office 365 — облачный сервис для бизнес-пользователей. Презентацию провел генеральный директор Microsoft Стив Балмер. На сайте Microsoft велась прямая трансляция с места событий. Одновременно с этим и российское подразделение Microsoft официально представило в Москве новый продукт компании и его возможности.

«Это важное событие потому, что уже в момент запуска свыше 20 международных компаний сервис-провайдеров, таких как Bell Canada, Intuit, Telstra, Vodafone и др., включили Office 365 в свои предложения для малого и среднего бизнеса», — заявил руководитель отдела по продвижению информационных офисных систем Microsoft в России Павел Кузьменко. По его словам, те компании, которые уже имели возможность протестировать облачный сервис Microsoft, дают положительные отзывы о нем.

Цель Office 365 — прийти на смену другому сервису Microsoft, Business Productivity Online Suite (BPOS). Office 365 — это онлайн-версия самых востребованных программ Microsoft для бизнеса, которая объединяет в себе основные офисные приложения компании — Office (Word, Excel, OneNote, PowerPoint), а также продукты для объединенных коммуникаций и совместной работы Exchange, SharePoint, Lync.

«Office 365 — это новый этап в реализации “облачной” стратегии Microsoft. Он заменит сервисы Business Productivity Online Suite, Office Live Small Business и Live@edu. При этом переход к Office 365 никаким образом не отразится на стиле работы пользователей, так как облачный сервис обеспечит доступ к нужным программам и файлам из любого места и с любого устройства, имеющего выход в Интернет», — отмечают в компании Microsoft.

В облачном воплощении все эти продукты получают приставку online, то есть становятся доступными с любого устройства, подключенного к Интернету. Бизнес-заказчики на основе Office 365 смогут получить электронную и голосовую почту, доступ к внутренним сетям организации, программы для обмена мгновенными сообщениями, а также возможность организации голосовых и видеоконференций.

В числе первых российских телекоммуникационных и ИТ-компаний, включивших Office 365 в свои пакетные предложения для бизнеса, «ВымпелКом» и «СКБ Контур».

Широкое бета-тестирование облачного сервиса во многих странах началось в апреле текущего года. А до этого, по сообщению

Microsoft, в закрытом режиме тестирования Office 365 опробовали тысячи организаций и компаний по всему миру.

Авторизованные партнеры Microsoft в России, имеющие право включать сервисы в свои пакетные бизнес-предложения, научились решать одну из проблем, связанную с лицензированием. Так, компания «СКБ Контур» уже предлагает Office 365 в своих наборах продуктов «Экстерн 365» и «Эльба 365» для малого и среднего бизнеса. Стоимость первого пакета, по словам представителя компании Павла Распутина, будет определяться индивидуально в зависимости от потребностей пользователя, а «Эльба 365» предназначена для небольших компаний и может обойтись фирме в 700 руб. за месяц.

Ранее сообщалось, что стоимость годового доступа к Office Web Apps (Word, Excel, OneNote и PowerPoint) составит $72 на одного работника. Для сравнения, годовая подписка на облачные сервисы Google (электронная почта, календарь, документы) стоит $50 в год. Однако для корпоративных клиентов, уже подписавших с Microsoft соглашение Enterprise Agreement, стоимость одной «подписки» на сервис будет зависеть от общего числа сотрудников компании.

После официального запуска Office 365 текущие клиенты более раннего сервиса BPOS должны будут перейти на новый пакет. На это им дается 12 месяцев, и ИТ-подразделениям компаний не мешало бы начать ознакомление с процессом.

В течение года Microsoft предоставляет своим корпоративным клиентам возможность тестировать Office 365 бесплатно, что, по мнению многих представителей бизнеса, является несомненным плюсом. Кроме того, на облачный Office распространяется соглашение SLA, которое гарантирует определенный уровень качества сервиса.

У принявших участие в тестировании Office 365 зарубежных компаний, как водится, уже возникли некоторые затруднения, в частности с синхронизацией документов и переносом почтовых адресов, отмечает ресурс Techworld. Некоторые эксперты выразили опасения, что у ИТ-служб компаний возникнут определенные проблемы и после запуска сервиса. Представители ИТ-подразделений российских фирм, в свою очередь, глобальных проблем в переходе на новый сервис пока не видят.


Стоит отметить, что Microsoft позаботилась об имеющихся клиентах: большую часть необходимой информации и подробные технические требования для перехода к Office 365, включая программное обеспечение, инструкции по синхронизации каталогов, советы по устранению неполадок и пр., компания выложила на своем сайте. Существует также дискуссионный форум и специальный портал по Office 365.

По мнению экспертов, запуск Office 365 положительно повлияет на деятельность Microsoft. Ранее компании Google удалось перетащить часть корпоративных клиентов Microsoft в свои облачные сервисы. «Совершенно очевидно, что Microsoft должна сделать это, чтобы оставаться конкурентоспособной по сравнению с Google. Если сервис будет эффективным и его одобрят, это будет изменением правил игры», — считает исполнительный директор YCMNET Advisors Майкл Йошиками.

Для российских пользователей облачные сервисы уже давно не являются чем-то незнакомым. Многие из них пользуется возможностями Google Apps. В Microsoft отмечают, что компания, в отличие от конкурентов, предложит пользователям, прежде всего корпоративным, не разрозненные сервисы, а «комплексный подход» к переходу «в облака». ■

# АНДРЕЙ БАДАЛОВ:

## «Главное в информационной безопасности — комплексный подход»

*Александр СЕМЕНОВ*

**Интервью первого заместителя генерального директора Российской корпорации средств связи (РКСС) Андрея Юрьевича Бадалова для журнала «Мобильные телекоммуникации»**

**— Расскажите, пожалуйста, об основных тенденциях российского рынка информационной безопасности. Что интересного происходит на нем?**

— С самого начала создания РКСС основной задачей ее деятельности ставилось обеспечение повышенной устойчивости и защищенности инфраструктуры, которая сегодня в России создается в интересах государственных организаций и предприятий с критически важными функциями. Основной вопрос в работе с любым оборудованием (в том числе и импортным), которое является основой телекоммуникационной и ИТ-инфраструктуры — это вопрос доверия: насколько пользователь может доверять оборудованию и программному обеспечению различных компаний, в том числе и известным западным вендорам, которые сегодня работают в РФ. Именно этот вопрос — производство доверенного оборудования в России — был поставлен во главу угла в деятельности РКСС.

Мы уже прошли серьезный этап осмысления этого направления работы и вышли на конкретные проекты. Первым таким проектом стало наше сотрудничество с компанией Alcatel-Lucent. В 2009 году РКСС и Alcatel-Lucent объявили о создании в России совместного предприятия Alcatel-Lucent RT для производства в России и других странах СНГ доверенного телекоммуникационного оборудования. Первые образцы этого оборудования были представлены на прошлогодней выставке «Связь-Экспокомм». В июне 2011 года компании объявили о расширении сотрудничества в области производства оборудования LTE в России и развития направления совместных инновационных исследований. Аналогичные проекты начаты с другими иностранными и отечественными компаниями.

Актуальность этой работы очевидна в условиях повышенного внимания к информационной безопасности.

Рынок информационной безопасности сегодня бурлит примерно так, как некоторые вулканы на поверхности Земли. В основном пейзаж планеты выглядит спокойным и контролируемым, но есть «горячие точки». Я бы отметил повышение «температуры» и напряженности в такой сфере, как обеспечение информационной безопасности критически важных отраслей промышленности, в частности энергетического комплекса.


Не так давно информационная безопасность рассматривалась только в аспекте защиты государственных секретов — кстати, в РФ эти вопросы решены достаточно хорошо. В обеспечении безопасности промышленных объектов и критически важной инфраструктуры процесс построения решений только начинается.

Пример повышенного внимания к этой области — недавнее подпи-

сание президентом РФ Дмитрием Медведевым закона о защите топливно-энергетического комплекса. В нем особое внимание уделяется безопасности информационных систем ТЭК. Это важно, поскольку сегодня зависимость инфраструктуры ТЭК и промышленности от информационных технологий высока и постоянно возрастает. Поэтому и рынок информационной безопасности бурлит именно в этой точке.

И совершенно естественно возникает вопрос о доверии к тому оборудованию и ПО, которое будут приобретать и устанавливать у себя компании. Речь о государственной тайне в этом сегменте рынка не идет, поскольку там немного такой информации, в нем крайне важна целостность и доступность услуг. Именно на это мы и обращаем внимание сегодня, поскольку в ближайшие годы это направление будет активно развиваться.

**— Расскажите о том, какие решения предлагает компания РКСС в этом направлении.**

— Начну с незначительного факта. Не секрет, что часто самое разное оборудование, установленное в российских компаниях, в том числе в критически важных отраслях, удаленно мониторится производителями (вендорами). Делается это с самыми благими целями — обеспечения его бесперебойной работы. При этом естественно возникают угрозы проникновения в информационные системы критически важной инфраструктуры. Очевидно, что необходимо находить более доверенные механизмы для обеспечения информационной безопасности в таких случаях, как для оборудования, так и для ПО. При этом все процессы мониторинга этого оборудования и ПО также должны быть сертифицированы. Этой работой мы предметно занимаемся.

Один из первых примеров такой работы — это наш проект для крупной элктроэнергетической компании РФ. Мы создаем для нее комплексную автоматизированную систему управления безопасностью. При этом мы не только решаем все вопросы, связанные с обеспечением физической безопасности, но и закладываем механизмы обеспечения информационной безопасности. Эта работа носит инновационный характер: впервые мы формулируем не только технические решения, но и перечисляем угрозы и риски, которые существуют сегодня в этой области. Мы обращаем внимание на наличие тех или иных уязвимостей и предлагаем решения для того, чтобы обеспечить устойчивость и целостность работы системы за счет применения отечественных доверенных технологий. В основу этой работы положено построение онтологической модели деятельности компании. Без понимания структуры объектов и субъектов управления, отношений между ними бессмысленно говорить об обеспечении безопасности. В РКСС работает сильная команда онтологов (инженеров по знаниям). Опыт ее работы может быть полезен для всей отрасли ТЭК.

Традиционно мы продолжаем работать для госсектора, предлагая и здесь наши собственные решения в области защиты информации. Совсем недавно РКСС подписала соглашение с компанией «Связьинтек» (входит в группу компаний «Связьинвест») о создании в России доверенной информационно-телекоммуникационной инфраструктуры, которая успешно начинает работать на рынке крупнейших операторов РФ, в том числе в области технологий. Это еще одно очень важное направление нашей работы.

Серьезным результатом нашей работы стало создание совместного предприятия с американской компанией Crossbeam. Продуктом этого СП станет унифицированная и сертифицированная платформа информационной безопасности для операторов связи и крупных предприятий.

Мне еще раз хотелось бы подчеркнуть, что обеспечение информационной безопасности — это комплексный процесс. Безопасность должна быть равнопрочной во всех сферах, только тогда можно быть уверенным в нормальной и бесперебойной работе инфраструктуры. Понимание того, что это важно, есть и у наших заказчиков. При этом осталось еще немало технических проблем, которые предстоит решить: это и колоссальная несовместимость продуктов, и отсутствие в ТЭК (как и во многих других отраслях) полномасштабной системы единых классификаторов, словарей, нормативно-справочной информации — мы это включаем в состав онтологических моделей деятельности. Как я ранее отметил, если мы не опишем такие модели, то будет сложно построить равнопрочную систему защиты. Только через понимание модели деятельности можно выйти на понимание уязвимостей и рисков; сначала необходимо описать структуру деятельности, а потом обеспечивать ее безопасность. Этим РКСС и занимается. Мы пошли не от технологий, а от понимания самого процесса, точнее — от понимания взаимосвязи целого комплекса процессов: технологических, экономических, обеспече-

ния безопасности. Эту взаимосвязь мы сегодня должны обеспечить и сделать ее защищенной.

Такая работа сегодня ведется в тесном взаимодействии с предприятиями Госкорпорации «Ростехнологии» и ее холдингами, в частности с ОАО «Росэлектроника» — нашей материнской компанией.

**— Вы говорите о ТЭК в целом. Есть ли у вас проекты с нефтяными и газовыми компаниями?**

— С ними идут активные переговоры и планируются серьезные проекты, мы также надеемся выйти с ними и на комплексные проекты в области безопасности, используя наш задел в электроэнергетике.

Также хотелось бы отметить, что мы входим в состав технологической платформы «Интеллектуальная энергетическая система России» и принимаем активное участие в перспективных научно-исследовательских и опытно-конструкторских работах по развитию интеллектуальной электрической сети России. Это некий аналог систем Smart Grid — интеллектуального управления энергетикой, которые активно распространяются сегодня во всем мире. Мы планируем войти в формируемую сейчас платформу по обеспечению безопасности объектов промышленности и ТЭК. Недавно у нас была очень продуктивная встреча с ее организаторами, где мы обратили внимание на то, что при создании этой платформы необходимо учитывать вопросы обеспечения информационной безопасности.

Отрасль ТЭК стала ИТ-зависимой, сегодня даже небольшие устройства имеют IP-адреса. В свое время ответственные за безопасность радовались простоте устройств нашего ТЭК, тому, что для своей работы они не требуют подключения к телекоммуникационным сетям. Ситуация изменилась. Умные сети требуют подключения к мощным сетям связи, а значит, и обеспечения информационной безопасности всех систем, участвующих в этом процессе.

Очень хороший пример уязвимости ТЭК — вирус, проникший на объекты энергетики одной из стран Ближнего Востока. Мы не будем сегодня обсуждать, кем он был создан, но он демонстрирует, насколько уязвимы критически важные объекты ТЭК и то, что их надо серьезно защищать.

**— Какие конкурентные преимущества компании РКСС вы бы выделили в работе на этом рынке?**

— Прежде всего, это возможность и практические результаты в области создания доверенного оборудования. Мы прошли достаточно сложный путь по созданию технологии (организационной и технической) взаимодействия между сертифицирующими органами и крупными мировыми вендорами с целью получения статуса доверенного оборудования. У нас есть опыт такой работы. Мы видим, что зарубежные лидеры ИТ-индустрии обращаются к нам как к экспертам по этим вопросам.

Естественно, абсолютного доверия достигнуть нельзя, процесс его построения никогда не заканчивается, а постоянно требует серьезных усилий, поскольку и оборудование, и версии ПО обновляются и совершенствуются. Но очень важно, что в процессе сотрудничества возникает доверие между партнерами.

Второе наше конкурентное преимущество — уход от понимания проблем безопасности в чисто техническом аспекте, мы говорим о них в аспекте управления компанией, причем управления — в широком смысле. Мы уже обратили ваше внимание на то, что РКСС обладает компетенцией в области разработки онтологических моделей крупных предприятий в самых разных отраслях промышленности, эти модели становятся основой для разработки систем обеспечения информационной безопасности, а также комплексных автоматизированных систем управления безопасностью, в том числе физической.

**— В России есть и другие критически важные сектора промышленности — транспорт, к примеру. Работаете ли вы с предприятиями этих секторов?**

— Да, работаем, но пока на уровень конкретных крупных проектов не вышли. Переговоры идут. Мы готовы предложить наши решения.

**— Какие угрозы в области информационной безопасности сегодня вы считаете наиболее опасными для тех отраслей, о которых мы говорили?**

— Очень непростой вопрос. Угроз много, они разные, и большое значение имеет вероятность их возникновения. Мировая статистика показывает, что очень серьезную угрозу представляют собой инсайдеры, которые могут изнутри провести определенные действия с оборудованием и ПО. При работе с доверенным оборудованием вероятность возникновения этой угрозы снижается. Инсайдеры просто не могут изменить режим работы оборудования внутри компании. Остальные угрозы достаточно хорошо известны.

**— Спасибо большое за очень интересное и содержательное интервью!** ■

# ЗАЩИЩЕННЫЙ КОНТЕНТ — это плохо, хорошо или относительно хорошо?

***Кристофер ШАУТЕН,***
*старший директор маркетинговых решений компании Irdeto*

**Обозреватели в области информационных технологий, такие как активист и журналист Кори Доктороу (Cory Doctorow), высказывают утопичную точку зрения, касающуюся медиаиндустрии, утверждая, что технические средства защиты контента (DRM) — это зло, и все средства массовой информации должны быть свободными и неконтролируемыми, для всеобщего удовольствия и безопасности. Из этого следует, что отрасль находится в переходном состоянии, и хотя взгляды на DRM как на отрицательное явление необоснованны, потребители хотят более свободного и гибкого использования премиум-контента.**

Представьте себе, что теория, согласно которой все средства массовой информации должны быть свободными и бесплатными, воплощена в жизнь. Но ведь просто невозможно, чтобы деньги, инвестированные в производство, и предоставление соответствующих товаров и услуг, были эффективно возвращены через данную модель. Примеры артистов, следующих модели бесплатных медиа, скорее являются исключением из правил. Трудно признать, что подход, основанный на доверии, использованный музыкантом и программистом Джонатаном Колтоном (Jonathan Coulton), был более выгодным, чем традиционная бизнес-модель.

Многомиллиардные киноиндустрии, такие как Голливуд, которые недавно начали предоставлять контент на мобильные платформы с использованием DRM, никогда бы не смогли оправдать вкладываемые инвестиции в создание блок-бастеров, применяя для продаж только подход, основанный на доверии. Торговля в силу своей природы веками полагалась на способность бизнеса уверенно рассчитать инвестиции, необходимые для создания продукта, и доход, который бизнес получит от его продажи. Любые радикальные перемены в этой модели не будут работать в крупных масштабах, потому что культурные изменения, необходимые для этих перемен, слишком велики. Чтобы преодолеть их, понадобится не одно поколение.

Так как же найти баланс между «контент везде и на любом устройстве» и необходимостью компаний получать доход за свой контент? К счастью, на сегодняшний день существуют факторы, которые могут разрешить данную ситуацию. Мир приложений, в котором мы сейчас живем, устроен следующим образом: если вы покупаете электронную книгу у провайдера, например Amazon, то впоследствии вы сможете использовать эту электронную книгу на любом устройстве, поддерживающем Kindle-платформу, от компании Amazon или на приложении Kindle на вашем смартфоне с платформами Apple, Android и Windows. Поэтому если вы меняете устройства, то ваш контент следует за вами. При переходе к другому провайдеру вы также не потеряете доступ к вашему контенту: для доступа к нему вам просто необходимо будет открыть другое приложение, использующее DRM, что необходимо компаниям для гарантированного возвращения инвестиций.

Сидящему внутри всех нас ребенку хочется думать, что мы должны получать все бесплатно, но мир устроен не так, и никогда не был так устроен. То, что ценно, должно быть продано по соответствующей цене. То, что желаемо, должно быть заработано. То, что драгоценно, должно быть защищено. Технология защиты контента — это и есть выражение данного базисного принципа. ■

# ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ: ЕДИНОЕ ЭЛЕКТРОННОЕ СНГ

***Евгений ИВАНОВ***

В рамках юбилейной Межгосударственной выставки, посвященной 20-летию Содружества Независимых Государств, которая прошла на территории Всероссийского выставочного центра, Исполнительным комитетом СНГ и Деловым центром экономического развития СНГ 29 июня 2011 года был организован и проведен научно-практический симпозиум «Информационно-коммуникационные технологии: единое электронное СНГ», на котором обсуждались вопросы формирования единого информационного пространства государств Содружества.

В работе симпозиума приняли участие специалисты в области информационных технологий, руководители научных, конструкторских, промышленных организаций. По общему мнению представителей государственных органов управления и руководителей компаний, необходимо полностью реализовать возможности информационного пространства СНГ и проводить согласованную политику в развитии ИТ. Лейтмотивом докладов прозвучала тема о том, что формирование единого информационного пространства государств — участников СНГ можно обеспечить только при взаимодействии национальных информационных пространств стран Содружества на взаимовыгодной основе, с учетом национальных и общих интересов в деле развития сотрудничества в согласованных сферах деятельности.

Симпозиум рассмотрел широкий круг вопросов, касающихся разработки программно-информационного обеспечения, предоставления инжиниринговых, консалтинговых, технологических и иных услуг, внедрения единой системы электронной транспортной логистики. Организации, специализирующиеся на разработке и эффективном управлении инвестиционными проектами, проинформировали о своих достижениях в следующих областях:

• внедрение технологий электронного обмена деловой и ком-

мерческой информацией на базе объединения и взаимодействия отраслевых и национальных телекоммуникационных и телепатических систем;

• создание интегрированной распределенной информационной системы и портала «Информация для научно-технической и инновационной деятельности государств — участников СНГ»;

• создание информационных ресурсов для государственных и местных органов власти;

• разработки систем обеспечения удаленного доступа граждан к информации о деятельности государственных органов на основе использования информационно-коммуникационных технологий.

Руководители и главные конструкторы проектных организаций предоставили материалы, наглядно характеризующие возможности в следующих направлениях:

• разработка программного обеспечения, создание сложных телекоммуникационных систем, в частности специальных приложений и компьютерной техники;

• внедрение современных электронных технических средств и программного обеспечения для преобразования, хранения, защиты, обработки, передачи и безопасного получения информации;

• создание современной платформы, позволяющей разрабатывать программные продукты специального назначения для различных целей, включая информационные системы государственного управления, военного назначения.

В заключительной части Международного научно-практического симпозиума прошло обсуждение результатов его работы и были отмечены такие существенные факты, как:

• значительное увеличение роли информационных знаний, информационно-коммуникационных технологий в повседневной жизни общества всех государств — участников СНГ;

• возрастание удельного веса информационно-коммуникационных секторов и, соответственно, повышение доли в сегменте информационных технологий, секторе электронных коммуникаций, а также в производстве информационных продуктов и оказании информационных услуг;

• повышение показателей информатизации общества;

• интеграция в глобальное информационное пространство, доступ к мировым и национальным информационным ресурсам;

• частичная или полная замена ряда услуг, требующих физического присутствия человека, на виртуальные и дистанционные услуги.

Особо была отмечена необходимость формирования современной информационной и телекоммуникационной площадки, представление на ее основе качественных услуг и обеспечение высокого уровня доступности информации для субъектов стран СНГ.

При подведении итогов работы симпозиума все выступавшие подчеркивали, что он стал хорошей площадкой для обсуждения новых идей и направлений исследований во всех областях внедрения информационных технологий, и поручили Деловому центру экономического развития СНГ создать информационно-коммуникационную площадку деловых кругов СНГ. ■

*По материалам пресс-центра НП «Деловой центр экономического развития СНГ»*

МОБИЛЬНЫЕ ТЕЛЕКОММУНИКАЦИИ

# Карта бесплатной подписки квалифицированного специалиста

Для получения статуса квалифицированного подписчика необходимо ответить на все вопросы настоящей анкеты.
Заполнив данную карту, вы получите бесплатно три выпуска журнала, начиная с момента получения редакцией анкеты.
Анкету необходимо заполнять разборчиво, печатными буквами.
С отдельными публикациями журнала можно ознакомиться на сайте: **www.mobilecomm.ru**

**Заполните и отправьте по факсу +7 (495) 502-92-64**

Фамилия_____

Имя_____

Отчество_____

Должность_____

Название организации_____

HTTP://_____

Страна_____

Индекс_____

Почтовый адрес_____

Телефон_____

Факс_____

E-mail:_____

## ДЛЯ ОФОРМЛЕНИЯ ПОДПИСКИ, ПОЖАЛУЙСТА, ОТВЕТЬТЕ НА 2 ВОПРОСА.

**1. Сфера деятельности вашей организации:**

- ☐ Оператор мобильной связи стандарта:
- ☐ GSM
- ☐ CDMA
- ☐ AMPS/DAMPS
- ☐ NMT-450
- ☐ Прочее
- ☐ Оператор пейджинговой связи
- ☐ Оператор профессиональной радиосвязи
- ☐ Оператор спутниковой связи
- ☐ Интернет-провайдер
- ☐ Системный интегратор
- ☐ Разработчик ПО
- ☐ Производитель телекоммуникационного оборудования
- ☐ Дистрибьютор/Дилер/Реселлер
- ☐ Салон связи/Розница
- ☐ Банк/Финансовая компания
- ☐ Консалтинговая компания
- ☐ Правительство/Государственное учреждение
- ☐ Силовые структуры/МЧС
- ☐ Машиностроение
- ☐ ТЭК
- ☐ Транспорт
- ☐ Образование
- ☐ СМИ
- ☐ Прочее

**2. Занимаемая должность**

- ☐ Руководитель предприятия
- ☐ Руководитель технической службы/службы связи
- ☐ Руководитель коммерческой службы/отдела продаж
- ☐ Руководитель службы маркетинга/рекламы
- ☐ Руководитель финансовой службы
- ☐ Менеджер по маркетингу
- ☐ Консультант
- ☐ IT-менеджер
- ☐ Менеджер по продукции
- ☐ Системный инженер
- ☐ Прочее