Деловой журнал | Телеком • ИТ • Медиа | www.iksmedia.ru

ИнформКурьер-Связь

ИКС

издается с 1992 года

№ 6-7 • июнь-июль • 2014

БУДЬ ИНФО БДИТЕЛЕН!

ТЕМА НОМЕРА

Конференция IT & Med`2014

ИТ-помощь медицине

Для профессионалов в области ИТ и здравоохранения

21 ноября 2014 г., Москва, гостиница «Холидей Инн Лесная»

К участию приглашаются:

- информатизаторы здравоохранения
- представители регулирующей сферы
- врачи
- руководители ИТ-направлений и ИТ-специалисты государственных и коммерческих медицинских учреждений
- общественные организации
- ИТ-компании, принимающие участие в проектах в сфере здравоохранения или заинтересованные в развитии бизнеса в этой сфере

IT & Med
ИТ-ПОМОЩЬ МЕДИЦИНЕ

Вопросы для обсуждения и выступлений (список открыт):

- как сделать ИТ-проект в здравоохранении эффективным. Критерии ИТ-эффективности в медицине
- каковы критерии качества решений для информатизации здравоохранения
- формирование электронной ресурсной базы здравоохранения, электронный документооборот, электронная карта, регистратура, другие базовые е-сервисы
- успехи информатизации коммерческой медицины. Есть ли смысл использовать подходы в бюджетной сфере?
- кадровый вопрос информатизации и фигура информатика. Где черпать кадры?
- реально ли реализовать требования закона «О персональных данных» в медучреждении
- соплатежи населения как резерв развития медучреждений
- телемедицина как инструмент доступности услуг и единого высокого стандарта здравоохранения
- роль дата-центров и инфраструктурных решений в повышении эффективности информатизации здравоохранения

Предложения по докладам ждем по адресу nk@iksmedia.ru

www.itmedforum.ru

ИКС МЕДИА

По вопросам участия обращайтесь по тел.: +7 (495) 785-14-90, 229-49-78 и e-mail: expo@iksmedia.ru

Партнеры

DELTA Smarter. Greener. Together.

АБИТЕХ абсолютная техника

POWERCOM Complete Power Solution

Издается с мая 1992 г.

Издатель
ЗАО «ИКС-холдинг»
Ю.В. Овчинникова

Генеральный директор
Д.Р. Бедердинов – dmitry@iks-media.ru

Учредители:
ЗАО Информационное агентство «ИнформКурьер-Связь»,
ЗАО «ИКС-холдинг»,
МНТОРЭС им. А.С. Попова

Главный редактор
Н.Б. Кий – nk@iks-media.ru

РЕДАКЦИОННЫЙ СОВЕТ
А.Ю. Рокотян – председатель
С.А. Брусиловский, Ю.В. Волкова,
А.П. Вронец, М. Ю. Емельянников,
Ю.Б. Зубарев (почетный председатель),
Н.Б. Кий, А.С. Комаров, К.И. Кукк,
Б.А. Ластович, Г.Е. Монина, Н.Н. Мухитдинов,
Н.Ф. Пожитков, В.В. Терехов, А. В. Шибаев,
И.В. Шибаева, В.К. Шульцева,
М.А. Шнепс-Шнеппе, М.В. Якушев

РЕДАКЦИЯ
iks@iks-media.ru

Ответственный редактор
Н.Н. Шталтовная – ns@iks-media.ru

Обозреватели
Е.А. Волынкина, А.Е. Крылова,
Л.В. Павлова

Редактор
Е.В. Харитонова – eh@iks-media.ru

Дизайн и верстка
Д.А. Поддъяков, А.Н. Воронова

КОММЕРЧЕСКАЯ СЛУЖБА
Г. Н. Новикова, коммерческий
директор – galina@iks-media.ru
Ю. В. Сухова, зам. коммерческого
директора – sukhova@iks-media.ru
Е.О. Самохина, ст. менеджер – es@iks-media.ru
Д.Ю. Жаров, координатор – dim@iks-media.ru

СЛУЖБА РАСПРОСТРАНЕНИЯ
А.С. Баранова – выставки, конференции
expo@iks-media.ru
С.С. Агуреева – подписка
podpiska@iks-media.ru

Журнал «ИнформКурьер-Связь» зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций 25 февраля 2000 г.; ПИ № 77-1761.

Адрес редакции и издателя:
127254, Москва,
Огородный пр-д, д. 5, стр. 3
Тел.: (495) 785-1490, 229-4978.
Факс: (495) 229-4976.
E-mail: iks@iks-media.ru
Адрес в Интернете: www.iksmedia.ru

№ 6-7/2014 подписан в печать 05.06.14.
Тираж 15 000 экз. Свободная цена.
Формат 64x84/8

ISSN 0869-7973

12+

Каждый занят своим делом. Люди (как минимум 55%) сидят в инете – часто с перебором. Государство регулирует – с избытком. Медиабизнес будирует и протестует – с эмоциями и накалом.

Российская и международная hi-tech-общественность, каждая по-своему, ощущают себя на виртуальных баррикадах борьбы за свободу жизни в Сети. И признают эту позиционную борьбу одной из самых тяжелых в сегодняшнем мире – Актуальный комментарий, Будущее уже здесь, О степенях свободы. Страшно далеки они от народа.

Жизнь дана нам в ощущениях. Этот тезис воспроизводится снова и снова. Например, профильное ведомство считает, что осуществляет реформу отрасли связи. И в качестве главного шага на этом пути называет переносимость номера, заявляя, что «MNP в России реально работает и оказывает реальное влияние на конкуренцию на рынке услуг подвижной связи». Притом, что на момент произнесения главой отрасли этих слов (13 мая с.г., итоговая расширенная коллегия Минкомсвязи) было перенесено 218 тыс. номеров – 0,089% от числа симок в стране за пять месяцев действия MNP. Это ли реальная работа и реальное влияние на конкуренцию?

Спустя лет шесть после завершения первого этапа внедрения универсального обслуживания на основе «реймофонов» регулятор определился с направлением развития универсальной услуги, впрочем, очевидным и звучавшим давно, – ШПД в населенные пункты от 500 человек (Рожденные регулятором). Единственный теперь оператор универсальной услуги, оператор всех услуг «Ростелеком» берет на себя дополнительные обязательства дать широкополосную связь в места, где живут более 250 человек. На горизонте цифрового разрыва возникла новая зарубка, которая за десять лет должна быть сведена к нулевой отметке, – 1300 сел и малых городов России, где нет связи, кроме красно-синего универсального таксофона.

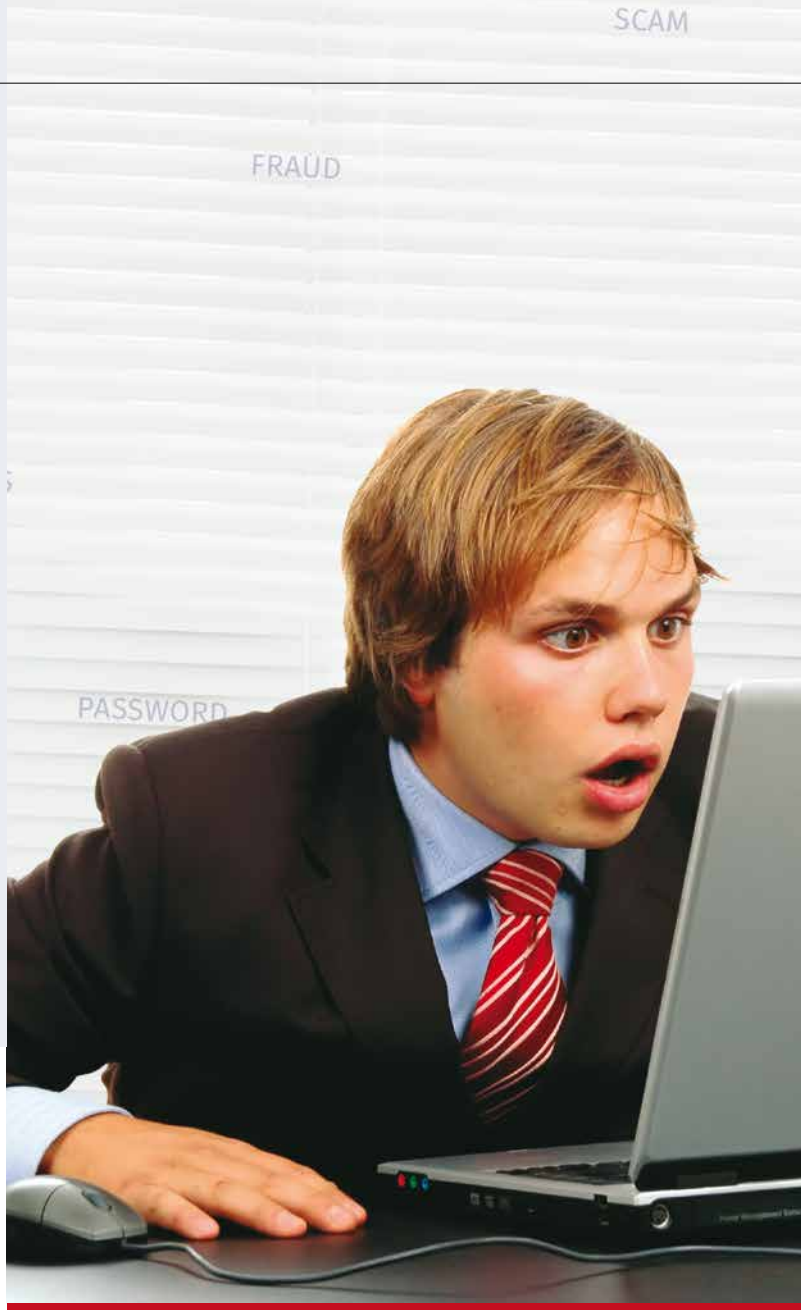
С не меньшими задержками, уже не раз обсуждавшимися на уровне вице-премьеров и выше, внедряется система «112». Спасительные цифры «112» – это не только замена с детства знакомых «01», «02», «03», «04», но и целый механизм обеспечения безопасности и помощи людям в городах, деревнях, на дорогах и в бездорожье. Цена его отсутствия еще пятилетку назад посчитана в самых важных в человеческом мире категориях. Но система «112» продолжает существовать в проектном режиме в десяти субъектах Федерации и в промышленной эксплуатации – в двух (в Татарстане и Курской области). Очередной срок запуска спасительного механизма обозначен 2017 годом.

Связь, отладившая бизнес до автоматизма, продолжает движение в социальном направлении. Оно и правильно, и человеколюбиво. Только ме-едленно.

До встречи.
Наталия Кий,
главный редактор

9
Т. ЗАРУБИНА.
Профессор с характером

15
Инерция взамен концепции



54 ДЕЛО

75 «ИКС» proТЕХнологии

Гуру

43 Д. КОСТРОВ. Заметки по практической психологии

Модель

45 С. СМОЛИН. «Лучше пять раз объяснить, чем один раз чинить»

Аналитик

47 Т. ФАРУКШИН. Тратить нельзя экономить

Подробности

48 П. ВОЛКОВ. Как найти то не знаю что

Дискуссионный клуб «ИКС»

50 Будни «дневных дозорных»

contents

How can IKS help YOU succeed in the Russian market?

9
T. ZARUBINA.
Professor with character

15
Inertness instead of conception

актуальный комментарий

Интрига планетарного масштаба

Подготовила
Александра КРЫЛОВА

Интернет – это объект, за равноправный доступ к управлению которым бьются многие страны, включая Россию. Очередной раунд этой борьбы ожидается уже этой осенью на Полномочной конференции МСЭ.

Вчера и сегодня

Создание в 1998 г. в США некоммерческой частной организации – Корпорации по присвоению имен и адресов в интернете (ICANN) – не отменило желания целого ряда других государств участвовать в управлении интернетом. На протяжении десятилетия вопрос об обеспечении равных прав всех стран в этом процессе поднимался с завидным постоянством. А в прошлом году Эдвард Сноуден своими разоблачениями спецслужб США вывел эти дискуссии на новый виток, вызвав всплеск интереса к проблеме со стороны как развитых стран, например, Германии, так и стран БРИК – Бразилии и России.

В настоящее время в управлении интернетом, помимо ICANN, участвуют и другие международные организации – IETF (Рабочая группа по проектированию интернета), ISOC (Общество интернета), W3C (Консорциум Всемирной паутины). У каждой из них свои задачи. Однако нет в этом ряду такой, которая занималась бы разработкой международных норм в области управления инфраструктурой интернета, координацией деятельности и взаимодействия профессиональных международных институтов. Собственно, об этом и говорил в выступлении на глобальной конференции по вопросу управления интернетом NETmundial-2014 министр связи и массовых коммуникаций России Николай Никифоров. Он предложил создать под эгидой ООН специальную организацию для решения этих задач или наделить такими функциями Международный союз электросвязи.

Как известно, МСЭ – это организация, которая за 149 лет своей истории выработала уникальную методику согласования позиций множества своих участников (на сегодняшний день в нее входят 193 страны и более 700 коммерческих организаций) по вопросам внедрения и развития самых перспективных технологий, а также использования радиочастотного спектра и геостационарных орбит. И Россия, как одна из стран ее учредивших, к тому же на протяжении многих лет вносившая интеллектуальный и финансовый вклад в ее деятельность, вправе рассчитывать на то, что позиция ее администрации связи будет услышана.

В обозримом будущем

Нынешний год весьма подходит для достижения этой цели: в октябре–ноябре в Пусане (Республика Корея) пройдет Полномочная конференция, на которой, помимо выборов генерального секретаря и его заместителя, директоров Бюро, членов Радиорегламентарного комитета, а также государств – членов Совета МСЭ, будут обсуждаться стратегические вопросы развития отрасли ИКТ на ближайшие четыре года. В их числе заявлены вопросы управления интернетом, обеспечения безопасности пользователей в Сети и их доверия ей, развития нового поколения технологий подвижной связи.

Отдельным пунктом в повестке Полномочной конференции значится рассмотрение отчета рабочей группы Совета по пересмотру устава и конвенции этой организации. По словам Валерия Тимофеева, советника генерального секретаря МСЭ, необходимость внесения изменений в основные документы Союза вызвана длительными и сложными национальными процедурами ратификации, из-за которых многие страны-члены формально живут по разным версиям устава и конвенции, так как внесенные в последние десятилетия поправки далеко не всеми странами были ратифицированы. Резолюция 163, принятая Полномочной конференцией МСЭ в 2010 г., поручила рабочей группе Совета пересмотреть и скорректировать эти документы. Цель – создать такой текст устава, который не нуждался бы в пересмотре на каждой Полномочной конференции, а был бы утвержден и ратифицирован раз и навсегда, и новую Конвенцию, которая была бы гибкой и не требовала формальной ратификации странами – членами Союза после каждой Полномочной конференции. Российская делегация принимала активное участие в деятельности рабочей группы и подготовке ее итогового отчета, который будет представлен осенью нынешнего года в Пусане.

Однако ожидать появления в этих документах пунктов, так или иначе связанных с управлением интернетом, не следует. Поскольку за каждым решением Полномочной конференции стоят серьезные интересы и большие деньги, для его принятия требуются и длительная работа в исследовательских комиссиях, и на-

пряженные усилия по согласованию позиций, которые, по большому счету, еще только предстоит приложить. О том, что договориться со всеми участниками МСЭ будет не так просто, свидетельствует тот факт, что на Всемирной конференции по развитию электросвязи–2014 в Дубае США и некоторые другие страны отказались подписать заключительный акт.

О компетенциях и возможностях

Вот потому и настраивается на участие в неизбежной дискуссии генеральный секретарь МСЭ Хамадун Туре, под руководством которого подготовка к Полномочной конференции в Пусане ведется в последний раз. На встрече с журналистами он повторяет свой ключевой посыл, с которым обратился к участникам NETmundial–2014: «Управление интернетом не должно находиться в руках одной страны, одного учреждения или организации: это непосильная ноша. Такая работа должна вестись на всеобъемлющей основе и быть абсолютно открытой и прозрачной».

На сегодняшний день деятельность МСЭ по разработке технических стандартов и регламентов, в том числе в области широкополосного доступа, взаимно дополняет работу других организаций, в ведении которых находятся те или иные аспекты регулирования интернета. С этой функцией МСЭ много лет успешно справляется, и генеральный секретарь союза не видит оснований для отказа от нее.

А вот регулировать содержательную сторону интернета (именно в таком стремлении подозревают МСЭ представители крупнейших американских и западноевропейских интернет-компаний, говоря, что оно приведет к установлению тотального контроля со стороны отдельных государств за распространением информации в Сети, к запрету и блокировке доступа к отдельным ресурсам) эта международная организация, по уверениям Х. Туре, не собирается. Как, впрочем, не собирается она брать на себя решение юридических вопросов. «Наша задача – обеспечить людям широкополосный доступ, – заявил Х. Туре, – определить политику этого доступа, его регламентные аспекты и обеспечить инвестиции. Другие вопросы к нашей компетенции не относятся».

Да и в целом вопрос управления интернетом, считает В. Тимофеев, которого господин Туре называет своим учителем, несколько выходит за рамки МСЭ. Хотя ответ на него можно найти, если отбросить политические коннотации и, не углубляясь в технические вопросы, выработать для интернета порядок, подобный хорошо зарекомендовавшему себя механизму разрешения противоречий в области радиосвязи. В этом сегменте у администрации связи, оказавшейся втянутой в конфликтную ситуацию, есть возможность обратиться в Бюро радиосвязи, затем в Радиорегламентарный комитет и, если и там компромисса достичь не удалось, выйти с наболевшим вопросом на Всемирную конференцию радиосвязи. В мировой интернет-индустрии подобных механизмов до сих пор не существует, а потому страна, которую по той или иной причине «отключили» от интернета, не знает, к кому ей обращаться за помощью. И все-таки, поскольку вопрос управления интернетом несколько шире, чем функции МСЭ, то решение Полномочной конференции по его поводу, если оно все-таки состоится, будет иметь вид рекомендаций или поручения. «Возможно, его нужно вынести на обсуждение на высшем уровне – на Генеральную Ассамблею ООН, – предполагает В. Тимофеев, – чтобы она, в свою очередь, поручила генеральному секретарю МСЭ проработать вопрос о введении международного регулирования интернета. А уж наша организация с этой задачей, несомненно, справится».

Вода камень точит

Пока же исследовательские группы Международного союза электросвязи, в которых участвуют представители разнообразных коммерческих компаний – поставщиков оборудования, операторов связи и сервис-провайдеров, работают над более приземленными вопросами на подступах к проблеме управления интернетом, в том числе в области регулирования взаимодействия традиционных телефонных и IP-сетей.

Например, Дмитрий Черкесов, представляющий интересы российского оператора связи МТТ, является заместителем председателя рабочей группы, занимающейся распространением глобальных, не привязанных к стране ресурсов нумерации. Такая нумерация позволяет осуществлять звонки из облака пользователей VoIP-сервисов и совершенно законно «приземлять» их на телефонную сеть общего пользования, и в обратном порядке – принимать звонки из ТфОП любому такому облачному абоненту.

Компания МТТ, получившая от МСЭ 1 млрд таких негеографических номеров, выделяет однозначный идентификатор из диапазона номерной емкости в коде +883 140, что делает звонки 25 млн своих пользователей на ТфОП «понятными» для операторов связи во всем мире. Недавно оператору удалось добиться разрешения на безвозмездную передачу части принадлежащих ему негеографических телефонных номеров другим поставщикам VoIP-услуг. Тем самым МТТ обеспечивает себе возможность наращивания абонентской базы и объема трафика в сети, а заодно расширяет круг игроков операторского рынка, которые перестанут бояться номеров серии +883 и начнут более активно прописывать их на своих сетях.

Иными словами, пока на глобальном уровне дискутируется вопрос, кому управлять инфраструктурой интернета, процесс налаживания взаимодействия традиционных операторов и поставщиков голосовых сервисов участникам сетевых (читай, интернет-) сообществ сдвинулся с места.

Поможет ли это разрешению главной интриги? Как говорится, вода камень точит.

Женева – Москва

О перипетиях законодательного наступления на Рунет → см. с. 20 и 23.

Человеческий фактор – самое слабое звено информационной безопасности. Но это точно не относится к нашим профи – гостям рубрики, участникам ТЕМЫ НОМЕРА (➔ с. 34–53 ➔).

Павел ГОЛОВЛЕВ, начальник службы информационной безопасности, СМП Банк

Родился в 1969 г. в Ленинграде. В 1991 г. окончил Военный инженерно-космический краснознаменный институт имени А.Ф. Можайского по специальности «радиоэлектронные средства». Имеет дополнительное образование по направлениям «безопасность информационных технологий», «финансовый менеджмент» и «менеджмент в сфере электронного бизнеса и интернет-проектов».

В банковской сфере с 1999 г. Работал в ОАО «ТрансКредитБанк», где принимал непосредственное участие в создании системы интернет-банкинга.

С 2010 г. работает в СМП Банке, занимается проблемами информационной безопасности, защиты персональных данных и противодействия высокотехнологичным видам мошенничества.

Является членом Ассоциации руководителей служб информационной безопасности и экспертом ассоциации BISA.

Александр ХРУСТАЛЕВ, директор департамента информационной безопасности, МГТС

Родился в 1986 г. в Москве. В 2009 г. окончил Московский государственный институт радиотехники, электроники и автоматики по специальности «радиотехника». Карьеру в сфере информационной безопасности в телекоме начал в 2008 г.

В июне 2010 г. был назначен руководителем группы информационной безопасности телекоммуникационных и радиосистем МТС, с 2011 г. – директор по проектам.

В марте 2012 г. перешел в МГТС на должность директора департамента информационной безопасности, которую занимает в настоящее время.

Алексей РАЕВСКИЙ, генеральный директор, Zecurion

Родился в 1973 г. в Москве. Окончил Московский государственный инженерно-физический институт (ныне – Национальный исследовательский ядерный университет «МИФИ») по специальности «прикладная математика» и аспирантуру Московского института электроники и математики (МИЭМ). Кандидат технических наук.

До 2001 г. участвовал в разработке систем защиты ПО от несанкционированного копирования и систем защиты информации от несанкционированного доступа.

В 2001 г. основал компанию Zecurion и в настоящий момент является ее гендиректором.

С 2004 г. – член Ассоциации защиты информации, а с 2008 г.– член IEEE.

С 2007 г. читает курс лекций по основам информационной безопасности для студентов МИЭМ. Награжден почетным дипломом Российской академии наук за большой вклад в развитие информационных технологий в России.

Павел ВОЛКОВ, эксперт по информационной безопасности, «Открытые Технологии»

Родился в 1974 г. Базовое образование – радиотехническое, специализировался на обработке информации с систем дистанционного зондирования Земли.

Информационной безопасностью профессионально занимается с 2000 г. В компании «Открытые Технологии» в 2004 г. руководил отделом информационной безопасности. В настоящий момент здесь же возглавляет Центр компетенции по управлению операционными рисками.

Профессиональные интересы: применение технологии Big Data, алгоритмы обнаружения аномалий и прогнозирования поведения сложных систем, системы моделирования векторов атак (SRM/SPM).

Татьяна ЗАРУБИНА

Профессор с характером

Судьба благоволит тем, кто видит цель и не видит препятствий. Татьяна Васильевна ЗАРУБИНА, завкафедрой медицинской кибернетики и информатики РНИМУ им. Н.И. Пирогова, как никто иной, знает об этом.

Теплое детство

Папа преподавал старшеклассникам историю и обществоведение в одном из райцентров Волгоградской области, где и жила семья. Мама учила детей русскому языку и литературе. «Отец был прирожденный учитель. Несмотря на его строгость, дети его очень любили, – рассказывает Татьяна Васильевна, – он много занимался с учениками, возил их на экскурсии, иногда дальние. Меня, свою младшую дочь, он любил безмерно, и это мне очень помогает в жизни: в моем окружении много мужчин».

Своей маме Татьяна Васильевна благодарна за то, что она научила ее писать сочинения: «Я до сих пор с удовольствием пишу письма, научные работы, статьи. Для меня это большое счастье – сесть в тихом месте и погрузиться в написание чего-либо».

Отличница поневоле

Учеба давалась Тане легко, самыми любимыми предметами были математика и химия. «Татьяна Михайловна, преподававшая нам алгебру и геометрию, фактически вела меня по отдельной программе, – вспоминает Татьяна Васильевна. – Первые десять минут я с классом решала контрольную, сдавала ее и получала задания совсем другого уровня сложности». Так по инициативе учителя девушка прошла программу заочной математической школы при МГУ.

За год до окончания школы Таня заявила, что не хочет получать золотую медаль, чтобы не давать повода к досужим разговорам: ведь она училась в школе, где работали ее родители. Но поскольку учеба на отлично вошла в привычку, остаться без медали у нее не получилось.

На выбор профессии повлияла книга А. Беляева «Голова профессора Доуэля». В ней Таня с удивлением отметила для себя, что по параметрам, снимаемым с отдельной части организма, можно делать вывод о его состоянии в целом и даже пытаться этим состоянием управлять. «Сама идея мне настолько понравилась, – признается Татьяна Васильевна, – что я начала прицельно искать место, где этому учат, и нашла медико-биологический факультет 2-го Московского ордена Ленина государственного медицинского института им. Н.И. Пирогова». Вопрос о специальности отпал сразу, как только взгляд упал на строчку «медицинская кибернетика».

Поступление, несмотря на высокий конкурс, Тане обеспечила та самая золотая медаль: первый и единственный экзамен по математике она сдала на пятерку.

Инициатива не наказуема

Поначалу учиться в институте было сложно, поскольку, помимо математики, в программу входили биологические дисциплины, которые нужно было зазубривать. Когда первые трудности были позади, на смену им пришли сомнения в правильности выбора, пока на четвертом курсе не появилось твердое желание создавать программные средства для клинической практики. Однако для того чтобы специализироваться по этому направлению, ей сначала пришлось заручиться поддержкой ректора Волгоградского мединститута. Недолго думая, она прилетела в Волгоград, нашла вуз, пришла туда и прямо «с улицы» направилась к ректору, который неожиданно ее принял. «Я сказала, что у меня редкая профессия и что, поскольку я из районного центра Волгоградской области, меня после окончания распределят в их институт, что я хочу заниматься разработками в клинической практике, но для этого нужно письмо за подписью ректора с просьбой о такой специализации», – вспоминает Татьяна Васильевна.

Ее настойчивость была вознаграждена. По возвращении в свой вуз Татьяна была включена в команду Александра Георгиевича Устинова, которая на базе 57-й городской больницы впервые в стране разрабатывала компьютеризированную мониторную прикроватную автоматизированную систему для реанимации и интенсивной терапии кардиопульмонологического профиля. Эта работа дала материал сначала для диплома, а со временем, после того, как Татьяну направили из Волгограда на стажировку в Москву, и для кандидатской диссертации.

Платье вышивала сама

«Когда ко мне сегодня приходят студенты 5–6-го курсов с вопросом, куда лучше идти, – говорит Татьяна Васильевна, – я им отвечаю,

что неинтересных направлений у нас нет и вопрос нужно ставить не так. Не куда, а к кому». И вспоминает, какую важную роль в ее собственной профессиональной судьбе сыграл

Учитель

Им для Татьяны Васильевны стал основатель первой в России кафедры медицинской и биологической кибернетики Сурен Ашотович Гаспарян, нашедший время обсудить с ней уже в целом готовую кандидатскую диссертацию. «Он указал мне на несколько проблем, – рассказывает она, – а я набралась смелости и сказала: “Это не все, по-хорошему нужно еще доделать тут и тут”». Обсуждение работы со всех сторон продолжалось шесть часов.

«Так и получилось, что пришла я к выдающемуся ученому, которого видела на пьедестале, а вышла от Учителя с пониманием, что в моей жизни случилось большое чудо», – резюмирует Татьяна Васильевна.

Учитель взял ее на кафедру ассистентом, а потом старался не сдерживать ее активность. К концу 80-х Татьяна Зарубина, уже кандидат наук, стала лидером команды врачей-кибернетиков, которая на базе 31-й клинической больницы создавала программные средства для прогнозирования исхода заболевания, оценки его тяжести, изменения течения при применении новых препаратов...

«У меня никогда не было цели сделать докторскую диссертацию, –

говорит Татьяна Васильевна, – она сделалась сама: нужно было помочь ребятам из нашей команды поставить кандидатские, потом шестеро из них друг за другом защитились. И тут я увидела, что у меня получается стройная система». Ценность результатов подтвердил учитель, сказав, что это докторская. И во второй половине 90-х Т.В. Зарубина начала ее писать. Диссертацию «Управление состоянием больных перитонитом в раннем послеоперационном периоде» она защитила 7 мая 1998 г.

После защиты С. А. Гаспарян начал брать ее с собой на встречи. «За два года, – рассказывает Татьяна Васильевна, – он научил меня входить в кабинет и выходить из кабинета, держать лицо в любой ситуации, даже когда это очень трудно, отвечать, если нужно, промолчать, когда требуется воздержаться от ответа».

Он сознательно готовил себе смену. А когда увидел, что любимая ученица все усвоила, передал в ее руки кафедру. «К моменту его ухода навсегда я уже третий год была заведующей, – говорит она и добавляет: – Вспоминается Сурен Ашотович очень светло, я по нему до сих пор скучаю».

Растить людей

«Если человеку не нравится растить людей, – убеждена Татьяна Васильевна, – он не должен заведовать выпускающей кафедрой, он профессионально для этого непригоден».

Сегодня на кафедре медицинской кибернетики и информатики трудятся высококлассные разработчики медицинских информационных систем самого разного назначения – от обработки сигналов и изображений, поддержки принятия врачебных решений до информационно-аналитических систем территориального и федерального уровней. Татьяна Васильевна Зарубина вырастила нескольких кандидатов наук, способных выступить ответственными исполнителями проектов. А теперь готовит их к тому, чтобы они стали докторами и сами, в свою очередь, для кого-то учителями.

Блиц. После 21.00

– Как вы познакомились со своей второй половиной?

– С мужем мы вместе учились в институте, причем сблизились на последнем курсе – оказалось, что у нас похожие интересы. Он был ленинским стипендиатом, я уже много и серьезно работала. В феврале мы начали встречаться, а в ноябре поженились.

– Как вам удается совмещать активную многостороннюю профессиональную деятельность с семьей?

– Мой муж хорошо знал, на ком женится. К тому же мы оба реализовывались и старались друг друга в этом плане поддерживать. Он защитил кандидатскую диссертацию по пульмонологии в 1986 г., а я свою – в 1989-м. С докторской я его опередила, и после его защиты в 2004 г. наш сын-студент, сидя на кухне, говорил кошке: «Ксюша, в этом доме только мы с тобой не доктора наук». На самом деле мне, наверное, всю жизнь везет с мужчинами: они меня понимают. С сыном мы по-настоящему дружим всю жизнь: когда он был маленький, я старалась общаться с ним каждый день. Надеюсь, что с внуком, которому пока семь месяцев, тоже получится.

– Как вы восстанавливаете силы после недели работы по 10–12 часов?

– Воскресная прогулка по несколько часов в лесу, в лесопарке для меня – святое. Я люблю воду, особенно текущую. С удовольствием слушаю классическую музыку и хожу в хорошие театры не менее пяти раз за сезон. Люблю классическую живопись и обязательно хожу на выставки. Саврасов, Поленов, Левитан, Ге – это те художники, чьи выставки нам удалось посмотреть за последние годы. Но все эти любимые занятия строго подчинены профессиональным интересам.

У меня есть грустная шутка, что если меня отовсюду выгонят, то я, наконец, буду гулять по Москве, смотреть усадебные дома, прокладывать для себя интересные маршруты... Ведь и сегодня в столице можно найти исторические здания, особенно при привычке к научной работе.

Беседовала **Александра КРЫЛОВА**

Россия поменяет США на Китай

Вань Бяо, президент Huawei в России: «Информационные технологии – стратегический выбор для Huawei»

Компания Huawei объявила о том, что теперь основным фокусом ее развития станет ИТ-оборудование (системы хранения данных, решения для облачных вычислений и для дата-центров). Несмотря на то, что системы хранения – сравнительно новое для компании направление, по данным Gartner, в 2013 г. Huawei занимала 18% глобального рынка СХД, а в Китае она в этом сегменте лидирует. В частности, система ее OceanStor 18000 насчитывает более 150 внедрений в крупных организациях Китая.

В Huawei отмечают, что компания во всем старается обходиться своими разработками, активно привлекая партнеров по всему миру. Это касается как, например, технологий виртуализации, которые на серверах вендора реализованы на платформе Huawei FusionSphere, так и аппаратной части – по словам представителей компании уже следующая новинка в области серверов будет реализована не на процессорах Intel, а на процессорах собственной разработки.

В России для продвижения ИТ-решений Huawei создано специальное подразделение. Компания уже продемонстрировала в Москве серверное оборудование 3-го поколения и системы хранения данных корпоративного класса.

По словам партнеров Huawei на российском рынке, в связи с наблюдающимся политическим курсом успех вендора в области поставок ИТ-оборудования отечественным заказчикам вполне возможен. Сейчас большинство российских компаний работает с техникой американского производства, и именно она может попасть «под замену» в случае углубления конфронтации между Россией и США.

Возможности ИТ отстают от потребностей бизнеса

Такое положение вещей признают 66% руководителей ИТ-отделов в России. Это выяснилось в результате опроса, проведенного компанией VMware совместно с агентством Vanson Bourne в странах региона EMEA, Ближнего Востока и Скандинавии. Российский показатель почти совпал со средним по EMEA, в Великобритании уровень самокритики гораздо выше – 80%, а в Дании, наоборот, ниже – 48%. Выяснилось также, что реальные сроки запуска новых ИТ-решений отстают от запросов бизнеса в среднем на 5 месяцев.

Два в одном

«Триколор ТВ» ввел новую услугу «Мультирум», позволяющую абонентам просматривать контент на двух экранах в рамках одной подписки. Техническое решение предоставил инвестиционно-промышленный холдинг GS Group, выпустив по заказу «Триколор ТВ» комплект из двух цифровых приставок, дающий телезрителю доступ по одной смарт-карте к разному контенту оператора на двух телевизорах одновременно.

А. Старобинец: «В отличие от распространенных на рынке решений multiscreen «Мультирум» не требует от абонента ежемесячной оплаты просмотра контента на каждом из экранов»

Комплект состоит из двух цифровых ТВ-приемников – основного и дополнительного. Обе приставки обеспечивают прием HD- и SD-каналов форматов MPEG-4 AVC/H.264 и MPEG-2. При этом, по словам Андрея Безрукова, директора по стратегическому маркетингу GS Group, цена комплекта будет немногим выше стоимости одного приемника.

Услуга «Мультирум» будет доступна абонентам «Триколор ТВ» на территории центральной России, СФО и части территорий Урала и Дальнего Востока. Как сообщил Александр Старобинец, директор по маркетингу «Триколор ТВ», сервис разработан с учетом данных об объемах продаж и предпочтениях потребителей по числу телевизоров, установленных в домохозяйствах крупных городов России: в одном домохозяйстве, по данным Росстата, в среднем 2,6 человека; 85% домохозяйств крупных городов имеют два и более телевизора. Очевидно, что удовлетворение спроса семейного телесмотрения ограничено необходимостью приобретения двух приемников по стандартной стоимости и оформления двух подписок как на основную услугу, так и на дополнительные ТВ-пакеты.

С введением новой услуги оператор рассчитывает улучшить качество семейного телесмотрения в стране, отмечает А. Старобинец. Кроме того, по расчетам компании, введение этого сервиса, снижающего затраты домохозяйств на покупку оборудования и подписку, повысит лояльность абонентов и увеличит ARPU.

Новый игрок на рынке диаспор

Мобильный виртуальный оператор Aiva Mobile запущен в Таджикистане компанией МТТ. В рамках этого проекта, ориентированного на этнорынок, абонентам предлагается SIM-карта с двумя одновременно активными телефонными номерами – таджикским и российским. В зависимости от своего местонахождения абонент может пользоваться одним или другим номером для приема и совершения звонков по «домашним тарифам» без дополнительных манипуляций. Такая возможность обеспечивается благодаря технологии интеллектуальной маршрутизации МТТ.

Базовым оператором для «российской» составляющей проекта, предоставившим MVNO инфраструктуру радиодоступа, выступила компания МТС, к слову, не присутствующая в Таджикистане и рассчитывающая благодаря сотрудничеству с МТТ приобрести в этой стране абонентов. В Таджикистане и других среднеазиатских республиках (до конца текущего года Aiva Mobile появится еще в двух из них) в роли базовых операторов будут выступать локальные партнеры. Они же будут заниматься продвижением этого проекта.

Запуск федерального MVNO потребовал от МТТ инвестиций в коммутатор GMSC, HLR и в биллинговую систему. По словам Евгения Васильева, генерального директора компании, они составили несколько миллионов долларов. «С одной стороны, рынок этноуслуг достаточно интересный: ежегодно в Россию приезжают 5 млн мигрантов, – сказал он, – с другой – мы понимаем, что вся большая тройка на нем очень активна». Вот почему при создании Aiva Mobile оператор задался целью добиться, чтобы новый продукт отличался от всех, существующих на рынке, своим удобством. В итоге, абоненты MVNO могут не беспокоиться о замене SIM-карт в телефонах. Кроме того, Aida Mobile предоставит и другие услуги, например платежные сервисы.

Кадровые назначения

Минкомсвязь России
Алексей СОКОЛОВ назначен заместителем министра.

«Ростелеком»
Диана САМОШКИНА назначена исполнительным директором – директором по работе с массовым сегментом.

«Т2 РТК Холдинг»
Юрий СОЛОВЬЕВ назначен председателем совета директоров.

МТС
Игорь ЕГОРОВ назначен директором в Центральном федеральном округе.

«ВымпелКом»
Владимир САВКИН назначен директором по информационным технологиям.

МГТС
Ольга БЕЛОУСОВА назначена финансовым директором.

«Скартел» (Yota)
Анатолий СМОРГОНСКИЙ назначен гендиректором.

«Интерспутник»
Питер ВАРИ избран председателем совета.

Ксения ДРОЗДОВА переизбрана председателем эксплуатационного комитета.

РДТЕХ
Анатолий ВОЛКОВ избран гендиректором.

«Техносерв»
Андрей ХРУЛЕВ назначен руководителем департамента биометрических и комплексных систем безопасности.

ViewSonic
Илья БУДКЕВИЧ назначен директором по работе с корпоративными заказчиками в России и странах СНГ.

Intel
Дмитрий КАЛИТА назначен директором в Украине, Беларуси и Молдове.

Стивен ФАНД назначен вице-президентом и директором по маркетингу.

Nokia
Раджив СУРИ назначен президентом и главным исполнительным директором.

M&A

«Ростелеком» приобрел 26% уставного капитала **«Т2 РТК Холдинг».**

ФАС удовлетворила ходатайство **«Т2 РТК Холдинг»** о приобретении 100% голосующих акций **«РТ-Мобайл».**

МТС купила 45,71% голосующих акций воронежского оператора **«Телесервис»** и тем довела свою долю в «Телесервисе» до 100%.

«Банки.ру» приобрели сайт **Finparty.ru.**

«Кокос», Корпорация РБС, SEO Dream, Arrow Media, Media Guru и **Webprofy** объявили об объединении в рамках **ГК Kokoc Group.**

ФАС удовлетворила ходатайство **«Озон холдингс лимитед»** о приобретении прав, позволяющих определять условия осуществления предпринимательской деятельности компании **«ЛитРес».**

Microsoft завершила приобретение подразделения Devices & Services компании **Nokia.**

Магические 5%

Именно на такую величину изменились основные финансовые показатели деятельности МТС в I квартале 2014 г. Общая выручка Группы МТС во всех странах присутствия (Россия, Украина, Армения, Туркменистан) составила 97,6 млрд руб. – это на 5% выше прошлогоднего результата того же квартала. Операционная прибыль OIBDA тоже увеличилась на 5% (до 41,5 млрд руб.). Правда, чистая прибыль выросла меньше – всего на 1% (до 13,0 млрд руб.), что объясняется изменением курса доллара. Аналогичный 5%-ный рост выручки и OIBDA наблюдался и в российском бизнесе оператора.

А. Дубовсков: «Мы гордимся сокращением на 5% доходов от контент-сервисов, потому что это результат нашей борьбы со спамом и мошенническими рассылками»

Что послужило предпосылками таких результатов? Как рассказал президент Группы МТС Андрей Дубовсков, в минувшем квартале компания запустила новую стратегию «3Д» («данные», «дифференциация», «дивиденды»), предусматривающую развитие мобильного интернета, диверсификацию услуг и увеличение выплат акционерам. МТС начала коммерческую эксплуатацию LTE-сетей в Татарстане, Башкирии, Приморском крае, Свердловской области, Санкт-Петербурге и Ленинградской области. Капитальные затраты на развитие сетей 3G, строительство сетей 4G, перевод сетей МГТС в Москве на технологию GPON и модернизация сетей в регионах достигли 10,1 млрд руб. Кроме того, компания подписала кредитные соглашения с Citibank Europe и Шведской корпорацией по экспортному кредитованию на сумму $300 млн (т.е. оператора не коснулись финансовые санкции на международном рынке кредитования).

В целом показатели работы кажутся скопированными с предыдущего квартала (в котором рост составил те же самые 5%), что, по мнению Василя Лацанича, вице-президента МТС по маркетингу, говорит о глубокой стабильности бизнеса компании.

Аутсорсинг по-взрослому

Похоже, ИТ-аутсорсинг в России наконец выходит из «детского» возраста, обращаясь к крупным инфраструктурным проектам. В банковском секторе впервые реализована в полном объеме модель «ИТ-сервисы и компетенции по требованию». Комплексный ИТ-аутсорсинг позволил «Лето Банку» (дочернему банку ВТБ24) быстро запустить банковские услуги с нуля и за два года открыть более 440 клиентских центров и 1,5 тыс. точек продаж в более чем 430 городах и поселках 59 регионов России. Услугами банка уже воспользовались более 720 тыс. клиентов. Генеральным ИТ-провайдером банка в части инфраструктуры и единым центром ответственности выступает компания «Инфосистемы Джет», заменяя своей службой эксплуатации и развития большую часть ИТ-службы банка, от операторов Service Desk и системных администраторов до менеджеров по логистике и обработке счетов операторов связи. В зоне ответственности аутсорсера также находится безопасность ИТ-инфраструктуры и прикладных систем согласно бизнес-требованиям банка.

Как отметил Владимир Елисеев, гендиректор «Инфосистемы Джет», из тысяч реализованных компанией за более чем

В. Елисеев (в центре): «Были моменты, когда становилось просто страшно»

20 лет проектов лишь единицы можно назвать веховыми не только для компании, но и для рынка в целом. «Проект в «Лето Банке» именно такой – понимание возможностей аутсорсинга он вывел на совершенно новый уровень, – заявил В. Елисеев. – В начале пути проект воспринимался как очень сложный. Риск был просчитанный, но высокий».

Как сообщил Дмитрий Назипов, руководитель департамента ИТ банка ВТБ, по итогам этого проекта в группе ВТБ планируется расширять использование аутсорсинга, доказавшего свою эффективность и гибкость.

Центр, еще центр!

А. Хлуденев: «Центр решений на базе технологий крупного вендора – мощный генератор пилотных проектов»

КРОК открыл Центр решений на базе технологий Dell. В компании действуют уже четыре подобных центра – на базе технологий Hitachi Data Systems, Symantec, HP, EMC. По словам Александра Хлуденева, заместителя гендиректора компании КРОК по перспективным направлениям бизнеса, при создании таких центров интегратор руководствуется намерениями вендоров активно развиваться на российском рынке и стремлением поддерживать эти намерения ресурсами, маркетингом, технологиями. «ИТ-инфраструктура любой организации – это сложный комплекс аппаратных и программных компонентов. Их слаженная работа – важная составляющая успешного бизнеса, – подчеркнул А. Хлуденев. – Но тестирование и пилотные внедрения отнимают ресурсы как у заказчика, так и у интегратора. Перерастет ли «пилот» в полноценный проект – остается только догадываться. А в центре решений на базе технологий вендора заказчики могут изучать новейшие продукты, моделировать инфраструктуру в зависимости от собственных бизнес-задач, и что важно – без излишних затрат на развертывание вычислительных мощностей».

В оптимистическом варианте тестирование в центре решений должно вести к реальному проекту. Как отметил Борис Щербаков, гендиректор Dell в России, в международной практике «конвертация» составляет 25–30%. И хотя в КРОКе такие центры не ведут статистику тестирований, приведших к реальным проектам, косвенно приведенные данные подтверждает и практика интегратора. По словам А. Хлуденева, около 30% пилотных проектов выходят на уровень коммерческих.

Кбайт фактов

Минкомсвязи представило комиссии Правительства РФ по законопроектной деятельности проект федерального закона «Об особенностях реорганизации ФГУП “Почта России”», согласно которому «Почта России» будет преобразована в открытое акционерное общество, на 100% принадлежащее государству.

«Ростелеком» запустил бета-версию сервисно-поисковой платформы «Спутник», ориентированной на социально значимые интернет-сервисы.

«ВымпелКом» сдал в коммерческую эксплуатацию сети 4-го поколения (LTE) в Ставрополе и Ростове-на-Дону.

«МегаФон» запустил сервис «СМС-контроль», с помощью которого абоненты могут оградить себя от нежелательных сообщений. Услуга позволяет самостоятельно отписываться от рекламно-сервисных рассылок, внося отправителей в «черный список».

AltegroSky перевела свою сеть со спутника «Экспресс-АМ3» (140° в.д.) на новый космический аппарат «Экспресс-АМ5» (140° в.д.), принадлежащий **ГПКС**, что позволило на 15% увеличить пропускную способность сети при той же арендуемой полосе на спутнике.

Компания ТТК с начала 2014 г. на 10% увеличила технический охват сети ШПД в Калининградской области, доведя его до 67 тыс. домохозяйств в 910 многоквартирных домах.

Panasonic анонсировал в России взрывозащищенную версию 10,1-дюймового планшета Toughpad FZ-G1, соответствующего директиве ATEX. Устройство с предустановленной ОС Windows 8 Pro предназначено для отраслей, характеризующихся повышенной опасностью, например, нефтегазовой промышленности.

Инерция взамен концепции

Выставка «Связь-Экспокомм–2014» год от года перестает отражать основные тренды телекома и ИТ-индустрии, усиливая инфраструктурную составляющую. Но все еще остается чуть ли не генетической связистской Меккой.

Остается не благодаря усилиям организаторов и патронирующих организаций, а скорее, вопреки – по традиции.

Почему? Потому что нет общей идеи (нынешний девиз «новации и традиции» ею назвать трудно), нет технической и маркетинговой концепции. А еще недавно были. Потому что утеряно умение зазывать в экспозицию ведущих и не самых ведущих операторов связи (справедливости ради – спутниковые поставщики услуг нынешнюю выставку не проигнорировали) и крупных мировых вендоров. Разумеется, вследствие объединительных тенденций на рынке это делать все труднее, ведь операторов и производителей стало заметно меньше, чем десять лет назад.

Потому что не найдены аргументы для того, чтобы на площадях «Экспоцентра» заняли свое место активные представители регулятора – в прошлом году структурно- и событийно-образующим стендом стала развернутая экспозиция Роскомнадзора и проведенная в ходе выставки его коллегия. В этом году такой силы среди экспонентов выставки не нашлось.

Зато из 221 зарубежного участника выставки более половины (около 130 компаний!) пришлось на Китай и Тайвань, что вполне соответствует планам ориентации экономики государства на Восток. Если так дело пойдет и дальше, скоро компании из Юго-Восточной Азии составят успешную конкуренцию отечественным производителям и поставщикам не только на сетях связи и в информационных системах предприятий, но и в последнем оплоте отечественного в сфере ИКТ – на профессиональных выставках.

Концептуальный вакуум экспозиции пыталась восполнить деловая программа выставки, в которой были заметны усилия специализированных СМИ (например, ИКС с круглым столом «Качество на рынке связи. Кому выгодно?» – см. с. 58), интернет-сообщества и Международной академии связи. Именно эти события привлекли на Красную Пресню представителей операторских компаний, регуляторов, общественных и бизнес-организаций, экспертов – пусть и не в день открытия «Связь-Экспокомма», на который то ли по задумке, то ли по недогляду пришлось проведение в пресс-центре «РИА Новости» годовой расширенной коллегии поддерживающего выставку профильного ведомства Минкомсвязи.

Запал у ИКТ-сообщества относительно «главной выставки года» еще остается – и эмоциональный, и профессиональный. А у выставки остается не так много времени, чтобы он не сошел на нет.

Наталия КИЙ

На «Связь-Экспокомм» в рамках тура по Европе

Год назад на Красной Пресне демонстрировался первый выставочный образец комплексного решения RiMatrix S компании **Rittal** для дата-центров, а нынешняя выставка стала этапом демонстрационного тура по Европе модульного контейнерного варианта RiMatrix S Single 6.

Комплексное решение для инженерной инфраструктуры дата-центра состоит из серверных и сетевых 19-дюймовых стоек TS IT, систем бесперебойного электроснабжения, распределения питания, охлаждения и мониторинга. RiMatrix S предлагается в двух вариантах с разным количеством стоек: модель Single 6 содержит шесть серверных стоек с общим энергопотреблением до 60 кВт, стойку для сетевого оборудования, стойку для ИБП и аккумуляторных батарей; в состав модели Single 9 с максимальным энергопотреблением 90 кВт входит восемь серверных стоек и одна стойка для сетевого оборудования (эта модель ориентирована на относительно крупные дата-центры, где есть централизованная система бесперебойного питания). Оба модуля можно сдваивать, получая варианты Double 6 и Double 9. В системе охлаждения не используются межрядные кондиционеры, она располагается под фальшполом, что обеспечивает компактность размещения оборудования и в обычном помещении, и в контейнере.

Стандартные модели RiMatrix S можно адаптировать к потребностям заказчика не только вариациями модулей Single 6 и Single 9, но и установкой резервного ввода электропитания, интеллектуальной системы распределения питания, системы увлажнения (или осушения) воздуха, а также ПО для управления ЦОДом RiZone. Модули Single 6 и Single 9 могут размещаться и в здании заказчика, и в комнате безопасности, и в контейнерах. Использование подобного модульного решения позволяет сократить финансовые и временные затраты на создание дата-центра. Например, готовые модули можно привезти в Россию со склада в Германии, собрать и сдать «под ключ» заказчику за шесть-восемь недель. Кроме того, отлаженное стандартизированное решение имеет предсказуемые технические характеристики (в том числе PUE и энергопотребление) и обходится дешевле в эксплуатации. За год, прошедший с премьеры RiMatrix S, в Европе уже появились семь инсталляций этого решения, а в России переговоры с потенциальными заказчиками пока только идут.

Е. ВОЛЫНКИНА

Даешь российское?

В наши дни, когда все чаще говорится не только о большом походе на Восток и встречном движении оттуда, но и об импортозамещении, важно понимать, на что способны российские производители. Скажем, в области оптического волокна и кабельных систем.

По данным ВНИИ кабельной промышленности, за 13 лет текущего века производство волоконно-оптического кабеля в мире выросло втрое. Медные кабели связи наружной установки демонстрируют четырехкратную отрицательную динамику. LAN-кабели внутренней установки пока не вытесняются оптическим волокном и потребляются с небольшим ростом. Цифры, приведенные главой ВНИИКП Геннадием Мещановым на конференции Международной академии связи во время «Связь-Экспокомма», кажутся вполне логичными, жизнеутверждающими и соответствующими тенденциям развития телеком- и ИТ-рынков.

Если углубиться в подробности, ситуация меняется. Суммарное количество ВОК, использованного в Северной Америке в 2008–2013 гг., – 193 млн км, в странах СНГ – 33 млн км. «Инфраструктура связи у нас явно отстает! – делает вывод Г. Мещанов и добавляет: – Производство медного кабеля в России начало падать с 2004 г. и с тех пор сократилось в семь раз. Производство LAN-кабеля в России растет, но удовлетворяет не более 20% нашего рынка».

И это еще не все. С 2011 г., вопреки мировым тенденциям, в России и СНГ начало падать производство ВОК. «Надо бить тревогу! – говорит Г. Мещанов. – За два года мы потеряли 30% объема производства: в 2012 г. падение составило 16,9%, в 2013 г. – 17,9%». И это притом, что в России действуют 16 современных производств ВОК, среди них «Инкаб», «Еврокабель-1», «Москабель–Фуджикура» и др. Часть из них были представлены на выставке в «Экспоцентре». По оценке ВНИИКП, «заводы находятся в очень неприятной ситуации». Одна из причин – импорт, составляющий 12 – 13% объема рынка. По мнению Г. Мещанова и судя по экспозиции «Связь-Экспокомма–2014», началось проникновение на рынок китайских кабелей, оно растет, что является причиной законного беспокойства наших производителей.

Н. КИЙ

Компания **«Т8»**, производитель телекоммуникационного оборудования спектрального уплотнения для оптических систем связи в России и СНГ, участвовала в выставке в статусе отечественного производителя, по традиции приурочив к мероприятию сразу два рекорда, отражающих состоятельность российской инженерной мысли.

Во-первых, демонстрировался работающий прототип единственной российской DWDM-системы, разработанный при участии фонда «Сколково». Инвестор выделил «Т8» грант на создание оборудования спектрального уплотнения с максимальной емкостью 25 Тбит/с. Однако инженеры-разработчики сумели найти техническое решение, обеспечившее более высокую пропускную способность системы – 27 Тбит/с. Расстояние между 100G-каналами в прототипе системы составляет 33 Гц, для облегчения управляемости каждые десять каналов объединены в суперканалы. Второй рекорд – передача сигнала 100G на 500 км без регенерационных пунктов и усилителей с электрическим питанием – был поставлен компанией «Т8» на ее уже известной рынку DWDM-системе «Волга», к слову, внесенной в реестр инновационной продукции, рекомендованной федеральными законами о госзакупках и закупках отдельными видами юрлиц.

Потеснить зарубежных производителей на рынке ИТ- и телекоммуникаций в России намерена группа компаний IEK – известный российский производитель электротехнических изделий для строительства, ЖКХ и промышленных предприятий. На прошлогодней выставке она анонсировала новую торговую марку – ITK – и представила первые относящиеся к ней модели оборудования для телекомрынка. В этом году на стенде **ITK** демонстрировались 19-дюймовые телекоммуникационные шкафы и стойки, LAN-кабель и инструменты, компоненты структурированных кабельных систем (СКС), электропитание 19-дюймовых стоек, кабеленесущие системы отечественного производства. Вся продукция прошла контроль качества, соответствует международным и российским стандартам, а потому имеет расширенную гарантию до 10 лет.

Гвоздем экспозиции ITK был новый Активный телекоммуникационный шкаф (АТШ), разработанный в соответствии с техническими требованиями МГТС в предельно короткие сроки: с получения ТЗ до представления опытного образца потребовалось 10 дней. В верхнем отсеке АТШ расположены вентиляторы, электропитание, элементы для подключения волоконно-оптического кабеля к активному телекоммуникационному оборудованию, а также для разводки телефонии. Нижний отсек отводится под батарейные блоки. Согласно техническому заданию оператора, АТШ имеет антивандальное исполнение, в нем используется как принудительное, так и естественное охлаждение.

Еще один российский производитель и поставщик оборудования, компания

TeleCore , представил мобильный центр обработки данных TeleCore DataBox-F на пять стоек с ИТ-оборудованием общей мощностью 50 кВ со всеми необходимыми инженерными системами. Производятся МЦОДы в Томске, по желанию заказчика укомплектовываются ИБП и кондиционерами, тестируются в его присутствии, затем пакуются и доставляются на объект. Для развертывания одного контейнера требуется три дня. Пока таких контейнерных ЦОДов выпущено 40, самый мощный рассчитан на 100 кВ. Заказчиками продукции выступают нефтегазовые компании, банки, учебные заведения, промышленные предприятия, в том числе и режимные.

Максимальная мощность одного модуля – 120 кВ, а дальнейшее наращивание возможно путем добавления контейнеров. При этом стыковка на объекте не требуется, а объединение происходит под общей системой управления.

А. КРЫЛОВА

Спутники в приоритете

Телекомы ушли с выставки – и пожалуй, впервые в истории «Связь-Экспокомма» в операторском блоке участников доминировали владельцы спутников – ГПКС, ГКС, «Интерспутник», Intelsat. Жемчужиной деловой программы стал семинар ГПКС, посвященный услугам на базе технологии VSAT в Ka- и Ku-диапазонах. Похоже, организаторы не предполагали, что «информационный дефицит» на площадке «Связь-Экспокомма» выльется в физическую нехватку воздуха: конференц-зал ломился от желающих послушать спикеров, люди плотной стеной стояли в проходах. Специалистов в области спутниковой связи на выставке оказалось, пожалуй, не меньше, чем на CSTB или даже SatComRus.

Ka-диапазон углубляется

Проект предоставления спутникового ШПД в Ka-диапазоне, начатый ГПКС в 2012 г. на спутнике Ka-Sat, захватывает лишь небольшую часть центра и северо-запада России. Как сообщил Михаил Глинка (ГПКС), сначала 70-75% клиентов были сосредоточены в «московском» луче (самом большом с точки зрения абонентской базы), а в последнее время активный прирост наблюдается в «воронежском» и «питерском» лучах. Количество пользователей приблизилось к 4,5 тыс. домохозяйств; растет объем трафика на пользовательский терминал, общий объем за апрель 2014 г. составил 32 Тбайт. По словам Игоря Чурсина (Россвязь), с развитием этого проекта в России начал формироваться новый сегмент рынка – частные пользователи спутникового ШПД. А ввод в эксплуатацию отечественной системы спутникового высокоскоростного широкополосного доступа на базе российских космических аппаратов «Экспресс-АМ5» и «Экспресс-АМ6» даст новый импульс развитию услуги.

«Экспресс-АМ5» (140° в.д.) уже введен в коммерческую эксплуатацию, запуск «Экспресс-АМ6» в точку 53° в.д. намечен на июль этого года. Зона покрытия обоих охватывает густонаселенные пункты всей территории России и, что немаловажно, Дальний Восток, особенно Сахалин и Камчатку. По словам Евгения Буйдинова (ГПКС), сейчас завершается строительство соответствующей наземной инфраструктуры Ka-диапазона стоимостью около 1 млрд руб. (станции в ЦКС «Медвежьи Озера», ЦКС «Дубна» и в Хабаровске, сеть IP-MPLS с оборудованием уплотнения DWDM). В качестве хабов выбрано оборудование Jupiter компании Hughes. «Это было непростое решение, мы около полугода выбирали оборудование, которое удовлетворяло бы и по ценовым параметрам, и по надежности и качеству, – пояснил Е. Буйдинов. – Сеть компании Hughes, которая одновременно является производителем оборудования и оператором, имеет самую большую абонентскую базу в Ka-диапазоне. Поэтому мы решили: когда в сети порядка 500 тыс. абонентов, все нюансы оборудования и ПО должны быть отработаны».

Килобайт экспонентов

МОКС «Интерспутник» представила возможности запущенного 7 февраля 2014 г. в точку 75° в.д. спутника ABS-2, часть емкости которого организация арендует на долгосрочной основе у оператора Asia Broadcast Satellite. Если сегодня для охвата всей территории России ТВ-вещанием требуется два-три спутника, то ABS-2 справится с этой

задачей в одиночку, уверен Тимофей Абрамов, коммерческий директор МОКС «Интерспутник». В настоящее время уже началась подготовка к созданию аппарата ABS-2A, который дополнит ABS-2 в орбитальной позиции 75° в.д.

* * *

На стенде компании **Entel** можно было увидеть серию модульных ИБП IPS мощностью 10–640 кВА. Их КПД в онлайновом режиме – 96%, а при работе от аккумуляторных батарей – 98%, входной коэффициент мощности – более 0,99. Они могут комплектоваться силовыми модулями мощностью 10, 20, 25 и 40 кВА, которые устанавливаются в стандартные стойки вместе с модулями мониторинга и управления. Замена модулей может осуществляться в горячем режиме, что позволяет построить систему необходимой мощности с нужным уровнем резервирования и возможностью масштабирования.

Килобайт экспонентов

В разделе беспроводных решений компания **ZyXEL** демонстрировала фемтосоты для улучшения качества 3G- и 4G-покрытия. Так, 3G-фемтосота FMT3211 не требует настройки при подключении к мобильному оператору и обеспечивает хэндовер с его базовыми станциями, поддерживает GSM-звонки и 3G-передачу данных. Модель FMT3251 имеет интегрированную точку доступа 802.11ac. Мини-БС LMT3313 поддерживает Voice over LTE, хэндовер с другими фемтосотами, режим открытого подключения всех абонентских устройств и фильтрацию их отдельных видов, а также возможность питания PoE+.

* * *

Ciena приурочила к выставке открытие совместно «АДВ Консалтинг» московского центра обучения для поставщиков услуг, операторов связи и корпоративных клиентов. В ходе обучения они получат знания и навыки, необходимые для развертывания конвергентных пакетно-оптических продуктов и решений управления сетью компании Ciena. Инженеры, проходящие обучение, смогут воспользоваться лабораторией с демонстрационным оборудованием.

Операторы готовятся к броску

Предполагается, что абонентское оборудование операторы наземных сетей спутниковой связи Ка-диапазона будут покупать у производителя сами. За основу взята модель, отработанная в «евтелсатовском» проекте: услуги предоставляют четыре дистрибьютора, каждый из которых арендует на три года около 20% емкости в каждом луче на одном из аппаратов. При этом оператор должен иметь сданную сеть, узел доступа, решить вопросы СОРМа и иметь возможность присоединиться к одному из узлов ГПКС в Москве или Хабаровске для работы на соответствующем кабеле. Цена «входного билета» будет сравнима с существующими расценками в «евтелсатовском» проекте: $1 тыс. за 1 Мбит/с пропускной способности.

Е. Буйдинов: «Мы собираемся строить самую большую сеть для российских операторов»

Точные расценки ГПКС обещает назвать после испытаний, которые планирует провести летом совместно с компаниями «Истар» и AltegroSky. Для этого разработано решение, обеспечивающее предоставление услуг высокоскоростного ШПД любой категории пользователей: крупным корпоративным заказчикам, небольшим компаниям, частным лицам. Сергей Пехтерев, глава AltegroSky, предполагает, что система в целом может в периоды максимальной загрузки обслуживать 150 тыс. абонентов на Дальнем Востоке. При этом AltegroSky намерена экстраполировать безлимитный тариф «евтелсатовского» проекта на проект ГПКС. «Надеемся, что в первые года три поработаем на Дальнем Востоке в таком же режиме, а дальше, если вся емкость «Экспресс-АМ5» будет использоваться, придется регулировать тарифы, это обычная коммерческая практика, – заметил С.Пехтерев. – Но на первых этапах абонентам сильно повезет».

По словам Павла Баканова («Истар»), в сфере B2B для операторов мобильной и фиксированной связи предлагаются выделенные каналы, для операторов мобильной связи – двухдиапазонные решения (Ка- и Ku-диапазоны) с автоматической балансировкой трафика, для вещательных медийных компаний – сети сбора новостей. Кроме того, компактные терминалы Ка-диапазона дадут толчок развитию спутниковой связи для оперативных служб – медицины катастроф, МЧС, силовых структур.

Ввести систему в тестовую эксплуатацию ГПКС планирует в октябре – ноябре, в коммерческую – в декабре. Впрочем, в связи с неудачным запуском 16 мая «Экспресс-АМ4R» эти планы могут измениться. Утерянный спутник предполагалось вывести в точку 80° в.д. и использовать для предоставления услуг телерадиовещания, ШПД, мультимедиа, телефонии и создания сетей связи на основе VSAT, а также для решения задач подвижной президентской и правительственной связи. Но теперь для обеспечения телерадиовещания

на территории РФ связной ресурс спутников может быть перераспределен и, соответственно, изменится плановая точка стояния «Экспресс-АМ6». Тем не менее вряд ли ГПКС откажется от выношенных планов относительно Ка-диапазона.

Лилия ПАВЛОВА

Веб-сайты – на мобильную платформу

Наряду с рынками мобильной, контекстной, видеорекламы, поисковой оптимизации и цифровых коммуникаций, веб-разработка рассматривается в составе одного из четырех сегментов экономики Рунета – маркетинга и рекламы. Его тренды, проблематика и перспективы живо обсуждались на круглом столе РАЭК в рамках выставки «Связь-Экспокомм–2014».

А. Терехов: «В 2014 г. на рынке веб-разработок должны наконец появиться консалтинговые компании»

Несмотря на долгую историю развития, рынок веб-разработки имеет мелкодисперсный характер, констатировал Андрей Терехов (Inforza). Это объясняется прежде всего низким порогом входа для новых игроков. Сегодня на рынке работают около 10 тыс. компаний, многие из которых не могут похвастаться высоким уровнем квалификации, а уж тем более – клиентского сервиса и техподдержки.

Тенденции на рынке несколько противоречивы. С одной стороны, это усиление конкуренции его участников с игроками смежных рынков – сетевыми рекламными агентствами, крупными системными интеграторами и компаниями, работающими в сегменте поисковой оптимизации, замедлившем свое развитие. С другой – нарастание дифференциации и углубление специализации самих веб-студий. Узкая направленность сегодня является конкурентным преимуществом. Обострение конкуренции вынуждает серьезных игроков заботиться о повышении эффективности бизнеса, переносить фокус с абстрактного креатива на построение бизнес-процессов, делать ставку на автоматизацию и детальные расчеты эффективности любых акций.

Технологическим трендом, который еще в течение двух-трех лет продолжит влиять на развитие рынка веб-разработки, является распространение и рост популярности SaaS-решений у заказчиков из числа SMB-компаний. Результатом станет сокращение количества небольших студий, обслуживающих таких клиентов, и переход этого бизнеса в руки крупных игроков, имеющих в своих портфелях продукт, готовый к предоставлению в облаке. Другой, не менее значимый технологический тренд – мобильность и кросс-платформенность.

Впрочем, быстрый рост аудитории мобильного интернета (по данным TNS от апреля 2014 г., этим каналом доступа в сеть пользовались 2,7 млн россиян) пока не убедил владельцев сайтов в необходимости сделать свои веб-ресурсы удобными для пользователей смартфонов. Сегодня больше половины (67%) не планируют адаптировать сайты к мобильным устройствам, отметил Егор Аристакесян (Articulmedia). Причин тому несколько: клиент может считать, что он и так достаточно представлен в «большом» вебе или что специфика его сайта этого не требует. Кроме того, трафик с мобильных устройств на ресурс может показаться незначительным. Однако «мобилизация» сайта имеет два преимущества: возможность прирастить аудиторию за счет пользователей мобильных устройств и

Килобайт экспонентов

Agilent Technologies представила контрольно-измерительные приборы для телекоммуникаций, аэрокосмической и оборонной промышленности, предприятий микроэлектроники и нанотехнологий. Это высокопроизводительные анализаторы сигналов реального времени PXA, решения для формирования и анализа сигналов ГЛОНАСС/GPS, LTE/LTE-Advanced, анализаторы цепей высшего класса

серии PNA-X до 67 ГГц, а также 18 новых моделей портативных ВЧ/СВЧ-анализаторов, широкий спектр осциллографов, генераторы ВЧ/СВЧ-сигналов и пр.

* * *

На стенде **Alcatel-Lucent** можно было познакомиться с оборудованием и приложениями, разработанными в рамках стратегии перехода в облако с целью построения облачной среды с высокой производительностью, надежностью и повышенной масштабируемостью на базе открытых виртуализованных сетей операторского и корпоративного класса. На выставке демонстрировалась SDN-платформа Nuage Virtualized Service Platform, отвечающая за обеспечение бесшовных соединений внутри дата-центра, между несколькими ЦОДами, а также между ЦОДами и VPN-сетями. Ее дополняли высокопроизводительные шлюзы для интеграции физического оборудования ЦОДов в SDN-платформу и новые сервисные маршрутизаторы для эффективного соединения ЦОДов и предоставления услуг корпоративным заказчикам.

Килобайт экспонентов

Этапом европейского турне стал «Связь-Экспокомм» для компании **Huber+Suhner,** в фирменном фургоне которой демонстрировались оптоволоконные решения для подключения высокоплотных коммутаторов в дата-центрах. Оптический кроссовый шкаф LISA высотой 2 м и глубиной 30 см позволяет разместить в кассетах до 3000 оптических портов с пропускной способностью 1, 10, 40 и 100 Гбит/с. Эти решения ориентированы на ЦОДы, где необходимо

одновременно обеспечить сорока- и стогигабитные соединения и минимизировать место, занимаемое сетевым оборудованием и кабельной разводкой.

* * *

Компания **TE Connectivity** представила программно-аппаратный комплекс Quareo, обеспечивающий функционирование СКС в дата-центре. Quareo позволяет автоматизировать процедуры администрирования сети и в реальном времени получать информацию о состоянии всех компонентов СКС ЦОДа. Система поддерживает использование QR-меток для сетевого оборудования и доступ к базе данных ПО ICM с мобильных устройств.

быстродействие работы на сайте с мобильного устройства, его «заточенность» под импульсивные действия пользователя.

При этом у клиента есть выбор, по какому пути – разработки мобильной версии сайта или мобильных приложений – пойти. Последний путь затратнее, поскольку для максимального охвата аудитории приложений потребуется разработать как минимум два – для iOS и для Android. Перед принятием решения о создании мобильного приложения, советует Александр Богданов (AGIMA), хорошо бы спросить себя и коллег, будут ли люди им пользоваться, и если ответ утвердительный, его стоит делать.

Для крупного агентства, работающего с разными каналами цифровых коммуникаций, в мобильной среде денег не так много, замечает Евгений Этин (Promo Interactive). Вот почему возглавляемая им компания не упускает из вида два других канала: Smart TV и second screen. «Платформа Smart TV органично объединяет в себе несколько устройств, по сути, закрывая потребность аудитории в получении медиаконтента», – отметил он. По его данным, Россия входит в тройку рынков сбыта «умных телевизоров», пропуская вперед Китай и Бразилию. В 2014 г. в нашей стране будет продано 2 млн таких устройств. Что же касается «второго экрана» (second screen), то эта категория сервисов, предполагающая использовать во время просмотра видеоконтента сразу несколько устройств, очень популярна за рубежом и ждет реализации в России. По крайней мере, около 30% участников опроса, из которых 40% обычно не смотрят телевизор, признались, что переходят с одного устройства на другое во время просмотра одного и того же видео.

Таким образом, рынок веб-разработки делает ставку на существующие технологии, но живет в ожидании прорыва, способного вызвать революционные изменения в медиапотреблении.

Александра КРЫЛОВА

Будущее уже здесь

Законотворчество в области контроля российского сегмента интернета идет семимильными шагами. Вот только в какую сторону?

Три года назад выставка «Связь-Экспокомм» стала площадкой для российского форума по управлению интернетом (RIGF). Одно из его заседаний было посвящено обсуждению трех намеренно утрированных сценариев развития глобальной сети в течение ближайших 10-15 лет – «Правление пользователей», «Интернет-острова» и «Глобальное правительство интернета». Первый предполагал рост социальных сетей, изменение способов общения между людьми, загрузку в сеть огромных объемов контента, в том числе и своих персональных

данных, клевету на других пользователей и массовые нарушения законов об авторском праве. Два последних предусматривали усиление роли государства в сети: прогнозировалось, что к 2020 г. борьба последнего за широко понимаемую безопасность «своих» пользователей приведет к массовому огораживанию национальных сегментов сети с образованием «интернет-островов», а «глобальное правительство интернета» к тому же сроку введет фильтрацию контента на национальном уровне, обязательную аутентификацию интернет-пользователей и даже их лицензирование для разрешения выхода в сеть. Тогда эти сценарии казались преувеличением, хотя, по результатам импровизированного опроса, больше 70% собравшихся согласились, что развитие интернета будет идти именно в «государственном» направлении.

Но мало кто мог подумать с какой скоростью, опережая все прогнозы, Россия устремится к этому будущему. Уже год спустя был принят закон №139-ФЗ от 28.07.2012 «О внесении изменений в ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети интернет», предусматривающий создание так называемых черных списков интернет-ресурсов и внесудебное закрытие сайтов (содержащих порнографию с участием несовершеннолетних, инструкции по способам самоубийства, изготовлению и приобретению наркотиков), неоднозначные формулировки которого вызвали протесты правозащитников и интернет-сообщества. Как отметила Ирина Левова (РАЭК), во время обсуждения проекта этого закона его разработчики говорили, что перечень категорий черных списков останется неизменным и не будет расширяться.

Но уже в 2013 г. последовал закон «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"» (№398-ФЗ от 28.12.2013), разрешивший досудебную блокировку сайтов за экстремизм и сепаратизм с весьма широкими трактовками последних. Затем настал черед ограничений на использование платежных интернет-систем, приравнивания блогеров к СМИ (№ 97-ФЗ от 05.05.2014 «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей»), законопроектов о регулировании облачных сервисов и переносе корпоративных серверов на территорию России и т.п. Так что в рамках нынешнего «Связь-Экспокомма» на круглом столе «Инициативы по изменению инфраструктуры российского сегмента сети интернет: КНР или КНДР?», организованном РАЭК, состоялось обсуждение результатов этого бурного запретительного законотворчества.

Стоит отметить, что, каким бы ни был характер законодательства, все его положения должны приниматься с учетом мнения экспертов

Килобайт экспонентов

На стенде **Enersys** демонстрировались контейнеры и термошкафы компании Purcell с интеллектуальной системой зонального охлаждения. Они экономят 55–90% электроэнергии, потребляемой активным оборудованием, создают оптимальный режим для эксплуатации аккумуляторных батарей (основной продукции Enersys). Все изделия Purcell собираются из готовых модульных блоков, легко

переконфигурируются, мало требовательны к обслуживанию. Управлять температурой в их зонах охлаждения можно дистанционно.

* * *

Концерн **Pentair** представил платформу Schroff для ЦОДов, использующую различные комбинации модульных компонентов и масштабируемых стандартных изделий (шкафы для серверов и сетевого оборудования Varistar; панели для управления потоками воздуха; системы охлаждения, распределения и регулировки мощности). Ассортимент изделий дополнен новой серией воздушно-водяных теплообменников. Внутрирядный теплообменник Schroff Varistar SHX30 разработан специально для охлаждения шкафов с высокой тепловой нагрузкой в системе изоляции коридоров.

Килобайт экспонентов

Заметное место на стенде **«Вимкома»** занимало VoIP-оборудование китайской компании Fanvil: видеотелефон D900 с 7-дюймовым TFT-экраном. Он работает под управлением Android 4.2, поддерживает четыре линии SIP и передает видео- и аудио- в формате HD. Другое интересное устройство – IP-домофон с полноценным SIP-клиентом, карточками для открытия двери, программируемыми через веб-интерфейс, питанием PoE, поддержкой набора номера и открывания двери по входящему DTMF.

* * *

Компания **ABB** привезла на выставку беспроводные широкополосные системы связи mesh-топологии для построения интеллектуальных энергосистем Smart grid, сетевой инфраструктуры для «умных городов», нефтегазовых и горнодобывающих компаний, складских комплексов и т.д., где требуются хорошо масштабируемые и отказоустойчивые решения. Эти сети строятся на базе mesh-маршрутизаторов семейства ABB Tropos, работающих в одном (2,4 ГГц) или двух (2,4 и 5,8 ГГц) частотных диапазонах по стандартам 802.11 a/b/g/n и предназначенных для установки на улице, в помещениях и на транспортных средствах (диапазон рабочих температур – от -40°C до +55°C, и даже до +75°C).

соответствующей отрасли, профильных министерств и ведомств, в том числе Минкомсвязи. В данном случае ключевые замечания и поправки, предлагавшиеся экспертами, были проигнорированы. Результат известен: был выбран самый простой способ блокировки интернет-ресурсов – по IP-адресам, что привело к наказанию ни в чем не повинных сайтов, оказавшихся на одном IP-адресе с нарушителями. Георгий Грицай (Минкомсвязь) высказал озабоченность той легкостью, с какой представители законодательной власти пользуются инструментами блокирования интернет-ресурсов. «Тяжелый, не очень естественный для интернет-бизнеса механизм ограничения доступа вызывает немало вопросов и с технической, и с организационной, и с экономической точек зрения», – добавил он.

Чей пример вдохновляет наших ревнителей чистоты сети? Северной Кореи, где доступ в полноценный интернет имеют лишь Ким Чен Ын и его ближайшее окружение? Или Китая с его «великим китайским файерволом»? Возможно. Но, как заметил Павел Храмцов (RU-Center), технические возможности блокировки нежелательного контента, реализованные в Китае, Рунету и не снились. Если у нас в качестве большого достижения преподносится система DPI, позволяющая блокировать контент не по IP-адресу, а по URL, то там контролируется поведение в сети более чем полумиллиарда человек, идет фильтровка по черным спискам сайтов, по ключевым словам, по информации о предыдущем поведении пользователя в сети. На это у нас банально нет ресурсов. Есть еще Иран, где заблокирована фактически треть всего интернета – тоже очень затратный проект. К тому же при его реализации можно забыть о тех 8,5% ВВП, которые, согласно исследованию РАЭК, сейчас приносят стране интернет-зависимые отрасли экономики (притом, что в них занято около 1,7% трудоспособного населения).

Однако, зная «продуманность» и «реализуемость» наших законов и учитывая непрекращающиеся усилия активной части интернет-сообщества наладить контакты с государством, а также принимая в расчет многочисленных умельцев, способных обходить любые «заборы», можно предположить, что нас ожидают еще несколько лет относительно свободного интернета. Есть и некоторая надежда на Конституционный суд, который может дать правовую оценку уже вступившим в силу законам. Совет при президенте РФ по развитию гражданского общества и правам человека свое мнение по поводу «закона о блогерах» уже высказал: «Данное ужесточение государственного контроля, фактически серьезнейшим образом ограничивает конституционную свободу искать, получать, передавать и распространять информацию. При этом неясно, для защиты каких конституционно значимых ценностей вводятся подобные ограничения. В то же время, нормы закона безмерно расширяют поле для произвольных действий должностных лиц государственных органов в отношении граждан и юридических лиц, чьим правам и законным интересам может быть нанесен серьезный ущерб».

Евгения ВОЛЫНКИНА

О степенях свободы

За неуклюжими попытками власти определить правила игры профессионалы медиарынка видят наступление на свободу слова, стремление контролировать информационные потоки в виртуальном пространстве и останавливать те, содержание которых государство не устраивает.

На апрельском форуме РИФ+КИБ–2014 было отмечено, что ограничениями, подобными содержащимся в так называемом антиблогерском законе, несудебными блокировками сайтов насадить в Рунете единообразие мыслей вряд ли удастся. «Интернет – это информационное пространство, работающее с электрической скоростью, скоростью мысли, – заявил, выступая на секции «СМИ: Территория выживания», Иван Засурский («Частный корреспондент», журфак МГУ). – Я не вижу, каким образом подобными действиями государство может что-то изменить, скорее, оно вызовет обратную реакцию – объединит против себя огромное количество людей с самыми разными интересами». По его мнению, лучший способ эффективной работы с такой открытой средой, как интернет, – повышение ответственности пользователей: надо давать им доступ к знаниям, увлекать их познавательными вопросами. «Антиблогерский» закон станут применять точечно. «Разбираться будут с теми, кого считают конкурентами в политической сфере», – заявил Алексей Венедиктов («Эхо Москвы»). Другое дело, что при определенных условиях такой точкой может стать каждый. И это заставляет владельцев ряда крупных веб-ресурсов подумывать о переходе в зону .com.

При этом людей, выступающих с теми или иными законодательными инициативами по закручиванию гаек в интернете, можно условно поделить на две группы. К первой относятся те депутаты и чиновники, кто в силу возраста не понимают специфики новой коммуникационной среды, в которой обитают миллионы человек. Ко второй – отдельные представители самой интернет-индустрии, заинтересованные в установлении тех или иных ограничений, выгодных их бизнесу. Представителям первой группы можно пытаться разъяснять мнение профессионального сообщества. Самые действенные аргументы для этого – доля экосистемы интернет-зависимых рынков в ВВП (по итогам 2013 г. прогнозировалась на уровне 8,5%, или 5,2 трлн руб.), а также конкурентоспособность российской интернет-индустрии.

С надеждой на читателей и пользователей

Если бы пользователи законопослушных веб-ресурсов, ставших недоступными вследствие блокировки другого сайта по IP-адресу, обращались с заявлениями о нарушении своих прав в суды, то, возможно, это заставило бы депутатов внести корректировки в закон. Такими «лоббистами» вполне могли бы стать люди, подписавшиеся на те или иные новости и аналитику и регулярно перечисляющие за это деньги. Правда, веб-ресурсов, предлагающих такие платные сервисы в Рунете, пока немного. Один из них, телеканал «Дождь», по словам его основательницы Натальи Синдеевой, делает ставку на пользователей Smart TV и стремится нарастить базу своих подписчиков (формирование которой началось еще в сентябре 2013 г.) до 300 тыс.

«Если люди заплатили нам за контент, значит, они в нас верят, – соглашается Елизавета Осетинская (РБК). – Читатель, понимающий, что бесплатной может быть только пропаганда, намного надежней рекламодателя». Для того чтобы показать, что в Рунете сложилась профессиональная среда, в которой люди активно занимаются раскрытием всевозможных фактов и выявлением связи между ними, РАЭК, «Эхо Москвы» и Notamedia учредили медиапремию Internet Media Awards, которая будет носить имя Эдварда Сноудена.

О чем заботится государство?

Вместе с тем именно благодаря бывшему сотруднику ANB мир задумался о необходимости в процессе свободного обмена информацией в интернете обеспечить безопасность на всех уровнях: межгосударственном, национальном, для бизнеса, граждан.

Как, не ущемляя прав граждан на свободный доступ к информации, защитить те миллионы неопытных пользователей, которые влились в аудиторию Рунета? На этот вопрос пытается ответить государство, правда, пока преимущественно путем ограничений. Свою задачу по обеспечению безопасности интернет-пользователей государство в лице Роскомнадзора видит в наращивании средств контроля за соблюдением соответствия обработки персональных данных действующему закону №152-ФЗ.

«Либеральные» методы защиты, которые используют госорганы, уже не являются эффективным средством против посягательств на частную жизнь», – отметила Антонина Приезжева (Роскомнадзор) на конференции АДЭ «Этические, культурологические и цивилизационные проблемы работы в сети Интернет». По ее словам, в ГД уже внесены законопроекты, которые допускают проведение неплановых проверок по обращениям граждан о нарушении их прав как субъектов персональных данных, а также возбуждение дел об административных правонарушениях. Санкции за такие нарушения увеличатся кратно. Кому-то эти меры покажутся слишком жесткими, но без них гарантировать сохранность персональных данных в условиях, когда личная информация является товаром, не представляется возможным.

Контроль государства за соблюдением сохранности персональных данных – условие обязательное, но недостаточное. Оно должно инициировать формирование культуры информационной безопасности, создать условия, в которых бизнес- и рядовые пользователи интернета должны знать о факторах, угрожающих ИБ, и возможных превентивных действиях. Нужно переносить в интернет общепринятые этические понятия и нормы и следить за соблюдением технических стандартов при использовании информационно-телекоммуникационных технологий.

Александра КРЫЛОВА

Гегемоны ЦОДостроения

Доля российских дата-центров в мировой базе этих объектов пока невелика, но многие тренды глобальной отрасли ЦОДов в России прослеживаются четко.

НАШИ 2% В МИРЕ ДАТА-ЦЕНТРОВ. На 2-й международной конференции Data Center Design & Engineering (DCDE), организованной журналом «ИКС», состоялась премьера предварительных результатов очередного опроса профессионалов отрасли дата-центров, который каждый год проводит Uptime Institute. Обычно данные оглашаются месяцем позже на традиционном симпозиуме организации, но, надеемся, что это исключение станет теперь правилом. Цель ежегодного опроса Uptime – понять финансовую ситуацию в отрасли, выявить технологические тенденции, драйверы и сдерживающие факторы развития индустрии. В текущем году в опросе приняли участие порядка 1500 операторов дата-центров, владельцев корпоративных ЦОДов и их сотрудников. Доли корпоративных и коммерческих ЦОДов оказались одинаковыми – по 50%. Как и следовало ожидать, большая часть дата-центров-участников (48%) представляла США и Канаду. 21% охваченных опросом ЦОДов располагается в Европе, 14% – в Азиатско-Тихоокеанском регионе,

10% – в Латинской Америке, 5% – в Африке и на Ближнем Востоке. Россию и СНГ представляли 2% участников опроса.

Пока, как видим, наша доля довольно скромная, но ведь и дата-центров у нас в стране совсем немного – по данным iKS-Consulting, крупных и средних коммерческих ЦОДов в России порядка 170. Корпоративные дата-центры подсчитать труднее в силу общей политики закрытости, но вряд ли их добавление изменит порядок величины, тем более что большинство корпоративных объектов относятся, скорее, к категории серверных комнат, чем ЦОДов. Тем не менее российские дата-центры имеют все возможности широкой вовлеченности в опросы мировой ЦОДоиндустрии, ведь в Москве уже более года работает Uptime Institute Russia. Так что надеемся, что в следующем году наше участие выйдет за пределы статистической погрешности. Ожидаем также, что российские ЦОДы станут более активно участвовать и в проводимом Uptime Institute конкурсе Brill Awards for Efficient IT на самый эффективный с точки зрения работы ИТ-систем дата-центр. Во всяком случае «наши» люди в составе соответствующего жюри уже есть.

ДЕНЬГИ И МОЩНОСТИ. Итак, какова общая ситуация «по больнице» и как ее можно проецировать на наши реалии? Сначала о деньгах: как оказалось, бюджеты 63% дата-центров за последний год выросли, в 24% ЦОДов они остались на прежнем уровне, а в 13% – снизились. Но это сильно усредненный показатель, потому что в 90% коммерческих дата-центров бюджеты увеличились, т.е. сокращения касаются главным образом корпоративных ЦОДов. Российская ситуация, скорее всего, соответствует мировой: регулярно появляются сообщения о запуске новых коммерческих дата-центров (в том числе очень крупных) или расширении мощностей имеющихся, а вот с корпоративными ЦОДами дело обстоит несколько иначе – проект мегаЦОДа Сбербанка уже отошел в историю, а из недавних событий можно вспомнить резкое сворачивание весьма амбициозной программы строительства ЦОДов «Ростелекомом».

В чем российская ситуация заметно отличается от общемировой, так это в мощности ЦОДов. В мире мощность более 1 МВт имеют 55% дата-центров, а у нас к таковым до сих пор относятся считанные проекты. Но курс на построение мегаваттных ЦОДов взяли все крупные игроки этого рынка. Например, компания DataPro уже запустила в Твери дата-центр с подведенной мощностью 4,5 МВт и строит в Москве новый ЦОД с проектной мощностью более 20 МВт.

КАКИМ ДОЛЖЕН БЫТЬ PUE? Предмет первостепенной заботы подавляющего большинства ЦОДов – энергопотребление и энергоэффективность. Энергопотреблением озабочены 83% руководителей компаний и 58% ИТ-директоров (здесь более низкий процент понятен: далеко не везде ИТ-департамент отвечает за затраты на электричество).

На 80% объектов в борьбе за повышение энергоэффективности разграничивают холодные и горячие коридоры, 63% – пытаются поднять температуру воздуха на входе в серверы, 36% – оптимизируют воздушные потоки в серверных залах, 20% – используют системы адиабатического охлаждения. Все эти технологии применяются и в наших дата-центрах, и чем ЦОД новее, тем шире они там представлены.

Отражением проблемы энергопотребления дата-центра является и внимание к коэффициенту энергоэффективности (PUE). Его измеряют в 73% всех ЦОДов, а среди коммерческих доля таковых еще выше – 98%, ведь от этого показателя напрямую зависят их издержки.

Интересными оказались ответы на вопрос «каким должен быть PUE дата-центра?». 49% ответов варьировались в диапазоне 1,2–1,5 (новые российские дата-центры заявляют в качестве целевых значений PUE такие же величины), 13% считают что PUE должен быть еще ниже – 1,0–1,2, 32% приемлемым назвали PUE, равный 1,5–2,0, 3% согласны на 2–2,5. А 3% специалистов дата-центров полагают, что PUE должен быть меньше 1, что Джулиан Кудрицки, исполнительный директор Uptime Institute, охарактеризовал как непонимание сути того, что такое PUE (получается, что «незнайки» есть и среди западных ЦОДов, которые мы считаем более продвинутыми по сравнению с российскими).

Интересно и отношение к публикации технических характеристик ЦОДов в открытых источниках: информацию о PUE во внешний мир выносят в общей сложности лишь 12% дата-центров, среди коммерческих ЦОДов их доля лишь немногим выше – 18%. В России ситуация аналогичная – только явно имиджевые корпоративные дата-центры сообщают свой PUE, а среди коммерческих эти данные озвучивают лишь те, кому есть чем похвастаться. К примеру, упомянутая компания DataPro заявила, что среднегодовое значение PUE ее строящегося в Москве ЦОДа не должно превышать 1,3.

ВПЕРЕД К МОДУЛЯМ. В последнее время у нас много говорят о модульном принципе построения дата-центров и связанной с ним практике создания инженерной инфраструктуры из относительно законченных решений. Практически все крупные вендоры движутся в сторону модулей (подробнее об этих тенденциях → см. с. 76). Как отметил системный архитектор Schneider Electric Алексей Соловьев, модульная стратегия создания ЦОДов позволяет упростить и ускорить проектирование всего объекта, обеспечить достижение заданных характеристик эффективности и надежности его работы (так как все компоненты собираются и тестируются в заводских условиях), сократить время инсталляции, избавиться от ручной доработки систем на площадке и облегчить последующее масштабирование дата-центра. Да, модульные конструкции при их возведении обходятся дороже обычных, но отлаженные решения обычно имеют более низкое энергопотребление и дешевле в эксплуатации. Как подчеркнул гендиректор компании «Ди Си квадрат» Александр Мартынюк, создателю дата-центра необходимо найти уникальный для каждого объекта баланс между такими противоречивыми параметрами, как надежность, стоимость и масштабируемость. Сделать это сложно, но от этого баланса зависит КПД потраченных на дата-центр денег и общая стоимость владения им за 10 лет (именно такие сроки рассматриваются сейчас серьезными заказчиками).

В мире модульный принцип уже фактически стал гегемоном: по данным упомянутого опроса Uptime Institute, на тиражируемых конструкциях строятся сегодня 57% дата-центров, а «индивидуальным пошивом» занимаются лишь 5% ЦОДов. В дальнейшем, по мнению экспертов, модульный крен будет только увеличиваться. Во всяком случае, если судить по количеству докладов, посвященных модульным дата-центрам на данной конференции DCDE, то движение в сторону модульности будет происходить и на российском рынке проектирования и строительства ЦОДов.

Евгения ВОЛЫНКИНА

Рожденные регулятором

Почему «не взлетела» MNP, что потребуется для реализации универсального обслуживания в новом наполнении? Эти вопросы российский телеком обсуждает с регулятором, инициировавшим внедрение этих услуг.

Пять лет до равенства

Справившись с телефонным неравенством, универсальная услуга связи выходит на новый уровень – ликвидации цифрового неравенства в области широкополосного доступа в интернет. В феврале 2014 г. был принят закон №9-ФЗ «О внесении изменений в Федеральный закон "О связи"», который направлен на реформирование системы универсального обслуживания и дает целевую установку достичь к 2018 г. 80% проникновения ШПД на всей территории страны. Согласно этому закону, обязанность по оказанию универсальных услуг связи возлагается на оператора, занимающего существенное положение в сети связи общего пользования на территориях не менее чем двух третей субъектов РФ. Этому требованию удовлетворяет только компания «Ростелеком» – и распоряжением правительства от 26 марта 2014 г. № 437-р именно она назначена оператором универсальных услуги связи в России.

К слову, подписанный в мае контракт между Россвязью и «Ростелекомом» несколько отодвигает заявленные в законе сроки, но поднимает планку проникновения ШПД до 93%. По контракту, будет сохранено 148 тыс. установленных таксофонов, а также 21 тыс. пунктов коллективного доступа в интернет. В то же время оператор универсального обслуживания обязан в течение пяти лет обеспечить высокоскоростным доступом в интернет населенные пункты численностью от 250 до 500 человек на скорости не менее 10 Мбит/с. Высокоскоростная ВОЛС пройдет по территории, на которой в целом проживает около 33 млн человек, точки доступа в интернет будут организованы более чем в 13,6 тыс. населенных пунктов страны.

Для реализации поставленной задачи «Ростелекому» потребуется построить около 200 тыс. км ВОЛС в дополнение к имеющимся 500 тыс. км собственных магистральных сетей и более чем 2,6 млн км местных сетей связи. По словам руководителя Россвязи Олега Духовницкого, с учетом того, что резерв универсального обслуживания небезграничен, к проекту, вероятно, потребуется «подтягивать какие-то инвестиционные программы». Как сообщил на X международном форуме операторов связи «Телеком–2014» Сергей Калугин («Ростелеком»), оператор решил войти в этот проект после того, как удалось снизить стоимость строительства километра оптического волокна практически в два раза. «Если бы этой работы не было сделано, наверное, за разумные деньги строить такую сеть было бы невозможно, – признал С. Калугин. – Нам удалось договориться с энергетиками строить сети в том числе по линиям электропередачи, что удешевит стоимость строительства и сократит его сроки».

При этом ликвидацию цифрового неравенства планируется вести и с мобильного фланга, для чего ГКРЧ в декабре 2013 г. приняла решение, в соответствии с которым операторы, продлевающие или вновь получающие лицензии на использование частот в диапазонах менее 1 ГГц, будут обязаны покрыть связью все населенные пункты численностью более 1тыс. человек, в диапазоне от 1 до 2,2 ГГц – с числом жителей более 2 тыс. человек, а в полосах частот от 2,2 ГГц до 3 ГГц – от 10 тыс. человек, расположенные на территории, где оператор имеет соответствующий частотный ресурс. «От реформы универсального обслуживания и решения ГКРЧ мы ожидаем синергического эффекта, когда ВОЛС, которые строит «Ростелеком», позволят мобильным операторам существенно расширить покрытие сотовых сетей и обеспечить население современной связью», – отметил К. Степаненко (Минкомсвязь России). По словам Павла Бородина («ВымпелКом»), для этого мобильным операторам необходимо понимать, сколько и какие именно населенные пункты должны быть покрыты сотовой связью, выбрать наиболее доступную для их населения технологию, определиться с критериями предоставления услуги. Кроме того, добавил Руслан Ибрагимов (МТС), операторы ждут законодательного закрепления форм государственно-частного партнерства, ранее реализованного в проектах телефонизации федеральных трасс и теперь планируемого к развитию при реализации универсальных услуг связи.

На базе планируемой инфраструктуры ВОЛС застраивать широкополосным доступом небольшие населенные пункты могут и другие операторы, но, как отметил глава ТТК Артем Кудрявцев, для этого им необходимо получить ясное представление о тарифах на доступ к магистралям «Ростелекома», а регулятору – помочь в снятии барьеров при входе операторов в жилые дома и, возможно, изменить подход к лицензированию. «Наверное, не совсем правильно в каждом маленьком городе выдавать много лицензий на фиксированный интернет – лучше выдавать одну лицензию, но с обязательством по застройке всей территории, – считает А. Кудрявцев. – Если у нас не будет излишней конкуренции на этой территории, то мы готовы застроить не только «лакомые» 5-этажные дома, но также и совсем малоэтажную застройку, куда идти экономически невыгодно». Пока это предложение поддержки у министерства не нашло. Относительно доступа в жилые дома К. Степаненко сообщил, что в скором времени ожидается выход постановления правительства, регулирующего создание в таких зданиях инфраструктуры, которую можно будет присоединять к внешним сетям связи.

Разбор полета MNP

Если к новой универсальной услуге отрасль только готовится, то первые результаты работы MNP уже известны и в буквальном смысле половинчаты: с момента запуска услуги из недели в неделю удовлетворяется чуть больше половины заявок на перенесение номера. Так, по данным ЦНИИС (оператора базы данных перенесенных номеров), на 8 мая уйти в другую сеть с сохранением номера пожелали 370 762 абонента, фактически перенесено 204 867 номеров. Централизованной статистики причин отказов не существует, однако операторы отмечают, что многие абоненты получают отказ по собственной вине (например, из-за долга или неправильно оформленного договора). К объективным причинам следует отнести крайне сжатые сроки, отведенные на разработку нормативно-правовой базы MNP и соответствующую модернизацию ИТ-систем операторов.

Как отметил П. Бородин, если бы услуга запускалась чуть позже, она, наверное, работала бы эффективнее. «Но это процесс новый, мы набиваем шишки, движемся вперед и совместными усилиями решим проблемы, – констатировал П. Бородин. – Надеемся, что шероховатости в нормативно-правовой базе в ближайшее время будут устранены, и MNP станет хорошо отлаженным механизмом». По мнению К. Степаненко, важен уже сам факт введения MNP. «Мы не вполне довольны процессом, который сейчас сложился, но мы его корректируем, учитывая мнения операторов и оператора базы данных переносимых номеров, – отметил К. Степаненко. – С вступлением в апреле в силу поправок, которые сделали сроки переноса номера понятными и четкими для всех абонентов (для физлиц – 8 дней, для юрлиц – 29), мы ожидаем, что II-III квартал покажет нам, насколько востребован этот сервис с уже отлаженной технологической процедурой переноса, с участием всех операторов, которые на сегодня полностью подключены к базе данных. В конце года можно будет подвести более точные итоги внедрения этой возможности для абонентов». Нормативно-правовая база будет пополняться, система – совершенствоваться, новые сервисы – внедряться, уверен и О. Духовницкий. Иначе говоря, связисты занимают оптимистичную позицию «стакан наполовину полон».

«Наполовину пустым» его считает Дмитрий Рутенберг (ФАС России), отметивший, что практически двукратный разрыв между количеством поданных заявлений на перенос и числом портированных номеров «вызывает серьезное недоумение и вопросы». Кроме того, Федеральная антимонопольная служба не удовлетворена наметившейся практикой отказа операторов «отдавать» крупных заказчиков конкурентам. «Большие надежды возлагались на MNP в секторе крупных корпоративных клиентов, в первую очередь госзаказчиков, поскольку переход органов власти от одного оператора к другому должен дать экономию для федерального бюджета, – признал Д. Рутенберг. – К сожалению, формирующаяся практика потребовала от нас административного вмешательства, и сейчас приходится мерами антимонопольного воздействия пытаться эту практику откорректировать или пустить ее в нужное русло».

MNP на весах регуляторов. О. Духовницкий (Россвязь), Д. Рутенберг (ФАС), К. Степаненко (Минкомсвязь)

По словам К. Степаненко, для упрощения перехода госзаказчиков от оператора к оператору по инициативе Минкомсвязи в настоящее время готовятся изменения в правилах оказания услуг: такая возможность будет учтена в госконтрактах. Анна Серебряникова («МегаФон») считает, что если с помощью ФАС и Минкомсвязи до конца года (начала тендеров на госконтракты) новая конкурсная процедура будет отработана, у операторов не возникнет проблем технического взаимодействия, которые сегодня влияют на MNP и его имидж. «Если проблемы возникают с большими государственными клиентами, об этом все сразу говорят, пишут, что плохо сказывается в целом на имидже услуги, – заметила А. Серебряникова. – Но я бы хотела сказать, что создание базы данных перенесенных номеров – это большой прорыв. В скором будущем ее можно использовать не только для MNP, но и для переносимости фиксированных номеров».

Примечательно, что все операторские волнения по MNP связаны именно с корпоративным сектором, а массовый, как и прогнозировалось, отреагировал на появление услуги вполне спокойно. Как заметил Александр Провоторов (Tele2 Россия), на фоне 200-миллионной абонентской базы число заявок на перенесение номера крайне незначительно. «Услуга имеет важное значение для антимонопольного регулирования и государству необходима, но нельзя сказать, что благодаря MNP ландшафт рынка драматически изменится», – резюмировал А. Провоторов.

В то же время операторы признают, что запуск MNP сработал как некий катализатор заботы об абонентах: как минимум, их начали обзванивать и интересоваться, удовлетворены ли они обслуживанием.

Само ее внедрение стало реальным дисциплинирующим фактором для операторов. Но добиться рыночного регулирования качества оказываемых операторами услуг можно лишь тогда, когда сама MNP станет отвечать предъявленным ей требованиям в полной мере. Для «подсчета цыплят» дождемся осени. А в отношении второй услуги – универсальной широкополосной – терпения придется набраться надолго.

Лилия ПАВЛОВА

Будущее финансовых сервисов – за небанковскими инструментами

Недружественные действия со стороны Visa и MasterCard заставляют задуматься о защите как национальной платежной системы, так и пользователей банковских карт. Какие небанковские инструменты выбрать банкам, стремящимся решать эти задачи? Конечно, мобильные.

Банк России планирует подходить к выбору платформы для национальной системы платежных карт (НСПК) с учетом потенциала мобильных технологий. «Формфактор карточки из пластика в обозримой перспективе будет трансформироваться, – заявил на IV международной конференции «Мобильные финансы–2014» Роман Прохоров (Банк России), – нам уже известны примеры реализации доступа к банковским счетам на базе SIM-карт, мы знаем о проекте национального электронного паспорта, который также может быть использован для авторизации клиентов». Технологическая база НСПК должна быть, во-первых, современной, во-вторых, российской, а в-третьих, совместимой с международными стандартами.

Все вышеперечисленные требования придется взять на заметку и розничным банкам, которые, согласно недавно подписанному закону «О внесении изменений в Федеральный закон "О национальной платежной системе" и отдельные законодательные акты РФ», обязаны будут предложить клиентам способ упрощенной идентификации с помощью мобильного телефона. А поскольку эта процедура требует получения подтверждения сообщенной клиентом информации от его оператора сотовой связи, кредитным организациям придется внедрять технические решения, обеспечивающие электронное взаимодействие в онлайн–режиме с базами персональных данных абонентов.

Новые мобильные технологии интересны кредитным организациям и как более экономичный, по сравнению с SMS, способ уведомить абонентов о произведенных ими транзакциях по банковским картам. Задача эта очень актуальна, поскольку незадолго до того как в силу вступила статья 9 Федерального Закона «О национальной платежной системе» № 161-ФЗ, обязывающая банки рассылать такие уведомления всем своим клиентам, операторы сотовой связи повысили тарифы на SMS.

О масштабах проблемы свидетельствуют цифры, приведенные Антоном Шишковским (MFMSolutions). Ежемесячно розничные банки отправляют своим клиентам 2,5 млрд–3 млрд уведомлений по таким «старым» и в последнее время достаточно дорогим каналам, как SMS и USSD. Между тем, переход к более современной технологии push-нотификации оповещения клиентов, пользующихся смартфонами, помог бы существенно снизить эти затраты. Это облачная технология, которую в том или ином виде поддерживают все ведущие поставщики мобильных платформ: Apple, Google, Microsoft, – их сервисы обеспечивают доставку любого контента на смартфоны по протоколу TCP/IP. При этом одно сообщение может использоваться для доставки контента любого формата (текста, изображения, аудио-, видеозаписи), тогда как SMS при превышении определенного объема знаков делятся оператором на сегменты, каждый из которых тарифицируется, как отдельное сообщение.

Работают сервисы push-нотификации следующим образом. Приложение, установленное на мобильное устройство, инициирует отправку его индивидуального идентификатора на push-сервер – регистрируется на платформе. После этого банк может передавать на нее свой контент. В свою очередь, эта платформа посредством сервисов Apple или Google отправляет на смартфон или планшет клиента push-нотификацию. С ее помощью приложение скачивает с сервера контент, а push-сервер сообщает банку статус доставки.

Компания MFMSolutions располагает решением push-рассылок, как на «участке взаимодействия» системы ДБО кредитной организации и платформы push-нотификации, так и между ней и мобильными устройствами клиентов. Похожее решение обещает к лету запустить компания BSS. Как утверждает Алексей Зотов (BSS), новый сервис будет доставлять push-уведомления банков не только на смартфоны клиентов (как частных, так и корпоративных), но и на некоторые носимые устройства, например, на «умные» часы Samsung Galaxy Gear. А в следующей версии продукта такие уведомления можно будет отправлять в популярные мобильные мессенджеры – Skype, Viber, WhatsApp, ICQ и другие, а также социальные сети Facebook и «ВКонтакте» и на электронную почту.

Понятно, что возможность взаимодействовать с клиентом через множество современных, а главное, привычных для него каналов будет оценена банковским сообществом по достоинству. А значит, велика вероятность, что спрос на SMS-рассылки операторов связи при сохранении их высокой цены будет снижаться, как это, собственно, и происходит сегодня на массовом рынке, где WhatsApp и Viber постепенно заменяют собой SMS.

Александра КРЫЛОВА

Законодательная гиря телемедицины

Тормозом для внедрения передовых телемедицинских решений остается отсутствие нормативно-законодательной базы.

На информатизацию здравоохранения в последние годы государство потратило внушительные суммы. Ушли они главным образом на инфраструктурные проекты, так что мгновенного практического эффекта от них для пациентов ожидать не приходится. По мнению специалистов, процесс информатизации явно тормозит состояние нормативно-правовой базы, которая никак не приблизится к реальности и возможностям информационных технологий. Поэтому информатизация здравоохранения по-прежнему носит лоскутный характер. Это же относится и к телемедицине, что в очередной раз подтвердила 2-я международная конференция «Инфокоммуникации в здравоохранении. Создание национальной телемедицинской системы».

В. Столяр: «Дистанционное обучение врачей – одно из направлений телемедицины с очень высокой экономической эффективностью»

Есть интересные телемедицинские проекты, работающие в рамках отдельных организаций и регионов. Особенно это касается приложений, для которых пробелы в нормативной базе не так критичны. Например, хорошо разработаны технологии для дистанционного обучения врачей и студентов-медиков. Руководитель УЦ научно-клинического центра «РЖД» Валерий Столяр считает, что такое обучение должно быть обязательно интерактивным и строиться на базе профессиональных систем ВКС с соответствующими каналами связи, потому что оно будет эффективным, только если у обучающихся есть возможность задавать вопросы, выбирать изображения с разных видеокамер, фиксирующих процесс операции, слышать комментарии хирурга, получать стереоскопическое изображение с камер на его шлеме и т.п. Но есть и телемедицинские приложения «для бедных»: в Татарстане уже прошло тестирование мобильного диагностического комплекса для фельдшерско-акушерских пунктов, и на этот год запланировано его внедрение в промышленную эксплуатацию. Весь «комплекс» упаковывается в небольшой чемоданчик, и входит в него только то, что потянет сельская медицина – тонометр, электрокардиограф, пульсоксиметр и т.п. Полученные данные сельский фельдшер может передать в республиканское «медицинское облако» и оттуда получить результаты по каналу со скоростью всего 16 Кбит/с.

Телемедицинских приложений разработано немало, но для их эффективного использования нужен объединяющий системный проект и законодательное обеспечение. Еще в 2001 г. появился приказ Минздрава и тогда еще существовавшей РАМН «О введении в действие концепции развития телемедицинских технологий в РФ». В 2010 г. на Межпарламентской ассамблее СНГ был принят модельный закон «О телемедицинских услугах», а затем в законе «Об обязательном медицинском страховании» (№ 326-ФЗ от 29.11.2010) определены возможности финансирования телемедицинских систем из средств ОМС. В конце декабря 2012 г. специалисты, работающие в разных направлениях, имеющих отношение к телемедицине, образовали рабочую группу, которая поставила своей целью инициировать построение национальной телемедицинской системы. Создание специального закона о телемедицинских услугах было признано слишком долгим делом, поэтому рабочая группа взялась за подготовку поправок в имеющийся закон «Об основах охраны здоровья граждан в РФ» (№323-ФЗ от 21.11.2011). Как рассказал заместитель директора ЦНИИ организации и информатизации здравоохранения Георгий Лебедев, предлагаемые рабочей группой изменения касаются 12 статей этого закона. В них нет ничего революционного, в большинстве своем это точечные дополнения, фиксирующие возможность использования телемедицинских технологий в системе организации медицинской помощи. Однако продвижение этих предложений, позволяющих создать законодательную основу для массового внедрения телемедицинских услуг, идет очень туго, дальше разговоров в околодумских кулуарах дело пока не двинулось.

Недавно Минздрав провел встречу с разработчиками и производителями решений в сфере телемедицины, заявленной целью которой была подготовка предложений по координации государственной политики и нормативному правовому регулированию в сфере телемедицины, но каковы будут ее последствия, пока непонятно.

Теперь в профессиональном сообществе появилась идея о создании саморегулируемой организации (СРО), которая могла бы объединить всех участников этого рынка для формирования его правил и продвижения законодательных изменений. Станислав Глазов («Интеллект Телеком»), считает, что в создании такого СРО заинтересованы не только страховые компании, медицинские учреждения, операторы телематических услуг, производители медицинских устройств и лекарств, но и само государство, если оно действительно хочет получить эффективно работающую телемедицину. Но насколько быстро будет реализована эта идея, будет ли она реализована вообще и если да, то в какой форме и с каким результатом, зависит, конечно, прежде всего, от активности потенциальных участников.

Евгения ВОЛЫНКИНА

Блог, еще раз блог!

Михаил ЕМЕЛЬЯННИКОВ

Проверьте ваши сайты

>>>> Роскомнадзор без особой помпы, тихо и спокойно стал использовать в ходе надзора за соблюдением законодательства о персональных данных такую форму контроля, как систематическое наблюдение. В «Докладе об осуществлении государственного контроля (надзора) и об эффективности такого контроля (надзора) за 2013 г.» сообщается, что «в 2013 г. центральным аппаратом Роскомнадзора была проведена оценка содержания и правовых оснований деятельности 250 интернет-ресурсов, осуществляющих деятельность в российском сегменте сети Интернет».

В 101 случае нарушений законодательства не было выявлено, на сайтах размещалась контактно-справочная информация государственных, муниципальных органов и юридических лиц, а также персональная информация, публикация которой разрешена в силу федеральных законов (данные из различных реестров: ЕГРЮЛ, ЕГРИП, Реестра кадастровых инженеров и т.п.). В деятельности 149 интернет-ресурсов выявлены нарушения требований законодательства, по результатам принятых Роскомнадзором мер реагирования в 60 случаях персональные данные удалены администраторами, в 19 случаях материалы по результатам мониторинга были направлены в органы прокуратуры для рассмотрения вопроса о возбуждении дела об административном правонарушении по ст. 13.11 КоАП РФ.

Если ваша организация разместила на своем сайте веб-форму, предусматривающую сбор персональных данных (кредитное заявление, анкета соискателя вакантной должности, форма для подготовки договора страхования и т.п.), создало пользователям личный кабинет, опубликовало списки аффилированных лиц или лиц, оказывающих существенное воздействие на деятельность организации и т.д., на сайте в интернете (логично на том же, но закон этого не требует) должна быть и политика в отношении обработки персональных данных и сведения о реализуемых требованиях к их защите. Есть веб-форма (кабинет, список) и нет политики – административное правонарушение. Выявляется легко и просто за несколько минут, и не нужны никакие выездные и документарные проверки.

комментировать

Михаил ТАРАСОВ

Так в «Аэрофлоте» умеют считать или нет?

>>>> «Аэрофлот» построил собственный ЦОД. Вот что говорит об этом заказчик.

Цитата 1: «Совокупная стоимость аренды необходимой нам инженерной инфраструктуры, включая дополнительные услуги, уже через два года превысила бы совокупную стоимость владения собственным ЦОДом, включая капитальные затраты на его реализацию и эксплуатацию за тот же период». Вот, молодец, посчитал.

Цитата 2 (о результате внедрения интеллектуальных технологий в компании): «Трудно назвать конкретную цифру в целом по компании, так как любой проект – это совокупность технических, организационных, финансовых и коммерческих мероприятий, и трудно вычленить именно роль интеллектуальных технологий и систем в конечном экономическом эффекте». А тут что-то стушевался....

комментировать

ДЕЙВ ЭВАНС

Носимые устройства – носители знаний

>>>> Зарождающийся рынок носимых устройств обладает серьезным потенциалом роста. На данный момент существуют около 160 наименований таких устройств, но, по прогнозам аналитиков из IDTechEx, в ближайшие 10 лет объем этого рынка достигнет $70 млрд. Тем не менее многие пока лишь смутно себе представляют, что такое носимые устройства и какие инновационные возможности они открывают в мобильном мире всеобъемлющего интернета.

Каждое следующее поколение технологий уменьшается в размерах по сравнению с предыдущим. За 10 лет габариты устройств сокращаются в 100 раз. В середине 1980-х мы пользовались отдельными музыкальными проигрывателями, телефонами и калькуляторами, а сегодня все они умещаются в одном устройстве – смартфоне. Так как наряду с этой тенденцией разрабатываются микроскопические датчики и компьютеры размером с песчинку, становится ясно: мы только приближаемся к пониманию того, сколь широки возможности интернета вещей и мобильных технологий.

Большинство доступных сегодня носимых устройств могут получать сведения о действиях, которые мы выполняем, но они ничего не сообщают нам о процессах, происходящих во время этих действий. Сейчас мы наблюдаем эволюцию носимых устройств: акцент смещается на процессы и сбор информации, способной изменить нашу жизнь. Например, нынешние браслеты или наручные часы могут определить, что человек двигается, но ничего не могут сообщить о происходящих в его организме биологических процессах – например, об уровне глюкозы или кровяном давлении. Однако недавно Google протестировала новый метод отслеживания уровня сахара в крови для диабетиков с помощью подключенной контактной линзы. Соприкасаясь с телом и измеряя уровень сахара в слезе и слезных протоках, линза позволяла получать показатели глюкозы ежесекундно.

комментировать

Петр ДИДЕНКО

Получил УЭК

>>>> Через четыре месяца и пять дней после обращения Сбербанк выдал мне универсальную электронную карту (УЭК) с платежной системой Pro100 на борту, которая готовится стать основой национальной платежной системы.

О процессе. Сегодня я увидел на сайте, что можно приходить за УЭК. Сами они никак не уведомляют о том, что карта готова. При этом у них есть мой телефон и e-mail. Но все равно надо ходить к ним на сайт и, вбивая в специальную формочку серию и номер заявления, проверять, не готова ли заветная карта. Три дня назад была не готова, сегодня оказалась готова.

Напомню, подавал я заявление через Сбербанк на Б. Грузинской, 37. Сегодня приехал туда в 17:30. Молодой человек в окошке с надписью «Выдача универсальной электронной карты» сказал мне, что уже закончил работу. Спасибо. По телефону сказали, что можно приезжать до 19:30. Оказалось, до 19:30 выдают любые карты, включая УЭК, а этот специалист по УЭК работает только до 17:00.

ОК. Но потом оказалось, что записать ЭЦП на УЭК может только он. Мистика – он сидит в двух метрах, но «закончил» работу и не хочет мне помогать. Операционист, которая отдала мне карточку, дала список из вороха мест, где мне завтра могут «записать ЭЦП». Посмотрим, как это будет.

комментировать

Sputnik

>>>> По поводу запуска «Ростелекомом» госпоисковика «Спутник». В общем, «Спутник» получился ничего для бета-версии ☺. Качество выдачи, конечно, похуже, чем у настоящих поисковиков, да и зарубежного контента почти нет. Но для тех, для кого этот сервис задумывался, такого качества поиска вполне достаточно. Да и если, как говаривал предыдущий министр связи, остальные поисковики «подотключить», то это качество автоматически станет лучшим на рынке.

Понравились попытки давать решения проблем пользователя, а не ответы на вопросы, как делают традиционные поисковики. Вот «Яндекс» придумал «Острова» и уже с полтора года ходит вокруг да около – никто особенного счастья от идеи так и не получил. А у «Спутника» видны попытки предлагать какие-то решения прикладных задач прямо с первого дня (та же оплата ЖКХ).

комментировать

Wireless cards

Подумалось, мой кошелек «светится» наружу целым ворохом беспроводных карточек – NFC-карты Visa и MasterCard нескольких банков, несколько proximity-кард для доступа в разные офисы и помещения, NFC-карта для доступа в метро и т.д.

Скоро, возможно, не нужно будет воровать мой кошелек, чтобы спереть у меня что-то ценное. Достаточно будет постоять рядом ☺. Действительно, сейчас можно спереть мой доступ в gmail и на время де-факто стать мной. На деле все не так страшно – защита от такого сценария есть, и она встроенная. Интересно, всегда ли она работает и в полной ли мере.

Недавно в мои руки попала американская green card довольно свежего выпуска. Оказывается, теперь их выдают в специальном чехольчике, который не позволяет карточке быть считанной без разрешения. Иногда такие чехлы раздают и банки. Интересно, сколько смысла в подобной защите и реально ли она что-то меняет.

комментировать

Джим СКОТТ

Малые соты

>>>> Сегодня ИТ-директор сталкивается с проблемами, которых просто не существовало в те времена, когда за подключение отвечал лишь Ethernet-кабель, подсоединенный к док-станции или настольному ПК. Мир изменился, и мы хотим более гибкого доступа и ждем, что на рабочем месте все будет так же, как при общении с собственными персональными устройствами.

Одно дело иметь структуру, которая при помощи политик обеспечит сотрудникам мобильность, и совсем другое – гарантировать доступ как реальный рабочий инструмент. Если из-за перемещения из одного места в другое доступ к приложению «мерцает», а разговор по телефону при входе в здание прерывается, то это большая проблема, и ее нужно решать.

В идеальной мобильной среде сотовые сети и Wi-Fi работают вместе, передача голоса и данных осуществляется одинаково для всех как внутри, так и вне зданий, а пользователям нет нужды знать, как реализуется доступ к приложениям и бизнес-сервисам – они просто должны иметь такую возможность.

А что вы скажете, узнав, что можете все это осуществить? Создать свою универсальную беспроводную сеть, где будет работать не только Wi-Fi, но и сотовая связь? Ключом к решению могут стать универсальные малые соты. Они обладают немалым интеллектом и высокой степенью автоматизации, поддерживают разнообразные протоколы беспроводной связи – 3G, 4G, Wi-Fi – и при этом достаточно просто встраиваются в существующие сетевые и Wi-Fi-инфраструктуры.

комментировать

11–12 сентября в Москве (отель Marriott Royal Aurora) пройдет 3-я отраслевая конференция **«IT в ритейле: идеальный маршрут к сердцу клиента через ноу-хау. Лучшие практики–2014».** Ключевые темы мероприятия: стратегия omni channel, ИТ-поддержка работы с клиентами, программы лояльности и прогнозирования спроса и др. В рамках дискуссионного клуба будут рассмотрены перспективы развития онлайн-ритейла и облачных технологий. Участников ждет топ-20 лучших практических примеров и выставка передовых ИТ- достижений.

Организатор – компания infor-media Russia.

www.itretail-conf.ru

выставки, семинары, конференции

Дата и место проведения, организатор, сайт	Наименование мероприятия
04–05.09. Москва. ИКС-МЕДИА: www.dcforum.ru	**9-я ежегодная международная конференция и выставка «ЦОД–2014»**
10.09. Москва. Connectica Lab: www.sharing-forum.com	4-й международный форум Telecom Networks 2.0. Broadband Infrastructure, Sharing, Engineering, Outsourcing, Development end Metering
10–13.09. Крым. НОУ «Академия информационных систем»: www.vipforum.ru	13-я всероссийская конференция «Информационная безопасность. Региональные аспекты. ИнфоБЕРЕГ–2014»
11–12.09. Москва. infor-media Russia: www.itretail-conf.ru	3-я отраслевая конференция «IT в ритейле: идеальный маршрут к сердцу клиента через ноу-хау. Лучшие практики–2014»
16–18.09. Санкт-Петербург. Минкомсвязь России: www.pki-forum.ru	XII международная конференция по проблематике инфраструктуры открытых ключей и электронной цифровой подписи «PKI-Forum Россия–2014»
19.09. Москва. DLP - Expert: http://bis-expert.ru/bis-summit	5-я международная конференция DLP-Russia
21–23.09. Подмосковье. Клуб топ-менеджеров 4CIO.ru: www.4cio.ru	8-й конгресс «Подмосковные вечера»

Присылайте анонсы ваших мероприятий на IKSMEDIA.RU

Еще больше на

9–10 октября в Москве (конгресс-центр гостиницы «Космос») пройдут юбилейная XV ежегодная специализированная конференция и выставка **«Информационные технологии в медицине».** К участию в работе конференции приглашаются руководители и специалисты медицинских организаций, отвечающие за внедрение информационных технологий в здравоохранении и социальной сфере.

Основные темы конференции: формирование информационных ресурсов в области здравоохранения, организация информационного взаимодействия различных уровней; персонифицированный учет медпомощи; структура ИЭМК и ЭМК; технология сбора и обработки, защиты данных, опыт реализации «пилотных» проектов; нормативное, правовое и технологическое обеспечение информационного взаимодействия в сфере здравоохранения; создание и использование единой унифицированной социальной карты гражданина РФ; комплексная автоматизация ЛПУ; специализированные медицинские информационные системы; телемедицинская помощь, применение телекоммуникационных, мобильных и веб-технологий при оказании медицинской помощи; информационные технологии в системе непрерывного профессионального образования работников здравоохранения. Планируется проведение специализированных семинаров и панельных дискуссий.

В рамках выставки и конференции традиционно проходит заключительный (смотровой) этап конкурса разработок в области информатизации здравоохранения «Лучшая медицинская информационная система–2014».

До 30 августа 2014 г. открыт прием заявок на участие в экспозиции со стендом.

Организатор – компания «Консэф».

www.itm.consef.ru

выставки, семинары, конференции

Дата и место проведения, организатор, сайт	Наименование мероприятия
23.09. Москва. AHConferences: www.ahconferences.com	XI CRM-форум
24.09. Москва. AHConferences: www.ahconferences.com	XIII конференция «Информационные технологии в страховании»
24–26.09. Москва. Компания «Гротек»: www.infosecurityrussia.ru	Международная выставка InfoSecurity Russia–2014
06–07.10. Москва. TelCap Ltd: www.capacityconferences.com	Capacity Russia & CIS–2014
15.10. Москва. Connectica Lab: www.revassurance-forum.com	V всероссийская конференция Revenue Assurance, Fraud & Risk Management–2014
15-16.10. Москва. Ассоциация российских банков, компания «АйФин медиа»: www.abaforum.ru	I международный форум «Вся банковская автоматизация–2014»
23.10. Москва. Ассоциация менеджеров России, издание Intelligent Enterprise, информационный ресурс iBusiness.ru, компания KPOK: www.itleader.ru	11-й ежегодный деловой форум «IT-Лидер»

21–23 сентября в Подмосковье («Атлас Парк-отель») состоится конгресс «Подмосковные вечера». Основная тема – «ИТ: в поисках позитива». Проводимый в восьмой раз конгресс – это крупнейшее независимое мероприятие, наиболее точно воспроизводящее атмосферу и веяния ИТ-отрасли, дающее возможность для личного профессионального роста и обмена опытом с коллегами; это множество событий как деловых, так и неформальных, традиционных и новых – и по формату, и по содержанию. Интерес к обсуждаемым темам обеспечен тем, что участники конгресса выбирают их заранее.

Организатор – клуб топ-менеджеров 4CIO.ru

http://www.4cio.ru

24–26 сентября в Москве (МВЦ «Крокус Экспо») пройдет выставка **InfoSecurity Russia–2014** – главное событие для заказчиков, вендоров и инсталляторов оборудования и систем в области хранения данных, электронного документооборота, ИТ-инфраструктур сетей и информационной безопасности. В деловой и экспозиционной программе – проведение лидерами рынка семинаров по инновационным разработкам и продуктам; прогнозы развития спроса в разных сегментах российской экономики, представленные ведущими консалтинговыми аналитическими агентствами; обсуждение перспектив технологического развития; брифинги регуляторов рынка для заказчиков и закрытые семинары для экспонентов выставки.

Ожидается более 6000 профессиональных посетителей (49, 4% – представители компаний-заказчиков), более 4000 слушателей мероприятий деловой программы.

Организатор – компания «Гротек».

www.infosecurityrussia.ru

24 октября на круглом столе **«Образование поколения NEXT: ИТ в школе и вузе»** речь пойдет о том, как ИТ и ИКТ помогают вывести образование на новый уровень. Техническое оснащение учебных заведений, умение педагогов пользоваться им в повседневной обучающей деятельности; внедрение электронных средств для взаимодействия всех участников образовательного процесса; e-learning и дистанционное обучение; электронные книги и библиотеки; использование частных и публичных социальных сервисов для обучения; использование интернет-технологий для организации непрерывного образования и вычерчивания индивидуальной образовательной траектории для каждого студента – вот лишь часть вопросов, которые стоят перед современными образовательными учреждениями и будут обсуждаться на круглом столе.

Организатор – ИКС-МЕДИА.

www.iksmedia.ru/conferences.html

Ведущая темы
Лилия ПАВЛОВА

Будь

В классической парадигме информационной безопасности «снаряд – броня» обычно рассматриваются технические средства нападения и защиты – условно говоря, пушки, танки, самолеты против крепостей, окопов, противотанковых мин и проч. Но на войне как на войне: первое и последнее слово – за человеком. Он нападает, он обороняется – и даже самая современная техника не защитит, если ею не пользоваться или, хуже того, открывать ворота крепости перед противником. И хотя потери в киберпространстве – это не человеческие жертвы, а «всего лишь» финансовый, репутационный, юридический и технический ущерб для предприятия, ценой этого ущерба может оказаться жизнеспособность бизнеса.

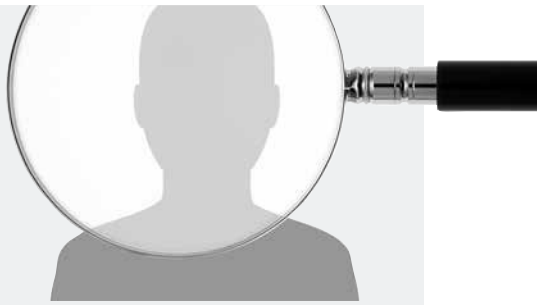
Ежегодные потери мировой экономики от киберпреступлений аналитики оценивают в $500 млрд. При этом большинство инцидентов информационной безопасности эксперты относят к категории неумышленных, когда персонал компании не выполняет необходимых инструкций, причем не из вредности, а в силу отсутствия соответствующих навыков.

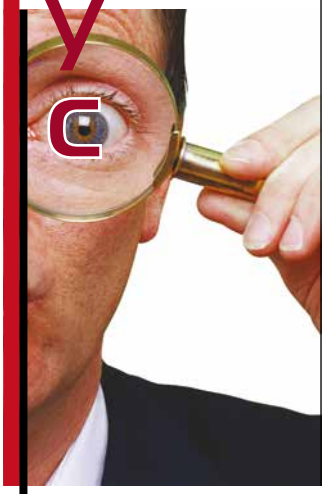
«Человеческий фактор» – самое слабое звено инфобезопасности. Как отметил один из экспертов «ИКС», иммунитет к физическим болезням человечество вырабатывало тысячелетиями, а теперь необходимо вырабатывать «информационный иммунитет». Как в реальной жизни мы привыкли заботиться о профилактике заболеваний, так и в виртуальной среде потребуется научиться с детских лет выполнять правила «информационной гигиены». Очевидно, процесс приучения займет не один год. И, на наш взгляд, в выработке «информационного иммунитета» человечества трудно преувеличить роль средств массовой информации, особенно профессиональных. Согласны?

инфобдителен!

фокус

Фактор «Ч»





Это изнанка рынка информационной безопасности. «Человеческий фактор» инфобезопасности вычерпывает из мировой экономики миллиарды долларов, но одновременно оказывается и драйвером индустрии. В чем особенности этого феномена?

Из трех групп угроз безопасности информации – антропогенной, техногенной, стихийной – первая самая массовая и всепроникающая. В результате деятельности злоумышленников, недобросовестных партнеров и конкурентов, а также ошибок собственного персонала бизнес в любой момент может оказаться перед фактом утечки/кражи конфиденциальной информации и персональных данных, воровства денежных средств, заражения вредоносным ПО, состоявшейся атаки на информационные ресурсы предприятия.

С одной стороны, организованным фронтом наступает мир киберпреступности, и это уже не хакеры-одиночки, пишущие вирусы из любви к искусству программирования, а крупные синдикаты с миллиардными прибылями, постоянно расширяющие круг потенциальных жертв. К слову, российский рынок киберпреступности стал первым, на котором еще в 2004 г. была организована торговля вредоносным кодом. По данным исследования Trend Micro Russian Underground Revisited, сейчас на нем представлен широкий ассортимент «услуг»: взлом аккаунтов в социальных сетях или аккаунтов электронной почты; услуги хакеров, связанные с обработкой сетевого трафика; продажа троянских программ и сплойтов (встроенного кода, эксплуатирующего уязвимости легальных программ, копии которых загружают пользователи), а также криптеров, которые с помощью «заглушек» скрывают зараженные файлы или вредоносное ПО от программ информационной безопасности; хостинг выделенного сервера, который может использоваться злоумышленниками для централизованного управления зараженными компьютерами или для размещения вредоносных файлов; спам-рассылки; организация DDoS-атак.

С другой стороны, компании стремятся защититься имеющимися в арсенале индустрии инфобезопасности средствами и организационными мерами. В центре этого противостояния – человек, который активно или пассивно, но неизбежно оказывается либо в стане защитников, либо в армии нападающих.

Синдром утекающей информации

Утечки конфиденциальной информации – это реалии жизни современных организаций во всем мире. По данным аналитического центра InfoWatch, только в первой половине прошлого года ущерб (затраты на ликвидацию последствий утечек, судебные разбирательства, ком-

Каналы утечек конфиденциальной информации

Рейтинг экспертов «ИКС»

1. **Съемные носители,** в том числе у привилегированных пользователей и администраторов (самая распространенная и ведущая к большим потерям проблема).
2. **Электронная почта** (утечки происходят как намеренно, так и по халатности).
3. **Веб-сервисы:** файлообменники, мессенджеры, социальные сети (легко выгрузить в облако большой объем информации или обнародовать непубличные сведения).
4. **Бумажные носители** (сложно контролировать вынос за периметр компании).
5. **Мобильные устройства** (сложно контролировать информационные потоки).
6. **Кража/потеря** мобильного устройства.

пенсационные выплаты), который понесли компании вследствие утечек информации, составил $3,67 млрд. На самом деле утечек гораздо больше, поскольку в СМИ, публичных материалах компаний и госорганов упоминается лишь об 1–5% всех утечек по разным каналам. Иначе говоря, размер возможного ущерба от утечек достигает десятков, а то и сотен миллиардов долларов. Информация упрямо утекает даже при использовании самых современных технологических средств ее защиты.

К объективным причинам эксперты «ИКС» относят постоянный рост объемов данных и числа мест их хранения (серверы, компьютеры, мобильные устройства пользователей, облачные хранилища и т.д.). Все больше процессов переходит в компьютерно-сетевую сферу – и в силу упрощения технологий передачи данных все чаще происходят неумышленные утечки. Одно дело запись файла на USB-флешку и совсем другое – автоматическая синхронизация данных между телефоном и ноутбуком через беспроводную сеть. Потеря пользователем контроля над тем, какие данные и где у него хранятся, – прямой путь к их утечке, уверены наши эксперты. Ситуация осложняется тем, что в конфликт входят удобство пользования и безопасность, и здесь в действие вступает субъективная причина – человек. И не только легкомысленный пользователь, но и главный в этом деле субъект – специалист в области информационной безопасности.

Почему бессильны технологии

Инструментарий безопасников для борьбы с утечками обширен. Это и решения вендоров для обеспечения безопасности данных на пользовательских устройствах, и системы предотвращения утечек (DLP), и средства обнаружения и предотвращения вторжений (IDS/IPS), и комплексы для идентификации и управления доступом к информационным ресурсам (IDM), и интегрированные системы управления информационной безопасностью (СУИБ), и другие технологии. Однако, как замечают эксперты «ИКС», все перечисленное – лишь средства контроля, которые неэффективны до тех пор, пока не будут определены объекты контроля, правила их перемещения и изменения, расписаны роли пользователей и определены наказания за нарушения. Любое перемещение информации имеет бизнес-контекст, без понимания которого невозможно принять автоматическое решение «разрешить/запретить», поэтому мало просто купить систему – необходимо обучить персонал правилам обращения информации в компании, а этому большинство сотрудников служб информационной безопасности просто не обучены. Без постоянной работы с сотрудниками по поддержанию и совершенствованию процессов компании ни одно средство защиты не стоит потраченных на него денег.

Более того, нередко в компаниях реализуются проекты внедрения технических средств защиты информации, но потом этими средствами практически не пользуются. Скажем, компания выбрала современную систему DLP, внедрила, на этом остановилась или перешла к следующему внедрению, а отчеты DLP-системы никто регулярно не изучает, не работает с инцидентами, не реагирует на них.

К слову, в ходе недавнего проекта Cisco по мониторингу угроз было обнаружено, что даже при использовании систем DLP в 100% проанализированных коммерческих сетей трафик направлялся на веб-сайты, на которых было размещено вредоносное ПО; в 92% сетей обнаружился трафик на пустые веб-страницы, на которых обычно осуществляются вредоносные действия; из 96% проанализированных сетей трафик направлялся на уже взломанные и скомпрометированные серверы.

Кто виноват и что делать

В идеале защитой информации в организации должны быть озабочены абсолютно все сотрудники, от гендиректора до уборщиц. Эксперты разделяют их вклад в обеспечение информационной безопасности на три категории: активная – управление и контроль за системами безопасности (службы ИБ, ИТ), косвенная – подбор и обучение персонала, корпоративная культура и этика (HR-служба и топ-менеджмент) и пассивная – соблюдение политик безопасности, недопущение возникновения инцидентов безопасности в пределах своей зоны ответственности и компетенции (рядовые пользователи).

Но жизнь далека от идеала. Топ-менеджмент в большинстве случаев основную роль в обеспечении информационной безопасности отводит ИБ-службе, требуя от нее быстрого самостоятельного решения всех проблем. В результате подразделения инфобезопасности не справляются с потоком задач, которые постоянно возникают в повседневной жизни любой организации. И хорошо еще, если такое подразделение в принципе на предприятии есть (по данным исследования «МФИ Софт», лишь в 18% российских компаний есть специалисты или отделы информационной безопасности). HR-службы не особенно обеспокоены прохождением сотрудниками тренингов по инфобезопасности при их приеме на работу, а также по окончании каждого года или при серьезном изменении информационной системы или бизнес-процессов компании; не работают над выявлением нелояльных и немотивированных пользователей и повышением их лояльности. Службы ИТ и ИБ нередко входят в конфликт (→ см. с. 41). А пользователи теряют, забывают, уносят, передают. Именно «пассивная» категория наносит основной ущерб, поскольку действия или бездействие рядовых сотрудников обычно и приводят к утечкам ценной информации.

Взращивание корпоративной культуры информационной безопасности – задача топ-менеджмента, считают эксперты «ИКС». От отношения к этому вопросу руководителей зависит эффективность и само существование организационной и технической инфраструктуры, обеспечивающей инфобезопасность предприятия. Еще лучше, если в состав топ-менеджмента вводится руководство ИТ/ИБ в ранге заместителей генерального директора или его прямых подчиненных, имеющих право выдавать распоряжения по компании в рамках своей компетенции. В этом случае роль ИТ/ИБ выходит на новый уровень. Безопасники и айтишники встают во главе формирования корпоративной культуры информационной безопасности: разрабатывают и

проводят в жизнь необходимые меры по совершенствованию процедур инфобезопасности в компании, контролируют их соблюдение. Но даже если руководство ИБ не возведено в ранг топов, корпоративная культура информационной безопасности может формироваться на основе «должностной инструкции», составленной по рекомендациям экспертов «ИКС».

Мы – не роботы, роботы – не мы

Если бы все сотрудники компаний все делали в соответствии с правилами и политиками информационной безопасности, никаких утечек не было бы. Но, судя по коллективному портрету, составленному экспертами «ИКС», достичь уровня идеального пользователя невозможно.

Будучи сотрудниками тех или иных организаций, все мы неизбежно оказываемся также частью массового рынка инфобезопасности, который должен защищаться от вирусов, мошенников и прочей кибернечисти. Как от нее обороняться? Эксперты «ИКС» выделяют три категории современных направленных против пользователей мошеннических схем: взлом рабочих мест пользователей, социальная инженерия и угрозы мобильным устройствам. В каждом случае эксплуатируются широкие возможности потребления контента пользователями – и проблем можно было бы избежать, если бы новостные порталы операторов, поисковые системы, социальные сети, системы онлайн-банкинга, магазины приложений при заключении договора информировали пользователей о сопутствующих рисках информационной безопасности. Кроме того, желающих злоупотребить доверчивостью или неосведомленностью пользователей стало бы гораздо меньше, если бы государство законодательно установило киберпреступникам более жесткое наказание, чем нынешние условные сроки, а примеры раскрытия их преступлений и последовавшего наказания широко освещались.

Думается, проблема «информационной гигиены» уже действительно назрела. Полумерами не отделаться. К этому выводу, похоже, приходит и государство, с трибуны Совета Федерации предлагающее ввести основы информационной безопасности и защиты от интернет-мошенничества в школьную программу ОБЖ и предусматривающее подключение к обучению инфобезопасности родителей и школьных учителей (что

Основы корпоративной культуры информационной безопасности

Топ-менеджмент. Обеспечивает административным и бюджетным ресурсом. Подтверждает важность информационной безопасности для бизнеса, утверждает общую концепцию ИБ, определяет приоритетность мероприятий по борьбе с утечками. Принимает правила обращения информации в компании, легитимизирует систему контроля этих правил и ответственность за их нарушение. Соблюдает правила работы с конфиденциальной информацией (пример для других сотрудников).

HR-служба. Совместно со специалистами классической службы безопасности на этапе собеседования и изучения резюме рассматривает кандидата с точки зрения рисков, обращает пристальное внимание на людей, переходящих из конкурирующих компаний, анализирует доступную информацию о кандидате в социальных сетях и т.п. При положительном решении о принятии кандидата в штат запускает процесс повышения осведомленности: информирует о важности той информации, с которой предстоит работать сотруднику, подписывает с ним договор о неразглашении. Регулярно проводит обучающие семинары для сотрудников по правилам работы с конфиденциальной информацией. Создает систему обратной связи, когда нарушители обязаны заново обучаться и подтверждать знание правил работы с конфиденциальной информацией. Совместно со службой экономической безопасности реализует принцип неотвратимости наказания. Обеспечивает систему поощрения (планирование карьеры, социальные пакеты, talent management, «пожизненный найм» и др.), препятствующую коммерческому подкупу или злоупотреблениям служебным положением, направленным на организацию утечки.

ИТ-служба. Учитывает вопросы защиты информации при проектировании, реализации и внедрении информационных систем. Обеспечивает надлежащий уровень безопасности при хранении информации и работе с ней (к примеру, шифрование на общих ресурсах и персональных компьютерах). Поддерживает средства мониторинга и отдельных расследований.

ИБ-служба. Обеспечивает комплексный подход к защите информации во взаимодействии со службами ИТ, внутренней безопасности, экономической безопасности, управления персоналом. Контролирует распространение информации (контроль доступа) и отслеживает работу пользователей с применением специализированных программно-аппаратных комплексов. Осуществляет мониторинг каналов утечки и расследование инцидентов. Поддерживает горячую линию сбора информации о нарушениях. Реагирует на инциденты, проводит внутренние расследования и передает их результаты топ-менеджменту, ИТ- и HR-службам. Совместно с HR-службой повышает осведомленность сотрудников, два-четыре раза в год проводит для них обучение. Отчитывается перед высшим руководством компании (развитие и при необходимости пересмотр концепции защиты информации; анализ инцидентов; развитие методологии, мер и средств обеспечения инфобезопасности).

Рядовые пользователи. Соблюдают правила работы с конфиденциальной информацией. Информируют ИБ-службу об обнаруженных нарушениях.

Идеальный с точки зрения информационной безопасности сотрудник предприятия – это:

… сотрудник, понимающий, что от его действий зависит будущее не только компании, но и его собственная информационная защищенность;

… фактически член команды безопасников, понимающий, что́ и зачем он делает, и прилагающий усилия для создания обратной связи в целях совершенствования системы безопасности;

… ответственный, внимательный и квалифицированный пользователь, которому не чужды интересы компании;

… информационно грамотный, думающий, лояльный и преданный компании специалист;

… ответственный человек, соблюдающий регламенты информационной безопасности, в полной мере осознающий важность их выполнения;

… хорошо мотивированный молодой карьерист;

… человек думающий;

… неизвестный науке индивидуум;

… компьютер, желательно не подключенный к интернету;

… робот, четко соблюдающий заложенные инструкции и не требующий обслуживания;

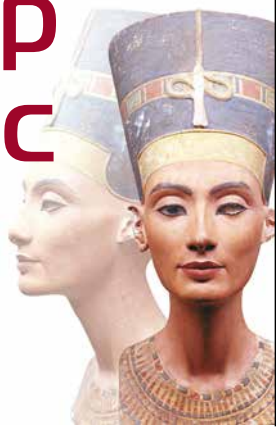
… робот или интерактивный скрипт, который делает только то, что должен, и не делает ничего из того, что не входит в его обязанности;

… мертвый сотрудник ☺.

Источник: коллективный разум экспертов «ИКС»

отражено в принятой недавно Концепции информационной безопасности детей). Для тех, кто уже покинул школьную скамью, было бы полезно регулярно публиковать циклы статей в средствах массовой информации или делать специализированные телепередачи аналогично программам о здоровье. ИКС

ракурс



Философия уровня зрелости

Иммунитет к физическим болезням человечество вырабатывало тысячелетиями. Теперь необходимо вырабатывать «информационный иммунитет», считает Павел ГОЛОВЛЕВ, начальник службы информационной безопасности СМП Банка.

Павел ГОЛОВЛЕВ

– Какой должна быть роль высшего руководства организации, служб ИТ, ИБ и HR, рядовых пользователей в борьбе с утечками конфиденциальной информации?

– Все зависит от емкого понятия «уровень зрелости». Как ни прискорбно, но в России основной уровень зрелости – это «жареный петух» или «грянувший гром». Впрочем, и в остальном мире уровень осознания проблем не намного выше, поскольку бизнес – это риск. И любое ограничение риска – это соответствующее ограничение возможностей бизнеса. Но корень проблем даже не в этом. Основным критерием эффективности бизнеса является «time to market» – время вывода продукта на рынок. И если бизнес еще хоть как-то заинтересован (или простимулирован) в охране собственных информационных ресурсов хотя бы на уровне защиты коммерческой тайны, то информационная безопасность выводимых на рынок продуктов – нечто столь же эфемерное, как социальная ответственность бизнеса. И порочный круг замыкается...

– Какие организационные меры обеспечения инфобезопасности компании обычно забывают принять?

– Зачастую не то чтобы забывают, а сознательно игнорируют. Организация Enterprise Management Associates провела исследование по заказу компании Security Mentor, занимающейся вопросами ком-

пьютерной защиты. 56% из более чем 600 опрошенных признались, что, например, тренировки по компьютерной безопасности, предоставленные их нанимателями, не дали никаких результатов. 45% респондентов сообщили, что подобные тренинги проводились всего раз в год. Все организационные мероприятия требуют привлечения и отвлечения человеческих ресурсов и при этом не создают ценности, поэтому для бизнеса они являются чаще всего непрофильными расходами, которые необходимо сокращать, особенно в условиях кризиса. Но, конечно, все опять-таки зависит от уровня зрелости компании.

– Какие технологические решения наиболее эффективны в борьбе с утечками (DLP, IDS/IPS, IDM, комплексные системы управления информационной безопасностью)?

– Все эти решения не работают сами по себе. Их работа должна обеспечиваться наличием необходимого количества людей, обладающих знаниями и умениями как в бизнесе, так и в технологиях. А также постоянными инвестициями в поддержание их функционирования. Да и сами по себе они «удовольствие» очень недешевое. У львиной доли организаций риски значительно ниже, чем стоимость таких решений.

– Как противостоять угрозам информационной безопасности со стороны BYOD?

– В современных условиях – пожалуй, никак. Ящик Пандоры открыт. С этим бороться уже невозможно. С этим надо научиться жить.

– Какие проблемы существующей системы подготовки специалистов по информационной безопасности вы бы отметили? Требуется ли дополнительное обучение?

– Основной минус – однобокость подготовки. Информационная безопасность – это не только и не столько криптография, сетевые технологии, программирование и администрирование информационных систем. Это и юриспруденция, и экономика, и менеджмент, и маркетинг, и психология, и социология..... Поэтому дополнительное обучение, конечно, необходимо. Причем постоянное.

– Считаете ли вы оправданной практику некоторых компаний привлекать к работе молодых талантливых «взломщиков»?

– Все зависит от бизнеса, от решаемых задач, от конкретного человека и его мотивации. В конце концов, игрушки в детстве ломали все. Сейчас игрушки стали другими. Талантливый человек на своем месте может сделать много полезного.

– Как повысить уровень осведомленности населения о способах самообороны от мобильных и онлайн-мошенников?

– Самое слабое место находится в основном в головах. Именно его и ломают в первую очередь. Мы живем во время, девиз которого вынесен на обложку одной из книг гуру маркетинга и веб-дизайна Стивена Круга: «Не заставляйте меня думать!». Иммунитет к физическим болезням человечество вырабатывало тысячелетиями. Теперь необходимо вырабатывать «информационный иммунитет».

– Как сформировать в корпоративной среде культуру информационной безопасности? Нужна ли государственная политика по формированию культуры информационной безопасности в обществе в целом?

– Ответить на эти вопросы можно, только поняв, что может заставить человека защищать чужие секреты сильнее, чем собственные. В современных условиях все рекомендации будут исключительно утопическими. Государственная политика, конечно, нужна. Но это должна быть политика, сравнимая с политикой здравоохранения, которая пронизывает все уровни существования человека в виртуальной среде. От правил элементарной гигиены до медицины катастроф, от центра планирования семьи до хосписа. ИКС

Владимир ПОИХАЛО,
начальник Отдела информационной безопасности, Федеральный фонд обязательного медицинского страхования; канд. техн. наук

Безопасность начинается с головы

Справиться с угрозами информационной безопасности, порождаемыми «фактором Ч», можно только создав комплексную систему, в которой важное место отводится организационным мерам.

«Человеческий фактор» – это действительно слабое звено в информационной безопасности любой компании. Анализируя статистику нарушений инфобезопасности, Gartner заключает, что порядка 60% таких нарушений происходят по вине персонала, причем 80% из них связаны с халатностью, недостаточной компетентностью и безответственностью работников. Аналогичные выводы делает аналитический центр InfoWatch: в 77% случаев основная причина утечек конфиденциальной информации – небрежность и безответственность сотрудников компаний. Работник может забыть ознакомиться с правилами информационной безопасности, недооценить, не понять, превратно истолковать, в силу разных причин игнорировать или даже сознательно нарушать установленные в организации требования. Причем такое поведение может быть обусловлено не тем, что он не хочет овладеть специальными знаниями и навыками, а неумением руководителей и сотрудников – специалистов в области информационной безопасности гра-

мотно донести необходимые сведения до персонала. Приходится признать, что минус существующей системы подготовки специалистов по информационной безопасности – отсутствие адресности: готовить специалистов по ИБ следует целенаправленно для конкретных заказчиков с годовой или полугодовой практикой и ровно столько, сколько возьмут на работу.

Более того, по моему мнению, усложнение информационных технологий и, как следствие, технологий обеспечения ИБ может привести к тому, что затраты на повышение компетентности работников в вопросах инфобезопасности превысят некий разумный уровень и заставят работодателей использовать иные пути ее обеспечения. Такими путями могут стать, например, широкое использование аутсорсинга, страхование рисков и т.п. Следует заметить, до сих пор говорилось только о работниках организации, а ведь еще есть поставщики, клиенты, партнеры, целенаправленные злоумышленники, любопытные студенты и школьники, разного рода «доброжелатели» и прочие категории людей, которые также могут представлять значительную угрозу информационной безопасности.

Вместе с тем надежные комплексные системы инфобезопасности как для известных, так и для перспективных и еще не опробованных информационных технологий конструируют представители другого подмножества того же «человеческого фактора». От уровня их квалификации, интуиции, порядочности, работоспособности и множества иных обстоятельств зависит, будет ли разработанная ими комплексная система информационной безопасности жизнеспособной и надежной. Обеспечить эту надежность должны именно люди – руководители организации. Об этом говорит и национальный стандарт ГОСТ Р ИСО/МЭК 17799-2005, прямо возлагающий ответственность за ИБ на высшее руководство организации (п. 4.1.1), и международный стандарт ISO/IEC 27002:2005, который определяет (п. 6.1.1), что «руководству организации следует активно поддерживать информационную безопасность в организации посредством четких распоряжений, демонстрируемых обязательств, точного назначения и признания обязанностей в области защиты информации».

Для того чтобы реализовать эти функции, топ-менеджменту следует:

- убедиться, что цели в области защиты информации определены, отвечают требованиям законодательства Российской Федерации по вопросам обеспечения инфобезопасности и встроены в значимые бизнес-процессы;
- определить, регулярно пересматривать и утверждать политику информационной безопасности организации;
- предоставить четкие указания и поддержку инициатив в области ИБ;
- выделять необходимые ресурсы;
- утвердить конкретные роли и ответственность за обеспечение информационной безопасности;
- инициировать выполнение планов и программ по поддержанию осведомленности работников в вопросах ИБ;
- убедиться, что механизмы контроля состояния инфобезопасности внедрены и их использование координируется во всей организации. ИКС

Азы круговой обороны

Роль каждого звена в иерархической системе предприятия, от топ-менеджмента до рядовых пользователей, чрезвычайно важна для эффективной борьбы с утечками, поскольку, как известно, рвется там, где тонко. Как обеспечить прочность каждого звена?

Алексей РАЕВСКИЙ,
генеральный директор,
Zecurion

Прежде всего топ-менеджмент, а иногда и владельцы бизнеса обязаны проявить политическую и управленческую волю и принять решение о том, что организация должна защищать данные, выделить на это средства и ресурсы. Без этого соответствующие процессы даже не будут запущены.

Службе информационной безопасности следует определить, какая информация в компании является конфиденциальной и в чем состоят риски инфобезопасности, разработать политику безопасности, концепцию защиты от утечек. В дальнейшем, как правило, именно эта служба обеспечивает выполнение политики информационной безопасности и поддерживает функционирование средств ИБ.

ИТ-департамент отвечает за интеграцию политик и средств инфобезопасности в бизнес-процессы и информационные потоки организации. На этой почве традиционно происходят конфликты ИТ- и ИБ-служб, поскольку для ИТ-департамента любые средства защиты информации усложняют инфраструктуру и затрудняют работу. Часто именно саботирование проектов внедрения средств инфобезопасности со стороны ИТ-отделов ставит на них крест, и чтобы преодолеть это сопротивление, требуется вмешательство топ-менеджмента.

Известно, что существенный процент утечек происходит по вине нелояльных и немотивированных пользователей. Выявление таких сотрудников и повышение их лояльности – задача HR-службы. Кроме того, HR-отделы играют важную роль в обучении пользователей правилам и политикам информационной безопасности, которое проводится, как правило, общими усилиями HR- и ИБ-служб.

Рядовые пользователи – это самое важное звено любой системы безопасности, поскольку именно их дей-

ствия или бездействие обычно приводят к утечкам. Если бы все пользователи все делали в соответствии с правилами и политиками инфобезопасности, никаких утечек не было бы, поэтому задача руководства любой компании – сделать так, чтобы пользователи были бдительны, их действия были осознанными и не нарушали политики информационной безопасности.

Надо признать, часто ИБ-отделы компании неохотно вовлекают персонал в борьбу с утечками. В некоторых компаниях даже могут скрывать от сотрудников наличие DLP-системы и просят вендоров доработать ее функционал таким образом, чтобы она стала еще более незаметной. На мой взгляд, это связано со спецификой оценки эффективности подразделений инфобезопасности в таких организациях. Там, видимо, считается, что служба безопасности хорошо работает, если ловит много инсайдеров. А если всем рассказать, что в компании стоит система, которая за всеми следит, то 99% сотрудников будут воздерживаться от попыток переслать что-либо запрещенное за пределы компании. Таким образом, пойманных нарушителей станет меньше и, следовательно, польза от безопасников окажется как бы тоже невелика. Но такой подход в принципе неправилен и может привести к большим проблемам.

Как известно, ни одна система защиты от утечек не обладает 100%-ной эффективностью, и на 10 обнаруженных попыток слива информации остается одна необнаруженная. В такой ситуации служба безопасности вроде бы отлично работает и ловит много инсайдеров, но утечки все равно случаются. А если сделать сотрудников союзниками ИБ-службы, регулярно рассказывать им про то, как опасны утечки, какую информацию нельзя посылать за пределы компании и что если все-таки кто-то ошибся, то есть специальная система, которая эту ошибку обнаружит и исправит, то они станут чаще задумываться над своими действиями, и число инцидентов снизится. Соответственно, снизится риск утечки и потенциальный ущерб для компании.

К слову, «человеческий фактор» самой службы безопасности во многих организациях нуждается в укреплении. Сегодняшние выпускники могут знать математические основы алгоритмов шифрования и содержание руководящих документов ФСТЭК, однако это никак не поможет им в будущей работе. Когда дело доходит до практических задач, даже базовых, таких, как, например, настройка межсетевого экрана, многие из них оказываются бессильны. Кроме этого, существующие программы обучения не учитывают потребностей современных предприятий, не учат смотреть на проблемы информационной безопасности с точки зрения бизнеса. На наш взгляд, специалистам по инфобезопасности требуется непрерывное дополнительное обучение. Если такой специалист не расширяет постоянно свой кругозор, не следит за развитием технологий, за состоянием отрасли и появлением новых угроз, то ценность его невелика. Для поддержания своей «актуальности» не нужны какие-то спецкурсы, каждый специалист вполне может сам этим заниматься, нужно лишь желание. Дополнительное обучение часто требуется по конкретным продуктам, используемым в организации. Но эта проблема легко решается с помощью курсов и систем сертификации, организованных соответствующими вендорами. ИКС

Образование и культура в минусе
Как перейти в плюс?

Алексей ЛУКАЦКИЙ,
эксперт
по информационной
безопасности, Cisco

Для эффективной работы в сфере инфобезопасности специалисту нужны разнообразные и постоянно обновляемые знания и навыки, а начинать формирование культуры ИБ необходимо буквально с дошкольного возраста.

Специалистов по информационной безопасности у нас в стране готовят в более чем сотне вузов. Их выпускники приобретают солидный багаж ненужных и давно устаревших теоретических знаний, но у них полностью отсутствуют нужные в реальной жизни практические навыки и теоретические знания по психологии, экономике, управлению рисками, социологии и другим дисциплинам, важным для выстраивания эффективного обеспечения ИБ в организации. В результате такие «специалисты» неспособны решать современные задачи обеспечения инфобезопасности предприятия.

О некачественном обучении по данной тематике говорилось неоднократно. Искать причины сейчас бессмысленно – лучше подумать над тем, как ситуацию изменить. Как сделать так, чтобы выпускники вузов получали востребованные на практике знания, а не устаревшие теоретические сведения, которые скорее мешают, чем помогают. Повлиять на Минобрнауки сложно, как и на Минтруда, недавно утвердившее профессиональный стандарт специалиста по информационной безопасности, на который без слез не взглянешь. Но можно попробовать сформировать свое видение тематики, которой должен владеть любой безопасник независимо от того, кем и где он работает. Готовясь стать администратором ИБ, аудитором, руководителем службы ИБ, служащим ФСТЭК, разработчиком средств защиты, сотрудником Центра информационной безопасности ФСБ или Бюро специальных технических мероприятий МВД, выпускник должен иметь общие представления о разных направлениях инфо-

безопасности. Дальше он может либо продолжить обучение по выбранному направлению (если найдет, где), либо заняться самообразованием.

Всю образовательную программу в части спецдисциплин можно разбить на четыре больших блока по образу лукьяненковских «Дозоров»:

1. Светлая сторона – методы защиты информации (собственно то, чем мы и занимаемся).
2. Темная сторона – угрозы, нарушители, их мотивация и бизнес-модели. В виду высокой динамичности предметной области материал по ней должен обновляться ежегодно как для обучения студентов, так и для курсов повышения квалификации.
3. Инквизиция – надзор в области информационной безопасности, правоприменительная практика, криминология и расследование инцидентов, лицензирование деятельности и т.п.
4. Информационные технологии. Инфобезопасность обычно непосредственно связана с ИТ, поэтому необходимо иметь представление как о существующих, так и о перспективных технологиях, которые могут повлиять на ИБ или возникающие риски. Как и в случае с угрозами, данный раздел курса нужно регулярно пересматривать.

По сути, предлагаемый список – это прообраз ФГОС в части спецпредметов (исключая общие дисциплины). Он может быть использован и для менее глобальной и более приземленной задачи повышения квалификации по темам, которые выпали из предыдущего опыта и образования.

С образованием тесно связана культура в области информационной безопасности. Многие службы ИБ сегодня слишком полагаются на технические меры, не желая или не умея работать с людьми, которые и являются самым слабым звеном в системе инфобезопасности любого предприятия. Почему-то считается, что технические меры могут заменить работу с персоналом, что абсолютно неправильно. Причем к работе с персоналом нельзя относить только кнут в виде запрета пользоваться корпоративными средствами вычислительной техники в личных целях или получения всеобъемлющего согласия на чтение всей переписки сотрудника. Нужен и пряник в виде поощрения за безынцидентную работу. А достичь ее можно только внедрением соответствующей культуры ИБ на предприятии. Формирование культуры информационной безопасности – непростой процесс, который занимает несколько лет и включает в себя множество различных направлений, таких, как повышение осведомленности, тренинги, специальные программы стимулирования, незапланированные аудиты и тесты на проникновение, проверяющие способность сотрудников действовать в нештатных ситуациях и т.п.

В прошлом году мне довелось поучаствовать в рабочей группе при Совете Безопасности, занимавшейся выработкой основ государственной политики в области формирования культуры инфобезопасности в России. В нынешнем году, если все сложится удачно, этот документ будет принят, и наше государство сможет начать процесс взращивания культуры в масштабах всей страны. В этой стратегии прописано участие и государства, и общественных организаций, и вузов, и школ, и даже детсадов с собесами, так как пожилые люди и дети дошкольного возраста тоже имеют доступ к компьютерам и тоже должны обладать навыками информационной безопасности. ИКС

гуру

Заметки по практической психологии

Для борьбы с угрозами «человеческого фактора» могут и должны использоваться человеческие же особенности, склонности и опасения.

Дмитрий КОСТРОВ,
вице-председатель подгруппы LSG TEL APEC Азиатско-Тихоокеанского экономического сотрудничества, ассоциированный репортер ИК17 (Безопасность) МСЭ-Т

Люди любят играть

Несколько лет назад в крупной операторской компании мы затеяли акцию веселого обучения сотрудников основам информационной безопасности – провели конкурс инфобезопасного плаката. На удивление, весь коллектив подключился к этой за-

тее с энтузиазмом: сочиняли афоризмы, короткостишия про пароли и логины, рисовали, состязались в остроумии и познаниях этого вроде бы скучного вопроса. Без преувеличения, всем было интересно играть в эту профессиональную игру, а число инцидентов ИБ после нее сократилось.

Культура информационной безопасности напрямую зависит от общей корпоративной культуры. Если люди пришли в компанию с нормальным желанием поработать на себя, на семью и на компанию, если их устраивают условия труда, то с помощью организационно-технических мер поддерживать минимальный уровень угроз инфобезопасности со стороны «человеческого фактора» не составит труда. При этом инструкции и требования должны быть просты и понятны всем, чтобы, например, уборщик понимал: если сильно хлопать дверью в серверную, штекеры могут выпасть из гнезд в серверах и связь прервется.

> Сформировать корпоративную культуру ИБ в отрыве от культуры инфобезопасности в обществе весьма проблематично

Надо признать, сформировать корпоративную культуру ИБ в отрыве от культуры инфобезопасности в обществе весьма проблематично. Во всем мире реализуются специальные программы в этом направлении, причем не только национальные, но и межгосударственные. Так, в APEC страны Азиатско-Тихоокеанского региона запускают специальные программы по повышению осведомленности простых граждан о проблемах и угрозах безопасности в интернете. При этом речь идет не о технологических системах защиты, акцент сделан на «человеческий фактор».

Когда не до игр

К сожалению, времена для инфобезопасности сейчас не самые благоприятные. В условиях сокращения штатов, задержки зарплат, серых схем их выплаты атмосфера в коллективе накаляется, люди нервничают, задумываются об уходе и по-тихому заготавливают себе «парашюты» в виде коммерческой информации, взятой на текущем месте работы. Или, напротив, шантажируют руководство. На моей памяти был случай, когда безопасник крупного банка поставил президенту ультиматум: если его уволят – сольет все данные о ключах для ДБО. Его оставили. А если увольняются программисты? У любого крупного предприятия половина всех систем доработана собственными сотрудниками, причем часто получается, что человек написал программу и уволился, следом пришел другой и тоже написал-уволился, потом третий... Нет никакой уверенности, что никто из них не заложил в систему «логическую бомбу», которая сработает в определенный день и час, предоставив своему автору удаленный доступ к системе расчетов, абонентским счетам или персональным данным. Сегодня одна из самых сложных проблем банков – огромные массивы самописных программ, к которым службы ИТ и ИБ боятся даже подходить: работает и ладно, лучше не трогать. А компании – разработчики центральных систем процессинга или биллинга отказываются от их поддержки, поскольку уже не понимают, что происходит в их недрах за тремя оболочками.

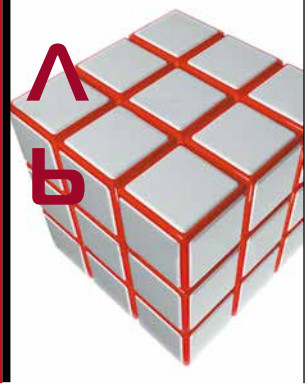
Утечки информации случаются и в госструктурах, куда служащих тщательно отбирают и где проводятся регулярные проверки. Что уж говорить о коммерческих организациях, если привлечь к серьезному наказанию за разглашение коммерческой тайны по нашим законам практически невозможно. Человек может по настроению или в силу обстоятельств нанести крупный ущерб компании – и ничего ему за это не будет. Все постараются сохранить хорошую мину при плохой игре. Более того, в моей практике был случай, когда пойманного на воровстве сотрудника защитил от наказания руководитель компании, заявивший, что этот человек приносит в пять раз больше денег, чем ворует. Если руководство так считает – значит, принимает риски. Но надо хотя бы законодательно обязать компании предавать гласности случаи утечек, как это делается в других странах.

Еще раз о пользе игрушек

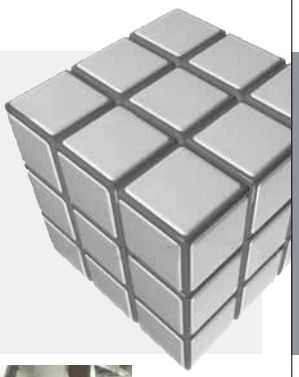
Ни для кого не секрет, что при оценке рисков компании риски информационной безопасности остаются на периферии внимания акционеров или высшего руководства. Очень мало у нас в стране владельцев компаний, которые считают, что надо обеспечивать защиту информации. Недавно с трибуны одной из специализированных конференций топ-менеджер крупной компании заявил: «Ну потеряю планшет – и что? Бывшие сотрудники спецслужб, которые работают в подразделениях инфобезопасности, всех нас просто пугают».

В свое время мне пришлось одному из таких руководителей продемонстрировать, как легко можно управлять его компьютером. Он никак не хотел верить, что это возможно. Надо сказать, в то время многие должностные лица любили играть в «шарики». Пришлось написать программу, красиво «зашить» ее в такую игрушку, сложить специальным файлом и подарить ему. Руководитель запустил программу, и у него стал отниматься экран, мышка, дисководы, вплоть до того, что можно было управлять его «шариками». Нужно положить в ячейку – а он не кладется. Человек был потрясен. После этого в компании появились бюджеты на информационную безопасность. Такой вот «человеческий фактор». ИКС

Модель



«Лучше пять раз объяснить, чем один раз чинить»



Постоянная работа с персоналом по такому принципу позволяет свести к минимуму число неумышленных инцидентов инфобезопасности, уверен Сергей СМОЛИН, руководитель службы ИБ ОАО «Медицина».

Сергей СМОЛИН

– ОАО «Медицина» – первое и пока единственное в России медучреждение, сертифицированное по международному стандарту информационной безопасности ISO/IEC 27001:2005. Чем вызвана необходимость сертификации и что в результате получили врачи и пациенты?

– У нас безбумажная клиника: с 2002 г. истории болезни пациентов ведутся в электронном виде, с 2010 г. обеспечена интернет-доступность электронных историй болезни для экспертов и пациентов, с 2013 г. «Медицина» стала именоваться смарт-клиникой – со смарт-палатами, смарт-операционными. Масштабное использование ИТ в медицинском учреждении требует обеспечения соответствующего уровня информационной безопасности – защиты собственно информационной системы организации от киберугроз и, разумеется, персональных данных пациентов, сотрудников и всей генерируемой в клинике информации – от утечек. Об объемах этой информации можно судить хотя бы по тому факту, что у клиники более 60 тыс. пациентов и только в 2013 г. здесь было оказано 2 млн 300 тыс. услуг (и сделано как минимум столько же записей, хранящихся многие годы).

Поэтому сертификация на соответствие ISO/IEC 27001:2005 была закономерна. В стандарте четко прописаны вопросы работы с персоналом – инструктаж, обучение, проверки. Что мне особенно нравится, стандарт подчеркивает ведущую роль топ-менеджмента. Нам повезло, что президент клиники понимает необходимость обеспечения информационной безопасности, уделяет ей большое внимание. Если мы обнаружили уязвимость – докладываем об этом начальству, и нас не станут упрекать («куда вы раньше смотрели»), а скажут: «Молодцы, что обнаружили. Давайте думать, как это устранить». Со своей стороны, мы приучаем сотрудников не стесняться задавать вопросы. Принцип такой: лучше пять раз объяснить, чем один раз чинить.

– Что представляют собой инструкции и программа обучения персонала?

– Готовясь к сертификации, мы разработали программу обучения с учетом специфики медицинского учреждения. Мы работаем с особой категорией персональных данных – врачебной тайной. В то же время сотрудники – люди, далекие от ИТ. Потребовалось найти золотую середину, чтобы обеспечить и защиту информации, и удобство работы врачам. При приеме на работу человек в течение нескольких дней прослушивает курс лекций, проходит определенную подготовку. Вводная лекция дает всем сотрудникам минимальный набор сведений (это не трогать, это не включать, это выключать, какие кнопки в какой последовательности нажимать).

Программа обучения имеет градации по категориям пользователей. Если сотрудники работают со съемными носителями информации или с ноутбуками, для них отдельный курс обучения, как и для тех, кто работает с электронной подписью. Ежегодно абсолютно все сотрудники, от академиков до уборщиц, проходят инструктаж по информационной безопасности. Причем мы стараемся объяснять, для чего в инструкцию вписан тот или иной пункт. Скажем, в обеденный перерыв доктор решил скачать игру. Объясняем, что у вируса нет обеда, он работает постоянно и именно в играх могут быть вирусы. Простые запреты не работают. А когда наглядно показываем, откуда в компьютере появился вирус, на устранение которого потребовалось два часа, и в это время у доктора не было приема, – всем становится ясно, что инструкцию лучше не нарушать.

Поскольку уровень конфиденциальности у нас высокий, мы придерживаемся принципа минимизации привилегий. Например, личные мобильные устройства использовать для работы у нас запрещено. Есть 28 ноутбуков для бригад скорой помощи и руководства, вход в систему осуществляется только с использованием VPN-клиента. Внешние устройства (те же флеш-

ки) запрещены всем, кроме отдельных сотрудников. Антивирусом Касперского мы просто заблокировали USB-порты на компьютерах. Но если сотруднику необходимо воспользоваться съемным носителем – он обращается в ИТ-службу и под нашим контролем может сделать все, что ему требуется, не нарушая инструкцию.

Любой документ в области инфобезопасности у нас действует в течение года. По прошествии этого срока он обновляется, согласовывается со всеми руководителями подразделений и утверждается президентом. И в течение следующего года мы постоянно контролируем выполнение инструкции.

– Каким образом контролируете?

– Более 90% инцидентов безопасности происходят по вине людей, причем не потому что люди плохи. Никто, приходя в компанию, не собирается шпионить и вредить, все хотят работать и зарабатывать, двигаться по служебной лестнице. Но могут не дочитать инструкцию, что-то забыть сделать и т.д. Приходится работать «цербером». В клинике существует график плановых проверок, утвержденный президентом. Каждое отделение заранее знает, когда его будут проверять, и наводит порядок на рабочих местах. Львиная доля проверок проводится дистанционно, но к каждому рабочему месту я обязательно подхожу хотя бы на две минуты. Во-первых, чтобы люди видели, что «цербер-безопасник» не дремлет. Во-вторых, есть вещи, которые дистанционно не проверишь. Например, любили доктора наклеивать «горчичники» с паролями на обратную сторону клавиатуры или монитора. Когда поняли, что я каждый раз их нахожу, перестали. Если забывают пароль – звонят мне.

Проверки полезны, но их недостаточно. Поэтому мы ежедневно проводим выборочный контроль 20–30 компьютеров из 650 имеющихся в клинике, причем сотрудники знают, что их могут проконтролировать в любой момент. Если обнаруживается инцидент – анализируем ситуацию, устраняем нарушение, виновник несет наказание, и вся история становится достоянием гласности. Президент издает приказ, в котором сообщает: такого-то числа при проведении проверки обнаружилось, что такой-то сотрудник нарушил такой-то пункт инструкции и это привело к такому-то результату. Приказ доводится до всего личного состава клиники. Такой подход дает неплохие результаты. Если в 2012 г. у нас было 12 инцидентов инфобезопасности, связанных с нарушением инструкции, то в 2013 г. – семь. В течение года нам удалось победить неинсталлированные игры, месяцев восемь мы их уже не ловим. Ну а если нарушения инструкции не было, но инцидент произошел – анализируем ситуацию. Смотрим, нужно ли доработать инструкцию или необходимо принимать другие меры.

– Сертификация по стандарту ISO/IEC 27001:2005 позволяет сделать «человеческий фактор» сильным звеном информационной безопасности?

– Скорее, сводит его риски к минимуму. Руководство и персонал понимают, что соблюдение прописанных в стандарте правил поведения приносит реальную пользу. Как минимум помогает избежать расходов. Утечка информации о пациентах нанесла бы клинике огромный репутационный ущерб. Утечка ноу-хау наших врачей, а у нас работают несколько академиков РАМН, разработавших оригинальные методики лечения разных заболеваний, причинила бы ощутимый моральный и материальный урон. Стандарт как раз нацелен на снижение такого рода рисков. На наш взгляд, все стандарты серии 2700 полезны для безопасников, но не все могут позволить себе затраты на сертификацию, начиная с оплаты услуг консалтинговой компании, которая помогает в подготовке к этому процессу. Разумеется, глупо защищаться за миллион, если ущерб не превысит пяти тысяч, но мы посчитали, что затраченные на сертификацию средства – это копейки по сравнению с тем, что мы можем потерять. Конечно, это дорого, но мы спокойны. И наши пациенты спокойны, видя, что клиника работает по европейским стандартам.

– Кстати, пациенты могут записываться на прием к врачу и просматривать свои истории болезни на сайте. Нет опасности утечки их персональных данных?

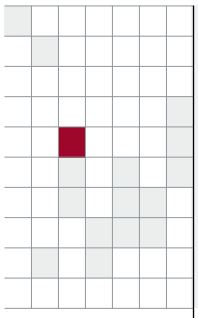
– Сейчас мы заключили договор с крупной аудиторской компанией, которая должна проверить сайт клиники на предмет защищенности, попытаться его взломать, выдать рекомендации и впоследствии осуществлять постоянный мониторинг. А защита персональных данных пациентов и в онлайне, и офлайне – наша прямая задача. Здесь действуют классические методы: кодовое слово, пин-код, обезличенная информация. Мы защищаем даже информацию на установленных в коридорах клиники камерах. Но если пациент передал кодовое слово третьему лицу, кто-то прослушал его телефонный разговор с доктором или вскрыл конверт с отправленной по почте информацией – ответственность за это клиника уже не несет. Мы отвечаем за свой периметр, и здесь у нас все хорошо.

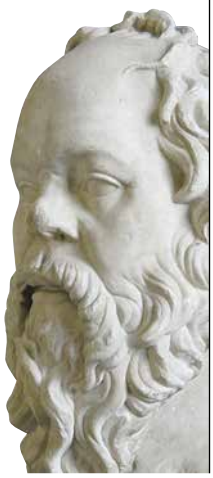
– По данным различных исследований, во всем мире именно медучреждения наравне с госсектором оказываются лидерами по утечкам информации. Неужели вашу клинику эта проблема не затронула?

– В целом у нас все инциденты инфобезопасности носят внутренний характер, утечек не было. Мы этим гордимся. Думаю, это объясняется общим уровнем корпоративной культуры в клинике. Здесь внимательно относятся к подбору сотрудников, созданы хорошие условия работы, зарплаты выше, чем в среднем по Москве. Люди держатся за свое рабочее место. Лично меня, когда я пришел сюда 10 лет назад после службы в ФАПСИ и ФСО, удивил высокий уровень дисциплины. Но и контроль жесткий. В то же время мы понимаем, что если в клинике появится злоумышленник, который захочет украсть конфиденциальную информацию, он может, скажем, сфотографировать на телефон экран компьютера. От таких защититься сложно. Не ставить же видеокамеры в кабинетах, где пациенты раздеваются. В «административный восторг» мы не впадаем. Реально опасаемся в основном вирусных заражений, которые приводят к простою ПК – рабочего инструмента доктора. Поэтому интернет разрешен

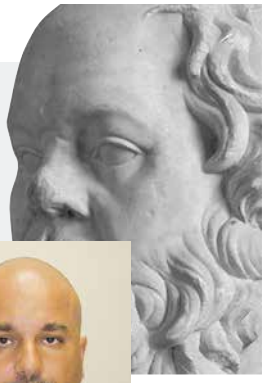
только для использования в бизнес-целях. Доктор должен иметь возможность узнать, какие есть лекарства, просматривать медицинские форумы и проч. На медицинских сайтах вирусов мало, а в интернет-магазинах полно. Когда антивирусная система сообщает, что на таком-то ПК обнаружен вирус, мы тщательно расследуем, на каком ресурсе он был подхвачен. Возможно, это перестраховка, но результаты дает неплохие. ИКС

аналитик





Тратить нельзя экономить



В 2014 г. потери российских компаний, вызванные использованием нелицензионного ПО, составят $20 млрд. Домашние пользователи потратят на обнаружение, определение вредоносного кода и восстановление данных более 1 млрд руб.

Тимур ФАРУКШИН,
директор по консалтингу, IDC Россия

В зоне четырех рисков

Как в мире, так и в России, примерно 30% сотрудников предприятий устанавливают нелицензионное ПО. Однако это значительно снижает уровень безопасности предприятия, повышает его технические, юридические, репутационные и финансовые риски. По данным международного и локального исследований IDC, $127 млрд в мире и $5 млрд в России будут потрачены в 2014 г. на устранение последствий технических рисков (обнаружение проблем и восстановление данных). Самые большие суммы в текущем году компании потеряют в результате утечек информации – $364 млрд в мире и $15 млрд в России.

Несмотря на неутешительные прогнозы, 66% опрошенных ИТ-руководителей российских компаний считают, что, используя нелицензионное ПО, они смогут сэкономить. Однако расчеты показывают, что ущерб от технических сбоев, вызванных использованием пиратского софта, значительно превосходит затраты на легальное ПО. Арифметика простая: российский рынок софта, закупленного в прошлом году официально, составил порядка $5 млрд. При уровне пиратства в 65% около $6–7 млрд «сэкономлено», но в итоге уже в нынешнем году ущерб составит порядка $20 млрд.

Наиболее серьезные опасения у опрошенных ИТ-руководителей российских компаний вызывают юридические риски. 82% участников опроса указали их в качестве наиболее значимых. Такие опасения обоснованы: затраты на выплату административных и уголовных штрафов, а также компенсаций правообладателям в двойном размере от стоимости лицензионного аналога используемого пиратского ПО составляют самую значительную статью расходов компаний.

На втором месте – риски финансовые, вытекающие из рисков юридических и технических. Наиболее значимыми их считают 72% опрошенных. 55% и 49% участников опроса указали в качестве наиболее существенных репутационные (55%) и технические (49%) риски. Несмотря на то, что технические риски беспокоят половину опрошенных ИТ-руководителей, статистика показывает: только 14% предприятий проводят ежедневно аудит компьютерного парка для выявления случаев несанкционированной установки стороннего софта. Это позволяет сотрудникам фактически бесконтрольно устанавливать нелицензионное ПО на рабочие машины.

Еще одна распространенная причина появления вредоносного ПО на офисных ПК – недостаточно ответственный подход к выбору поставщиков оборудования. Так, 52% российских предприятий приобретают компьютеры через каналы, не гарантирующие 100%-ную легальность установленного ПО: компьютерные рынки и магазины. По данным IDC, доля зараженных компьютеров в таких каналах составляет 56% в России и 61% в мире.

Экономия на спичках

Если бизнес при использовании нелицензионного ПО подвергает себя четырем рискам, то главный вопрос «частников» – выгодно или невыгодно. Пиратский софт они также устанавливают на свои компьютеры из желания сэкономить – и основной проблемой для них становится заражение вредоносными программами, на «лечение» которого придется потратить деньги и время (один инцидент информационной безопасности отнимает у пользователя порядка $50 и около 11 часов личного времени). Ежегодно на одного

пользователя приходится в среднем четыре-пять таких инцидентов, и по оценке IDC, в текущем году российские домашние пользователи, применяющие контрафактное ПО, потратят на обнаружение, определение вредоносного кода и восстановление данных более 1 млрд руб. и порядка 80 млн часов.

Как показал опрос, почти 80% респондентов, имеющих проблемы с установленным на их домашних компьютерах ПО, либо скачали его в интернете, либо взяли у знакомых. Самые распространенные проблемы – снижение скорости работы в интернете, замедление работы компьютера, появление всплывающих рекламных объявлений, заражение компьютера вирусом, порча жесткого диска. Многие считают, что, получив софт бесплатно, с этими неудобствами можно мириться, но не задумываются о том, что снижение скорости доступа в интернет или замедление работы компьютера, по сути, свидетельствует о производящихся с ним несанкционированных действиях – либо скачиваются данные, либо компьютер стал частью ботнета и с его использованием осуществляются атаки, распространяется пиратский софт и т.д. Пользователь превращается либо в мишень для злоумышленников, либо в часть системы вредоносного ПО, так или иначе подвергаясь риску.

Создание вредоносного ПО – это бизнес. Две трети потерянных в результате использования пиратского ПО денег приходится на потери по вине злоумышленников. Это огромная индустрия, оборот которой исчисляется сотнями миллиардов долларов в год. На кону большие деньги, поэтому не надо обольщаться, что деятельность злоумышленников вдруг прекратится, и не надо экономить на безопасности. ИКС

ПОДРОБНОСТИ

Как найти то не знаю что

Многие вендоры эксплуатируют существование таргетированных атак как очередную «пугалку». Но на деле эти атаки не так страшны, как их пытаются представить.

Павел ВОЛКОВ,
эксперт по информационной безопасности, «Открытые Технологии»

Эти ужасные, ужасные, ужасные APTs

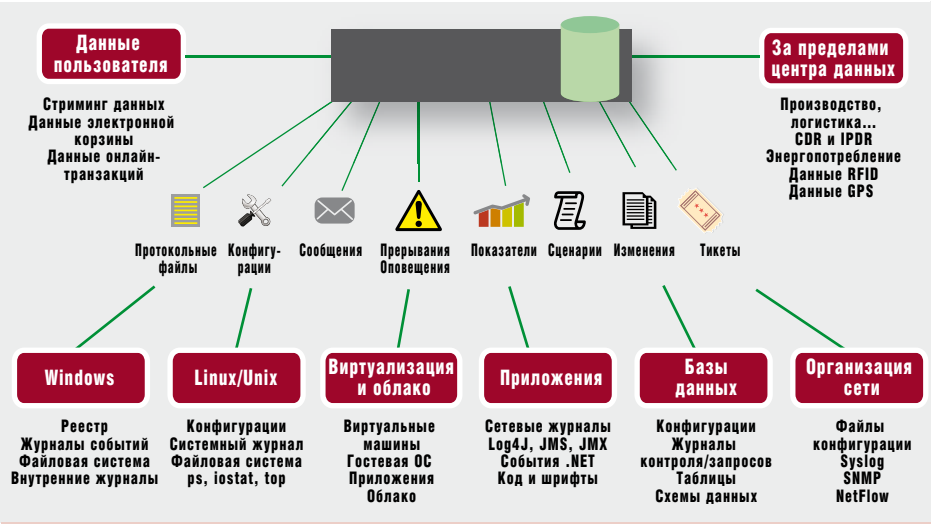
Тема таргетированных атак, или постоянных угроз повышенной сложности (APTs, advanced persistent threats) с недавнего времени стала крайне актуальной. Эти длительные и направленные на конкретную организацию атаки, которые не прекращаются в случае обнаружения более легкой цели или невозможности получить желаемое простыми средствами, используют уязвимости «нулевого дня» и «неведомые» технологии маскировки присутствия агента в атакованной системе. Они играют на естественной склонности людей доверять друг другу и игнорировать требования инструкций по информационной безопасности (что сейчас гордо именуют социальной инженерией). Примеры таких атак – настоящая «мечта параноика» и любителя теории заговоров.

APTs действительно существуют, как бы ни хотелось разговоры о них назвать сказками и маркетингом. И обладают они тремя особенностями. Во-первых, направлены такие атаки на «крупную рыбу» вроде государственных или технологических секретов и, как правило, опираются на существенную финансовую и технологическую поддержку для реализации новых методов осуществления. Во-вторых, они часто эксплуатируют слабости защиты небольших компаний – подрядчиков, партнеров или клиентов больших структур (истинных целей атаки), чем ставят их на грань гибели, вызывая огромные репутационные риски. Наконец, в них максимально используется слабейшее из звеньев современной ИТ-системы – человек. Активное использование методов социальной инженерии делает возможным практически любое начало атаки, и уже невозможно сказать: тут у нас доверенная сеть, а тут – «враг». Кроме того, такие атаки уникальны, т.е. не предполагается, что их сценарий будет повторяться.

По следам их узнаете их

С другой стороны, современная ИТ-инфраструктура практически исключает возможность выполнения операций,

Консолидация массива из ИТ- и ИБ-журналов компании



Источник: Splunk

не оставляющих в ней следов. Сразу оговоримся, речь не идет об инфраструктуре, которая сознательно реализована так, чтобы ничего не регистрировать. В абсолютном большинстве случаев ИТ-инфраструктура компании – источник информации сравнимого, а то и большего объема, чем та полезная информация, которая в ней обрабатывается. Достаточно вспомнить логи – неизбежное зло, которое расходует место, вызывает деградацию производительности и т.п., но абсолютно необходимо, чтобы понять, «где сломалось», и не только.

Эти две стороны одного явления создают интереснейшее противоречие: мы не знаем, как нас будут атаковать, и вроде бы не имеем возможности такую атаку обнаружить. Но мы знаем наверняка, что процесс реализации атаки оставит заметные следы в ИТ-инфраструктуре (правда, непонятно, какие именно). Как такое противоречие разрешить?

Разные производители придерживаются разных мнений о том, что важнее всего в процессе защиты от APTs. Одни утверждают, что нужно защищать рабочие станции; другие рвутся перехватить и анализировать весь корпоративный трафик; третьи называют панацеей от APTs древний как мир скоринг и смакуют подробности влияния конкретного события на «уникальную систему весов для каждого события» и т.п. При этом правда будет пылиться в уже упомянутых логах. Конечно, как любое категорическое высказывание, утверждение, что в журналах регистрации есть всё, не совсем правдива. Там есть почти все, но если в развитой с точки зрения ИТ и информационной безопасности организации собрать логи в единую систему, то там действительно будет ВСЁ.

Как бы ни расхваливали производители свои «глобальные системы мониторинга», уникальные модели оценки и превосходные средства защиты рабочих станций, остается большой и принципиальный вопрос – как атака типа APT может быть обнаружена, если точка вторжения произвольна, как и использованный метод? Этот вопрос достаточно общий, чтобы дать на него три общих ответа: никакие локальные средства не способны в реальной жизни обнаружить новую APT; для увеличения вероятности обнаружения APT требуется как минимум иметь информацию со всех потенциальных точек начала атаки; необходима технология обработки информации, способная учесть тот событийный хаос, который легко создает самый главный и самый ненадежный элемент системы – человек. Увы, традиционные приемы инфобезопасности в части обработки информации не будут достаточно хороши для такой задачи. Они просто не предполагают анализа явлений такой протяженности во времени и малости отличий от нормального поведения. Традиционные системы SIEM (Security Information and Event Management) на практике не способны справиться с такой задачей как с точки зрения объема обрабатываемых «исторических» данных, так и с точки зрения применяемых алгоритмов. Что же можно тут предложить?

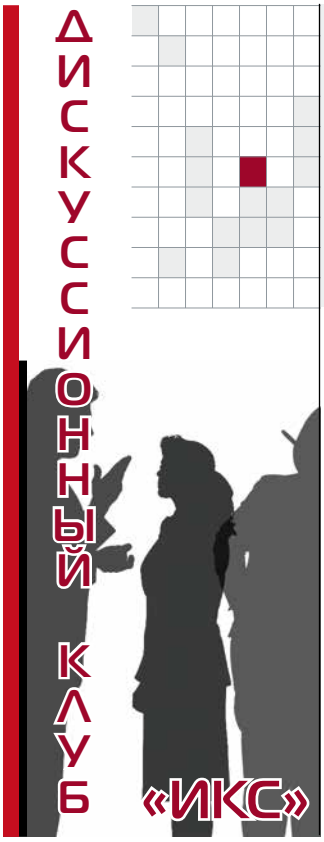
Фабрики поиска

Первая часть задачи имеет довольно хорошо проработанное технологическое решение: собрать и обеспечить возможность обработки в реальном времени всего массива журналов регистрации ИТ-инфраструктуры и средств ИБ могут современные системы из арсенала «больших данных» (см. рисунок). Сегодня это уже решения промышленного уровня, способные обрабатывать десятки терабайт в день.

Что касается алгоритмов обработки, то и тут есть хорошие возможности. Такими обладает, например, новое поколение алгоритмов обнаружения аномалий, использующих адаптивные функции распределения плотности вероятности событий. Ведь именно история потока событий с множества рабочих станций и активного сетевого оборудования, серверов, средств инфобезопасности со всеми периодическими всплесками и провалами образует то, что позволяет увидеть малое воздействие на фоне сильных, но ожидаемых возмущений.

■ ■ ■

Проблема таргетированных атак лежит между зонами ответственности отделов информационной безопасности и ИТ, и ее решение невозможно локальными средствами, так как чаще всего точка начала атаки – человек, пользователь системы. Решение проблемы должно опираться прежде всего на собственные возможности ИТ-инфраструктуры по регистрации активности пользователей и может быть достигнуто только путем объединенной обработки всего массива данных, доступного ИТ- и ИБ-службам. Практически применимые методы решения этой задачи уже существуют. ИКС



Будни «дневных дозорных»

Внешние атаки современных безопасников не пугают, самая большая проблема сегодня – внутренние угрозы. И она, как считают эксперты «ИКС», еще долго не будет решена.

В каменном веке

«ИКС»: Какие организационные меры обеспечения информационной безопасности компании обычно забывают принять?

Андрей ПРОЗОРОВ, ведущий эксперт по информационной безопасности, InfoWatch: Несмотря на то, что организационные меры обычно недороги и достаточно эффективны, их часто недооценивают и не применяют. Вот топ-5 важных мер, которые обычно забывают принять: разработка и утверждение политики допустимого использования ресурсов (электронной почты, интернета, мобильных устройств, ноутбуков и пр.); первичный инструктаж по правилам обработки и защиты информации; повышение осведомленности пользователей по вопросам актуальных угроз и защиты информации; внедрение политики «чистых столов и экранов»; составление детализированного перечня информации ограниченного доступа, обрабатываемой в компании, и правил работы с ней.


А. СКОК

Артур СКОК, ведущий специалист по внедрению систем защиты информации, «СКБ Контур»: Чаще всего слабым звеном в защите оказываются сами сотрудники. В некотором роде идеальным способом защиты является построение системы по принципу «всё, что не разрешено, – запрещено». То есть сотрудник должен иметь доступ только к тем информационным сервисам, которые ему требуются для выполнения должностных функций. Но в реальности это может сильно демотивировать персонал и снизить его производительность.

Александр ХРУСТАЛЕВ, директор департамента информационной безопасности, МГТС: Как правило, забывают именно про обучение персонала азам грамотности по части информационной безопасности. Мало ввести правила и проинформировать о них сотрудника, надо донести до него практическую необходимость соблюдения этих правил для защиты конфиденциальной информации и обозначить его персональную ответственность за их нарушение. В МГТС для сотрудников действуют обучающие курсы по инфобезопасности с последующим тестированием. Это позволило вдвое сократить риски утечек конфиденциальной информации.


А. САНИН

Александр САНИН, коммерческий директор, «Аванпост»: Выстроенную и функционирующую систему периодического обучения персонала и повышения осведомленности в области информационной безопасности я за все время работы в ИБ (это больше 10 лет) встречал не более 10 раз. И в основном это были западные компании, действующие и в России.

Рустэм ХАЙРЕТДИНОВ, исполнительный директор, Appercut Security: По организационным мерам российские компании находятся в «каменном веке», чаще всего единственный «инструктаж» – подписание пары страниц текста при приеме на работу. Поскольку борьбой с утечками занимается служба ИБ, которая не имеет административных ресурсов для воздействия на персонал, исповедуется «технический» подход – установка на компьютеры или шлюзы агентов, собирающих данные о перемещении информации, и их постанализ.

Дмитрий БАРАБАШ, руководитель отдела защиты данных, T-Systems CIS: Сегодня многие российские компании уже используют меры повышения осведомленности персонала. Для тех, кто этого еще не делает, можно предложить градацию по степени доступности: информационные рассылки по почте, публикация тематических новостей на интранет-портале, размещение постеров и памяток в переговорных и около общих принтеров, очные тренинги силами специалистов информационной безопасности. По опыту нашей компании, КПД этих мер достаточно высокий.


Д. БАРАБАШ

Александр БОДРИК, ведущий консультант Центра информационной безопасности, R-Style:

Как правило, основная проблема при обеспечении инфобезопасности в компаниях – недостаточная поддержка со стороны администрации. Это не позволяет реализовать наиболее эффективные меры, такие, как регулярная аттестация и проверка знаний сотрудников по вопросам ИБ, создание горячих линий, интеграция показателей нарушений правил информационной безопасности с финансовой мотивацией сотрудников. Без них классические меры – внедрение режима коммерческой тайны, обучение персонала, интеграция обязанностей по соблюдению правил ИБ в должностные обязанности сотрудников – недостаточно эффективны.


А. БОДРИК

Учиться и учиться

«ИКС»: Какие плюсы и минусы существующей системы подготовки специалистов по информационной безопасности вы бы отметили?


И. КОРЧАГИН

Игорь КОРЧАГИН, руководитель группы обеспечения безопасности информации, ИВК: Один из наиболее заметных и важных минусов существующей системы подготовки в вузах специалистов по инфобезопасности – крен самой программы обучения в теоретические основы и недостаток практических знаний по техническим и организационным методам защиты информации. В особенности это заметно при оценке знаний молодых специалистов по совершенно новым методам защиты информации, а также по актуальным требованиям законодательства в области ИБ.


А. ПРОКУДИН

Аркадий ПРОКУДИН, заместитель руководителя Центра компетенции информационной безопасности, «АйТи»: Обучать работе с конкретными средствами защиты не имеет смысла. Основной плюс российской системы образования безопасников заключается в том, что учат не конкретике, а принципам построения систем. При изменениях в средствах защиты сами принципы не меняются.


А. ПРОЗОРОВ

А. ПРОЗОРОВ: К плюсам можно отнести то, что на рынке услуг обучения инфобезопасности довольно много курсов и учебных центров. Минусов, впрочем, тоже немало. В первую очередь, это качество образования: программы четырех- и шестилетнего высшего образования часто устаревшие и неактуальные, краткосрочные программы обучения также неоптимальны, а цены на них весьма высокие. При этом краткосрочных программ стало слишком много, сложно выбрать действительно стоящие. Уровень подготовки преподавательского состава – еще одно слабое место, поскольку часто преподаватели не имеют практического опыта.

Вячеслав МЕДВЕДЕВ, старший аналитик, DrWeb: Современная система обучения не направлена на формирование эрудированных и мыслящих специалистов. Очевидно, не хватает грамотных преподавателей и курсов, обучающих управлению совместно с бизнесом. Подразумевается, что хороший студент должен работать с третьего курса. Это приводит к непосещению лекций и неполучению возможных знаний. Вместо обучения студенты работают и сдают экзамены. Можно ли назвать специалистом человека, который только сдавал экзамены?


В. МЕДВЕДЕВ

А. БОДРИК: Хорошее фундаментальное образование позволяет профилировать экспертов самых разных специализаций для сферы ИБ, вместе с этим фактическая готовность к работе после окончания вуза составляет порядка 10%. Без дополнительного обучения выпускники могут выполнять только простые рутинные задачи, такие, как обработка заявок на доступ, поддержка простых средств безопасности и выпуск сертификатов.

Сергей ИВАНОВ, руководитель офиса технологии защиты информации, «Первый БИТ»: Широко распространены два подхода к обучению специалистов по инфобезопасности. Первый – подготовка специалистов для работы по стандартам и требованиям ИБ, второй – знание инструментов защиты информации. У флагманов рынка, как производителей средств защиты информации, так и крупных интеграторов, есть авторизованные курсы и учебные центры. Таким образом, на российском рынке обладающий фундаментальными знаниями специалист всегда сможет повысить свою квалификацию. Подход же, сочетающий теорию и практику, вырабатывается «в полях».


С. ИВАНОВ

Р. ХАЙРЕТДИНОВ: Когда речь идет о защите информации от внешних атак, то можно сказать, что современные безопасники готовы к современным вызовам. Методическая и техническая подготовка их в массе своей соответствует задачам, перед ними стоящим. В противодействии же внутренним угрозам ИБ-образование находится только в начале пути – для эффективного решения задач внутренней информа-

ционной безопасности специалистам необходима подготовка в области психологии, юриспруденции, навыки описания бизнес-процессов и многое другое, чему сейчас в вузах на такой специальности не учат.

Темная, светлая где сторона?

«ИКС»: Считаете ли вы оправданной практику некоторых компаний привлекать к работе молодых талантливых «взломщиков»?

А. САНИН: Я к такой практике отношусь сугубо положительно. Есть те, кто защищают, и те, кто нападают. И если первые – это вполне легитимные специалисты, то ко второй категории относят полукриминальных и криминальных личностей (в народе – «хакеров»). Я считаю, что чем раньше «защитники» увидят потенциал и талант в специалисте и раньше переведут его на светлую сторону, тем лучше: одним потенциальным преступником будет меньше. Но я вполне отдаю себе отчет, что темная сторона так же активно пополняет свои ряды такими же талантливыми специалистами. Там и соблазнов больше, и доход порой обещается просто заоблачный. В современной инфобезопасности эти две стороны неразрывно связаны. Отчасти можно даже сказать, что именно проделки хакеров, нашедших, к примеру, критическую уязвимость, зачастую двигают развитие ИБ вперед.

А. ПРОЗОРОВ: С этим надо быть очень аккуратным, я бы не рекомендовал принимать на работу лиц с «подмоченной» репутацией. Особенно, если дело касается информационной безопасности.


Р. ХАЙРЕТДИНОВ

Р. ХАЙРЕТДИНОВ: В крупных компаниях есть свои подразделения внутренних аудиторов инфобезопасности, в задачу которых входят в том числе и тесты на проникновение. По их словам, пользы от «юных дарований» немного. Пентест – методически сложный процесс, и для исследования комплексной системы мало просто уметь «ломать», нужно уметь работать в команде, документировать свою работу и, самое главное, – предлагать решения по закрытию найденной «дыры». В этом юные хакеры ужасно слабы, если не сказать некомпетентны – они могут только писать в твиттере «нашел дыру на сайте – ха-ха-ха». Обычно компании рассматривают их не как пентестеров, а как стажеров, из которых после нескольких лет наставничества может получиться (а может и не получиться – ввиду вспыльчивости, неуживчивости и интровертности) неплохой корпоративный пентестер.


А. ТРОШИН

Александр ТРОШИН, технический директор, «Манго Телеком»: Не скажу, что люди, которые учатся, и талантливо учатся (или только собираются учиться) на факультетах инфобезопасности, не могут в детстве «шалить» и быть «взломщиками». Могут, так как часто это серьезные вызовы, заставляющие работать мозг, искать и находить нетривиальные решения, вырабатывающие привычку не бросать поиск решения на полпути и справляться со сложными задачами. Главное, чтобы все это было в правовом поле и не наносило ущерба компаниям, их репутации и бизнесу. В правовом поле оставаться можно, как минимум, за счет проводимых многими мировыми компаниями конкурсов по взлому их информационных систем и привлечению к работе победителей таких конкурсов. Это больше мировая практика, в России пока отмечены единичные случаи. Но участие российских специалистов в подобных конкурсах – уже система.

BYOD не ждет

«ИКС»: Насколько ощутимы проблемы безопасности в условиях широкого использования личных мобильных устройств на работе и как противостоять угрозам BYOD?

Сергей СЕРЕДА, руководитель проектов, «Энергодата»: Наиболее вероятная проблема – вынос с рабочего места распечатки или флешки с конфиденциальной информацией или ее копирование в облако через сервисы типа Dropbox. Продвинутым пользователям заменой флешки довольно часто служат мобильные телефоны или планшеты при том, что записываемые туда данные никак не защищаются. Противодействовать подобным угрозам можно по крайней мере двумя путями: использовать устройства, поддерживающие многопользовательский режим работы (с несколькими учетными записями и разделением доступа), либо создавать на мобильном устройстве защищенное виртуальное окружение. Второй подход более перспективен, так как требует сертификации средства создания защищенного виртуального окружения, а не устройства в целом. Кроме того, нельзя списывать со счетов и запретительный подход со сдачей на хранение всех мобильных устройств при входе в служебное помещение (возможно, с перенаправлением вызовов через офисную АТС).


С. СЕРЕДА

А. ХРУСТАЛЕВ: В МГТС было принято решение не ограничивать использование мобильных устройств в работе сотрудников, а создать механизм, который позволит повысить эффективность их труда и соблюсти все требования


А. ХРУСТАЛЕВ

политики конфиденциальности. Так, любой сотрудник компании имеет доступ к корпоративной почте через интернет. Как только он подключается к серверу, на его мобильное устройство автоматически загружаются корпоративные политики информационной безопасности (парольная политика, антивирус, контроль приложений, защищенное хранилище и пр.). Конечно, единый подход, который подойдет всем организациям, тут вряд ли возможен, но современные технические средства позволяют найти приемлемое решение для любых сценариев.

А. ПРОЗОРОВ: Основная проблема BYOD – существенное повышение рисков утечки информации. Организации должны ответственно подходить к принятию решения о разрешении/запрете BYOD. Должны быть оценены риски компрометации важной информации. А если все же принимается решение о допустимости BYOD, то необходимо внедрить комплексную систему защиты: начиная с повышения осведомленности пользователей и обучения минимальным правилам инфобезопасности мобильных устройств и заканчивая внедрением специализированных средств обработки и защиты информации на мобильных устройствах.


М. БАШЛЫКОВ

Владимир ВОРОТНИКОВ, руководитель отдела перспективных исследований и проектов, «С-Терра СиЭсПи»: К личным мобильным устройствам следует относиться так же, как и к прочим устройствам сети. Если они получают доступ к корпоративным ресурсам, они должны быть аутентифицированы, их работа должна контролироваться в рамках существующей политики безопасности. Это касается не только очевидных аспектов, вроде списка разрешенных и запрещенных ресурсов, но и менее очевидных – например, наличия актуального антивируса.


В. ВОРОТНИКОВ

Михаил БАШЛЫКОВ, руководитель направления информационной безопасности, КРОК: Число мобильных устройств в корпоративном сегменте растет, сервисами стали пользоваться даже топ-менеджеры при решении своих бизнес-задач. Производители ПО прекрасно видят эту тенденцию и стремятся представить решения, которые эффективно защитили бы от утечек. Например, сейчас востребованы технологии контейнеризации. Они позволяют размещать рабочее приложение (ту же электронную почту) в защищенную ячейку. А использовать приложение можно, только если владелец введет дополнительно пароль.

Культурная эволюция

«ИКС»: Нужна ли государственная политика формирования культуры информационной безопасности в обществе?

А. ПРОЗОРОВ: Скорее нужна, но насколько она будет эффективной? Тут вопрос надо решать на уровне ниже. Например, внедрять в школьную и университетскую программы уроки по «гигиене инфобезопасности», проводить соответствующие курсы на предприятиях. Но не уверен, что тут нужна единая и «утвержденная сверху» программа обучения.


А. РАЗУМОВ

Антон РАЗУМОВ, руководитель группы консультантов по безопасности, Check Point Software Technologies: Разумеется, государство обязано не только регулировать эту отрасль, но и играть важную роль в формировании культуры инфобезопасности в обществе в целом. К сожалению, принимаемые законы свидетельствуют о том, что даже если в процессе их подготовки эксперты привлекались, то их мнение было проигнорировано, а основное регулирование заключается не столько в обеспечении безопасности, сколько в запрете неугодных ресурсов. В частности, дико смотрятся недавние требования к интернет-провайдерам блокировать некоторые страницы пользователей социальных сетей по защищенному протоколу HTTPS (https://facebook.com/<имя> или https://twitter.com/<имя>). Этот протокол специально разрабатывался для того, чтобы было невозможно «подслушать» содержимое, в том числе выделить <имя>.

С. ИВАНОВ: Только осознание личной ответственности каждым участником процесса обработки конфиденциальной информации является надежным средством обеспечения безопасности. Сформировать это осознание поможет выработка прозрачного механизма доказательств вины и адекватной системы наказаний.

Р. ХАЙРЕТДИНОВ: Нужна планомерная работа по формированию правил пользования информационными ресурсами, начиная со школы и продолжающаяся всю жизнь. Так, как это делается с пропагандой гигиены заболеваний: мой руки перед едой, чихай в платок, в эпидемию носи маску, заболел – сходи к врачу и т.д. Правила поведения в корпоративной системе и домашней сети должны внедряться постоянно, примеры пострадавших из-за собственной глупости (попил из лужи – заболел холерой) должны приводиться не только в специализированных, но и в обычных СМИ.

ПОЛНЫЙ ТЕКСТ
Дискуссионного клуба читайте на
www iksmedia.ru

ИТ-активы растут вместе с широким рынком

В конце апреля – начале мая динамика основных биржевых индикаторов, несмотря на значительную коррекцию примерно в середине периода, оставалась весьма позитивной.

Максим КЛЯГИН,
аналитик,
УК «Финам Менеджмент»

На вторую декаду апреля пришелся существенный успех «быков» – позитивные настроения формировались на фоне четырехсторонней встречи в Женеве по урегулированию украинского внутриполитического кризиса. Однако неисполнение декларируемых договоренностей, отсутствие прогресса в деэскалации конфликта на Украине и усугубление кризиса на юго-востоке республики в 20-х числах апреля оказали на российский рынок сильное давление. Максимальное падение было отмечено, когда агентство Standard & Poor's понизило суверенный долгосрочный рейтинг РФ в иностранной валюте с BBB до BBB-, долгосрочный рейтинг в национальной валюте с BBB+ до BBB, а краткосрочный рейтинг в иностранной валюте до A-3.

Впрочем, в дальнейшем, по мере снижения напряженности на Украине и ближе к датам проведения референдумов в Донецкой и Луганской областях, конъюнктура стабилизировалась. Наибольшее повышение российских индексов пришлось на момент заявления президента РФ Владимира Путина об отводе российских вооруженных сил от границ с Украиной и его обращения к сторонникам федерализации с просьбой перенести референдумы.

С опорой на дивиденды

С конца апреля, на фоне снижения политических рисков, российский рынок торговался в уверенном восходящем тренде, а рубль смог заметно укрепиться и достиг локальных максимумов с начала февраля, что говорит о росте спроса на рублевые активы.

Основной вклад в опережающее повышение профильного индекса ТМТ-сектора внесли бумаги МТС. За рассматриваемый период они подорожали на 11% до 266,57 руб. за шт. Поддержку котировкам акций оказывает, в первую очередь, высокая дивидендная доходность – около 7,5% годовых, что в совокупности с высокой устойчивостью и перспективами роста делает МТС одной из наиболее привлекательных дивидендных компаний на рынке: каждый раз при стабилизации внешнего фона мы наблюдаем формирование высокого инвестиционного интереса к ее бумагам.

К позитивным корпоративным новостям, косвенно поддержавшим МТС, можно отнести сообщение об открытии Сбербанком кредитной линии для компании на 20 млрд руб., что может положительно отразиться на долговом профиле. Кроме того, несомненно, в благоприятном ключе можно интерпретировать сообщение о вхождении МТС, совместно с материнской АФК «Системы», в капитал одного из крупнейших российских онлайн-ритейлеров – группы Ozon. Покупка 10,8% миноритарного пакета позволит получить экспертизу быстрорастущего рынка электронной торговли и, возможно, подготовить позиции для динамичного развития в этой индустрии.

Довольно высокие темпы роста продемонстрировали и бумаги «МегаФона». Впрочем, динамика оказалась в рамках рынка – акции подорожали на 4,36%. При этом основным драйвером торгов здесь также выступала привлекательная дивидендная политика компании – совет директоров рекомендовал ГОСА направить на выплату дивидендов по итогам 2013 г. около 39,996 млрд руб. и утвердить дивиденды в размере 64,51 руб. за обыкновенную акцию – и ряд позитивных корпоративных новостей.

В частности, отметим, что в отчетный период дочерняя компания «Скартел» (бренд Yota) заявила о выходе в сегмент мобильной связи: состоялся запуск full MVNO оператора, а сам «МегаФон» сообщил о завершении объединения и интеграции бизнеса «Скартела», что должно положительно отразиться на ключевых показателях уже в среднесрочный период. Кроме того, в конце отчетного периода в рамках квартального пересмотра был повышен до 1,27% вес акций «МегаФона» в индексе MSCI Russia, что в среднесрочной перспективе также будет выступать фактором поддержки.

В свою очередь, акции «Ростелекома» выглядели несколько хуже рынка. Однако падение было умеренным и составило около 1,8%, стоимость снизилась до 79,86 руб. за бумагу. Акции довольно сильно (видимо, играл роль

Справка ИКС

С 15 апреля до 15 мая индекс ММВБ вырос на 5,41% (до 1381,99 п.), а долларовый индекс РТС увеличился на 9,64% (до 1253 п.). Отраслевой индекс «ММВБ телекоммуникации» прибавил 7,44% (до 1931,17 п.).

фактор государственного участия) «проваливались» во время обострения конфликта на юго-востоке Украины и развития политических рисков в конце апреля. И хотя после стабилизации тренд развернулся вместе с рынком, «Ростелеком» все-таки не удержался в «зеленой зоне», несмотря на довольно позитивные в целом корпоративные новости. Так, компания опубликовала неплохую предварительную отчетность по РСБУ за I квартал – выручка выросла на 8%, прибыль – на 45%. Видимо, это найдет свое отражение после публикации данных по стандартам МСФО и поддержит бумаги уже в мае – июне. Одновременно довольно позитивной стала новость о том, что «Ростелеком» прогнозируемо получил 10-летний государственный контракт на общую сумму около 163 млрд руб. для оказания универсальных услуг связи.

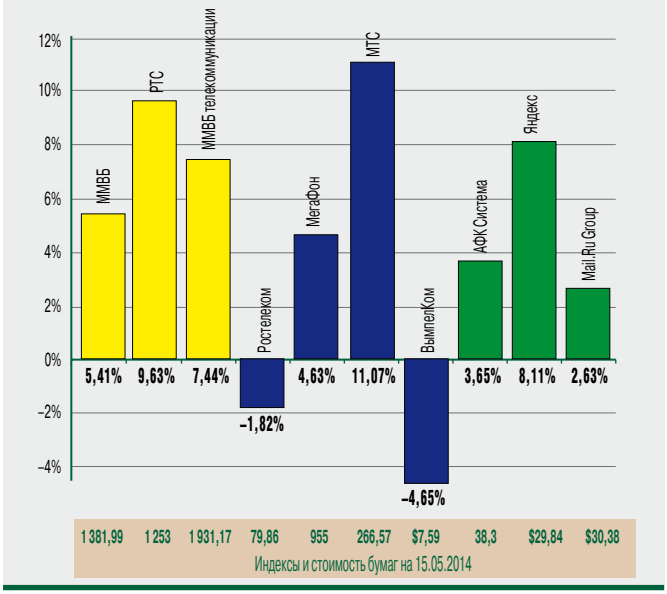
Не удалось избежать коррекции и бумагам «ВымпелКома». Акции компании на NASDAQ подешевели на 4,65% до $7,59. Триггером падения стали планы по сокращению дивидендных выплат с целью снижения долговой нагрузки и, в частности, сообщение о рекомендации совета директоров российского «ВымпелКома» не выплачивать дивиденды по обыкновенным акциям за 2013 г. в пользу материнской компании VimpelCom. Данный фактор, несмотря на частичную компенсацию выпадающих платежей за счет доходов от продажи 51% алжирского оператора Djezzy (стоимость сделки составила более $2,64 млрд), весьма негативно повлиял на денежный поток глобальной компании (в 2012 г. отчисления составили около 36 млрд руб.), что и вызывало отрицательную реакцию рынка. Впрочем, это позволит перенаправить прибыль локального оператора на капитальные инвестиции в России, в том числе – расширить инфраструктурное строительство, что должно повысить конкурентоспособность на рынке и привести к положительным результатам в среднесрочной перспективе. Дополнительным негативом, вероятно, стали слабые результаты по итогам I квартала 2014 г., опубликованные в конце рассматриваемого периода.

Политика отходит на второй план

Акции АФК «Системы» торговались в рамках рыночного тренда, что обеспечило дальнейшее восходящее движение. Несмотря на отдельные коррекции, бумаги компании продолжают расти в цене, постепенно возвращаясь к локальным максимумам января – февраля. Помимо позитивных корпоративных событий, в том числе перспективных сделок M&A, а также сильных результатов компаний, контролируемых группой, интерес к АФК поддерживается лояльной дивидендной политикой – в конце апреля совет директоров рекомендовал общему собранию акционеров утвердить дивиденды за 2013 г. в размере 19,879 млрд руб. (или 2,06 руб. за акцию), что соответствует доходности более 5% годовых.

Умеренно позитивными оказались итоги апреля – мая и для российских интернет-гигантов – «Яндекса» и Mail.Ru Group. В середине периода, на фоне разрастания кризиса на Украине и роста геополитической нестабильности, бумаги этих эмитентов демонстрировали очень сильную просадку. В случае с «Яндексом»,

Изменения биржевых индексов и котировок телеком- и ИТ-компаний с 15.04.2014 по 15.05.2014



упавшим до $24 (ниже цены размещения), видимо, сказалась и полемически заостренная критика компании со стороны президента Путина. Однако после существенного падения, формирования привлекательных уровней и стабилизации общей конъюнктуры, бумаги и «Яндекса», и Mail.Ru быстро восстановились, и по итогам торгов за отчетный период даже вышли в значительный плюс – «Яндекс» прибавил 8%, Mail.Ru – 2,6%.

Одним из драйверов роста стала довольно сильная отчетность обеих компаний. У «Яндекса» положительное впечатление производит, в первую очередь, значительная динамика операционных показателей – выручка поисковика продолжает расти очень высокими темпами. За I квартал консолидированные продажи год к году выросли на 36% до 10,885 млрд руб., что только на 1 п.п. уступает результатам предыдущего периода и выглядит в условиях общего выраженного спада в экономике довольно убедительно.

Основным локомотивом быстрого повышения выручки остаются высокие рекламные доходы, формирующиеся на фоне сильных результатов в контекстном сегменте. Одновременно можно отметить, что диверсификация остается актуальной среднесрочной задачей. Ключевым негативным фактором в отчетности выступает сохранение тренда к замедлению роста рентабельности. Год к году маржинальность бизнеса продолжает расти, но второй квартал подряд серьезно снижается.

Можно отметить, что динамика операционных результатов «Яндекса» и Mail.Ru Group по итогам I квартала 2014 г. сопоставима. Mail.Ru несколько отстает в наращивании продаж (база существенно выше), но в целом темпы роста бизнеса обеих компаний формируются на высоком уровне. При этом в плане диверсификации Mail.Ru Group выглядит интереснее, демонстрируя отличные результаты в очень перспективном сегменте ММО-игр. Кроме того, группа показывает лучшую рентабельность при более значительном масштабе бизнеса, что сейчас, похоже, может быть приоритетом для инвесторов. ИКС

Онлайн-кинотеатры
Взлет на волне спроса

Сегодня телевизионный экран утрачивает монополию на просмотр видео. Рынок предлагает все новые устройства и возможности, стремительно расширяя круг игроков, участвующих в цепочке создания продукта.

Елена КРЫЛОВА,
директор
по проектам,
iKS-Consulting

В числе факторов, влияющих на рост рынка, – техническая эволюция пользовательских устройств и повсеместное распространение широкополосного интернета – как фиксированного, так и мобильного. Все чаще для просмотра видео используются компьютеры и мобильные устройства – планшеты и смартфоны. В среднем один городской житель сегодня владеет 2,4 устройствами, отвечающими этой цели (рис. 1).

Общеизвестно, что старшее поколение больше времени тратит на просмотр телевизора. Однако проведенное iKS-Consulting исследование, охватившее 1006 человек – жителей крупных городов, показало, что по просмотру видео на всех устройствах (суммарно) лидирует молодая аудитория – более того, разрыв между длительностью видеопросмотра самой молодой и самой старшей групп составляет целых 5 часов в неделю(рис. 2).

Зрительские предпочтения

По виду просматриваемого видеоконтента все устройства четко распределились на 3 группы:

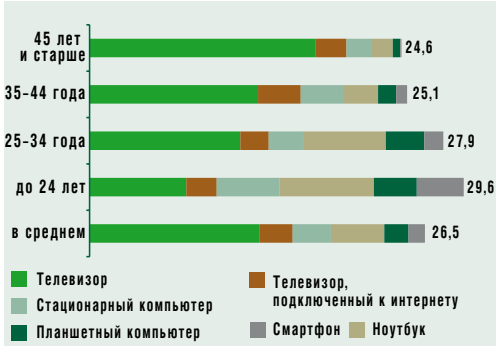
- **телевизоры** (включая смарт-телевизоры), с помощью которых большинство телезрителей смотрят новости и художественные фильмы;
- **компьютеры,** для которых наиболее популярный контент – фильмы; более половины пользователей также просматривают ролики в соцсетях;
- **мобильные устройства,** на которых предпочитают смотреть видеоролики; на втором месте для планшетов с достаточно большим экраном – художественные фильмы, для смартфонов – видеоклипы.

Как видно, наиболее популярным контентом являются фильмы, особенно на устройствах с большим экраном – телевизорах, компьютерах. Телевизор до недавнего времени использовался в основном для просмотра линейного (потокового) телевидения. Однако с появлением новых моделей телевизионных приемников – с USB-портом, с возможностью подключения к интернету (так называемых смарт-телевизоров) – пользователи все чаще стали смотреть на телевизионных экранах видео из сети. Безусловно, это удобно: контент по собственному выбору, в любое время, без рекламы, часто – в HD-качестве, что немаловажно, когда для просмотра используется телевизор с разрешением Ultra HD и с большой диагональю. Именно такие приемники, по мере снижения их стоимости, покупают все чаще.

Рис. 1. Чем пользуются и на чем смотрят видео в России, %

Источник: iKS-Consulting, октябрь 2013

Рис. 2. Длительность просмотра телевизионного и видеоконтента,часы в неделю



Источник: iKS-Consulting, октябрь 2013

Рис. 3. Пользователи приложений Smart TV, домохозяйства

Источник: iKS-Consulting, октябрь 2013

О популярности подобной модели потребления говорят результаты опроса: уже более половины владельцев смарт-телевизоров смотрят на них видео из интернета, а значительная часть (10%) и вовсе отказалась от просмотра линейного телевидения.

Растущий спрос на фильмы и сериалы из сети до недавнего времени почти полностью удовлетворялся пиратскими ресурсами. Однако с развитием операторского VoD* и интернет-сервисов, работающих по технологии OTT**, а также в связи с ужесточением борьбы с пиратами легальный сегмент интернет-видео значительно окреп. Особенно заметный рывок совершили онлайн-кинотеатры – видеоресурсы, предлагающие к просмотру легальный, большей частью профессиональный видеоконтент по запросу (VoD) через интернет по модели OTT.

Платно или бесплатно?

По оценкам iKS-Consulting, рынок онлайн-кинотеатров в 2013 г. вырос более, чем в 2 раза, и составил 1,65 млрд руб.: 1,29 млрд руб. были получены от размещения рекламы, 0,36 млрд руб. – от оплаты видеоконтента пользователями. Несмотря на незначительную (всего 22%) долю в доходах пользовательских платежей, именно этот сегмент сегодня самый быстрорастущий. С чем это связано? Во-первых, выросла готовая платить аудитория смарт-телевизоров – устройств, наиболее подходящих для просмотра фильмов в хорошем качестве. Во-вторых, пользователям был предложен удобный инструмент – встроенные приложения Smart TV. И в-третьих, сказалось то, что наиболее востребованный видеоконтент – новинки кинопроката – предоставляется правообладателями только по платной модели (рис. 3).

Таким образом, предположение, что российские пользователи никогда не станут платить за контент в сети, а развитие легального рынка возможно только по рекламной модели, оказалось несостоятельным. Доказательством жизнеспособности платной модели может служить успех сервиса Play, доходы которого за 2013 г. выросли в 11 раз, а сам он занял второе место в рейтинге онлайн-кинотеатров и стал первым и пока что единственным легальным российским видеоресурсом, прошедшим точку безубыточности бизнеса.

Рост доходов, получаемых игроками по рекламной модели, вызван увеличением аудитории онлайн-кинотеатров (по итогам 2013 г., она составила 24 млн домохозяйств) и, как следствие этого, – растущим интересом рекламодателей к сегменту интернет-видео: рекламодатели стремятся завладеть аудиторией, которая не смотрит телевизор. Весомым для них является и то, что онлайн-видеореклама, в отличие от телевизионной, обладает такими преимуществами, как персонализированный таргетинг, контроль рекламной нагрузки, интерактивность.

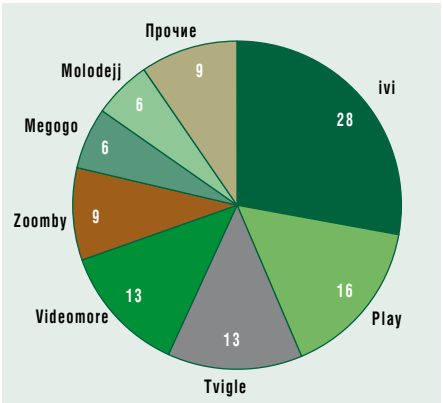
Игроки

Всего на российском рынке OTT-видеосервисов сегодня действуют свыше двух десятков игроков, при этом на семь из них приходится 91% рынка (рис. 4).

Поскольку рынок находится на начальной стадии развития, говорить о наиболее эффективных моделях бизнеса еще рано. Даже все игроки из топ-3 используют разные модели: платную (Play), рекламную (Tvigle) или обе (лидер рынка – ivi).

Контентная политика игроков также существенно различается – это создание широкого и разнообразного каталога (ivi, Megogo), фокус на киноновинках (Play), наличие эксклюзивного ТВ-контента (Zoomby, Videomore). Общей чертой является стремление онлайн-кинотеатров охватить аудиторию всех устройств, присутствуя на максимально возможном числе платформ – телевизорах, компьютерах, мобильных устройствах.

Рис. 4. Рынок онлайн-кинотеатров, %



Источник: iKS-Consulting, октябрь 2013

Пока онлайн-кинотеатры ищут наиболее эффективные модели, пользователи не отдают предпочтение какому-то одному сервису – основная часть аудитории использует несколько видеоресурсов, среди которых, конечно же, не только легальные. Формирование лояльной аудитории – основная задача, которая стоит сегодня перед всеми онлайн-кинотеатрами, и решать эту задачу приходится в очень непростых условиях конкурентной борьбы, выстраивания отношений с правообладателями и рекламодателями, поиска новых технологий оказания услуги. Кто победит – покажет время. Возможно всё. ИКС

* VoD – сервис, предлагаемый операторами платного телевидения.

** OTT – технология, предоставляющая услугу всем интернет-пользователям, независимо от того, к какому оператору ШПД или платного TV они подключены.

Организатор: ИКС МЕДИА

Партнеры: РУССКИЕ БАШНИ, Schneider Electric

При поддержке «Связь–Экспокомм»

Открытое качество

В вопросах контроля качества услуг связи государство и бизнес продолжают противостоять друг другу, однако позиции их постепенно сближаются, показала дискуссия участников организованного журналом «ИКС» круглого стола «Качество на рынке связи. Кому выгодно? От проектирования до сервиса, от эксплуатации до конкуренции».

Реформа у порога

Качество услуг связи – сложная и тонкая материя, которая в последнее время часто рвется, заметила ведущая круглого стола Наталия Кий, главный редактор «ИКС». Во многом это следствие перегрузки сетей с увеличением проникновения мобильного и фиксированного широкополосного доступа. «Сегодня, в период интенсивного развития телекома, вопросы качества – производная не только эксплуатации, как это было в 90-е годы, в пору активного строительства сетей связи, но и бизнеса, конкуренции, экономической эффективности, наконец, – констатировала Н.Кий. – Кроме того, качество услуг обходится операторам все дороже. Какие механизмы следует использовать для укрепления «тонкой материи» – надзор со стороны государства, саморегулирование операторов, новые, публичные рычаги конкуренции?

Н. КИЙ («ИКС»), В. БАРАНЦЕВ (ДИТ Москвы)

Д. НЕЛЮБОВ («Русские Башни»), С. КУНЕГИН (МГТС), Д. ПЕТРОВ («МегаФон»)

Дискуссия о приоритетности механизмов обеспечения качества услуг связи началась в 2012 г., когда Роскомнадзор предложил концепцию системы госконтроля качества оказания услуг связи в РФ. Несколько позже проявили заинтересованность Совет Федерации, общественные и некоммерческие организации, местные власти, наконец, сами операторы. По замечанию Дмитрия Нелюбова, генерального директора компании «Русские Башни», на «политических спонсоров» из Госдумы немалое давление оказывают их избиратели. «Я видел много писем в адрес депутатов с просьбами разобраться с операторами и с министерством по поводу того, что абсолютно нет связи, например, в малых населенных пунктах. На мой взгляд, очень хорошо, что на этот рынок вступило государство», – считает Д. Нелюбов. Тем не менее накал спора между государством и бизнесом о выработке подходов к регулированию качества услуг связи не снижается, поскольку по ряду вопросов позиции его участников принципиально расходятся.

По словам Дениса Пальцина, начальника управления контроля и надзора в сфере связи Роскомнадзора, разработанная по заказу службы концепция контроля качества предполагает комбинированный подход: закрепление на нормативном уровне перечня показателей качества услуг связи и их минимальные значения, оказание услуг связи операторами с соблюдением установленных минимальных значений показателей качества, контроль соблюдения операторами установленных показателей качества по разработанным программам и методикам контроля и предоставление инструментария абонентам для самостоятельного контроля качества. Роскомнадзор планирует контролировать соблюдение именно минимальных значений параметров качества, которые позволят защитить права абонентов. В настоящий момент для 14 услуг связи разработаны программы и методики, которые должны быть включены как приложения в правила оказания услуг связи. «Это даст возможность, не внося изменений в лицензионные условия оказания услуг связи, добиться введения нормативных требований к качеству услуг связи для всех операторов, – считает Д. Пальцин. – Все остальное предлагаем отдать на саморегулирование. При этом принципиально важно, чтобы оценка качества осуществлялась и Роскомнадзором, и саморегулируемой организацией по утвержденным единым методикам, которые не противоречили бы международной практике».

В то же время операторы возражают против избыточного госконтроля и, соответственно, госнаказания. Мониторинга и саморегулирования операторов вполне достаточно для решения проблем качества, считают они. «Сейчас в мобильной связи более 98% абонентов обслуживаются четырьмя крупнейшими, вполне ответственными компаниями, – подчеркнул Юрий Домбровский, президент АРОС. – Они в состоянии и нести ответственность, и контролировать, и быть прозрачными, и пр.». К выработке консолидированной позиции операторы приступили в рамках комиссии РСПП по телекоммуникациям и ИТ. По словам Вячеслава Судьина, ответственного секретаря комиссии, специально созданной для этого рабочей группе поручено проанализировать представленную Роскомнадзором концепцию, разработать свои предложения по регулированию и контролю качества услуг связи.


Д. ПАЛЬЦИН (Роскомнадзор)

Первый этап работы этой группы практически завершен: подготовлено заключение на концепцию. Как сообщил руководитель РГ Василий Левчик, в заключении отмечено, что для предлагаемых мер госрегулирования в концепции не приводится убедительного обоснования; это госрегулирование качества услуг связи предполагает неоправданно жесткое администрирование и дает Роскомнадзору избыточные контрольно-надзорные функции, в то время как в подавляющем большинстве стран используется рыночный метод – мониторинг с опубликованием результатов. По мнению Владимира Вальковича, руководителя департамента технического развития и эксплуатации Orange Business Services в России и СНГ, такой мониторинг должен осуществляться на государственном уровне, независимо от операторов и без применения к операторам санкций более строгих, чем штрафы. «Я считаю, надо давать абоненту выбрать, к кому он пойдет, – отметил эксперт. – Логично публиковать рейтинги по регионам, по технологиям, по операторам. Если мы действительно добьемся равноудаленных и объективных оценок независимого органа, который будет их публиковать, клиент сам сможет решать, переходить или не переходить от оператора к оператору».

Тем не менее система наказаний должна существовать, но не на основе государственного надзора, а в силу правил саморегулирования, считает Александр Вронец, генеральный директор «ПроектСвязьТелекома»: «Члены объединения могут принять внутренний стандарт, которому все обязаны следовать. Ни один государственный карающий орган такой стандарт не создаст, а вот сами компании придумают, примут и будут работать, дабы не было демпинга, дабы оператор не давал на рынок халтуру и не говорил при этом, что он самый быстрый и т.д. Только профессиональное сообщество в виде принятия своего стандарта может закрыть эти вещи, которые вводят в заблуждение и органы управления и контроля, и население».

Итак, реформа контроля качества услуг связи на пороге, и в ее неизбежности никто не сомневается. Другой вопрос, будет она проводиться по административной или по рыночной модели. По мнению Олега Скокова, директора по развитию и ИТ ЦНИИС, обе модели должны не отрицать, а дополнять друг друга, действуя как в государственных, так и в рыночных интересах.


В. ЛЕВЧИК (АРОС), А. ВРОНЕЦ («Проектсвязьтелеком»), К. ЮЛДАШЕВА («АКАДО Телеком»)

В. ВАЛЬКОВИЧ (Orange Business Services), С. ФОМИЧЕВ («Мастертел»), А. ПОДРЯБИННИКОВ И Д. НЕЛЮБОВ («Русские Башни»)

При этом должны быть выработаны единые параметры и показатели качества, единые методики измерений, единые механизмы измерения качества и единая централизованная структура контроля качества, целью деятельности которой является формирование публичных рейтингов для сравнения операторов связи. «Надо сразу сказать, что методики не могут быть определены раз и навсегда, – подчеркнул О. Скоков. – Формирование методик измерений – это творческий процесс. Должны измеряться не только технические показатели, но и процессные – время, затраченное на обработку заявок, ошибки биллинга и т.п. Одним из показателей качества работы операторов подвижной связи может быть количество перенесенных номеров. ЦНИИС, обеспечивающий в настоящее время процесс переноса номеров, предлагает себя как центр контроля качества».

О. СКОКОВ (ЦНИИС)

Представляется, что процесс будет непростым и перманентным и в нем свою роль смогут сыграть и регулятор, и научные организации, и бизнес, и местные власти. К слову, положительный опыт такой консолидации усилий уже есть.

Проверка на качество

В 2013 г. Роскомнадзор совместно с Департаментом информационных технологий Москвы и операторами большой тройки начал практическую отработку программ и методик оценки качества услуг сотовой связи на пилотном проекте в Северном административном округе столицы. К этому проекту ДИТ Москвы пришел уже подготовленным. Как сообщил Виктор Баранцев, руководитель направления по работе с сотовыми операторами ДИТ Москвы, к этому времени были разработаны методики измерений применительно к условиям мегаполиса, которые прошли общественную экспертизу, согласованы с операторами и переданы в Роскомнадзор.

С запуском проекта проспекты, улицы и проезды округа «патрулировали» мобильные измерительные комплексы, проверяя качество сотовой связи на сети каждого из операторов. Первые замеры показали, в каких местах показатели качества ниже минимальных значений, установленных на договорной основе, где необходимо установить новые базовые станции. ДИТ Москвы помог операторам в вопросах размещения БС на жилых и административных зданиях, Роскомнадзор – в части упрощения порядка регистрации станций (сроки выдачи разрешений сократились с полугода до месяца). Как показали контрольные измерения, пилотный проект дал положительный результат. В 2014 г. проект масштабируется на территорию всей Москвы. «В полномочиях субъекта РФ упростить порядок размещения радиоэлектронных средств операторов на объектах городской собственности. При этом в Москве расположено много федеральных объектов, – отметил В. Баранцев. – Сейчас задача обеспечить благоприятные условия для работы операторов и на них. В этом вопросе мы надеемся на поддержку Правительства Российской Федерации».

К концу года аналогичные проекты планируется начать в Санкт-Петербурге, Краснодаре, Казани, Новосибирске, Хабаровске и Екатеринбурге. Со стороны Роскомнадзора для перенесения опыта столичного проекта на другие города потребуется, по словам Д. Пальцина, создание автоматизированной системы контроля качества услуг подвижной радиотелефонной связи, которая будет состоять из мониторинговой системы и системы измерения параметров качества. Она позволит проводить автоматизированные измерения, автоматическую программную обработку, расчет на программном уровне показателей голосовых сервисов и передачи сообщений, тестирование качества передачи данных и речи для всех стандартов сотовой связи. Результаты измерений будут доступны в том числе на портале Роскомнадзора. «На основании измерений будут формироваться рейтинги, выдаваться рекомендации операторам связи. Совместно с операторами

И. ДЕГТЯРЕВ (Schneider Electric), Ю. ДОМБРОВСКИЙ (АРОС), С. АРХИПОВ (GISware Integro)

будем прорабатывать вопросы улучшения качества, как мы делали в пилотной зоне в Москве, – сообщил Д. Пальцин. – В дальнейшем, когда у нас появится нормативная правовая база, будем уже, может быть, и штрафовать».

К триединству измерений

Безусловный плюс предлагаемой Роскомнадзором концепции – инициатива создания единой системы измерений по единым методикам и их публичная доступность. В идеале – без разночтений в оценке качества государством, оператором и абонентом. Как отметил Дмитрий Петров, руководитель по взаимодействию с законодательной и исполнительной властью «МегаФона», компания инвестирует десятки и сотни миллионов долларов в сеть – и заинтересована в том, чтобы существовали измеримые параметры качества услуг на этой сети, чтобы качеству была проставлена соответствующая оценка. «Невозможно улучшить то, что нельзя измерить, – констатировал Д. Петров. – Поэтому нам нужно создать понятные измерители. Но в российском законодательстве вообще нет понятия «качество», и создать механизм регулирования в отдельно взятой отрасли – задача не из простых. Мы приветствуем усилия Роскомнадзора, мы хотим измерять качество и на его основе конкурировать. Конкуренция по качеству на сегодняшний день становится более приоритетной, чем конкуренция по цене. Но необходимо выработать определенные подходы к измерениям». По мнению Д. Петрова, установить параметры качества и жестко их контролировать имеет смысл для государственных услуг в социально важных сферах (например, время доставки SMS «Скорой помощи») и услуг, связанных с обороной страны и безопасностью государства, а все остальные вопросы передать операторам на саморегулирование. «Сейчас усилия операторов в первую очередь нужно направить в сторону саморегулирования, – считает Д. Петров. – Нам следует попытаться измерить по методике Роскомнадзора качество своих услуг и выставить по всей стране оценку этому качеству».

Б. ЛАСТОВИЧ (МАС), В. СУДЬИН (Комиссия РСПП по телекоммуникациям и ИТ)

По словам Сергея Архипова, заместителя директора по научно-техническому развитию GISware Integro, сегодня каждый оператор оценивает качество предоставляемых услуг связи с помощью измерений параметров работы сети и для этого имеет в своем распоряжении более тысячи индикаторов, выражаемых разными формулами. Большинство операторов, руководствуясь международными стандартами и рекомендациями производителей оборудования, для оценки качества работы сети используют практически одни и те же индикаторы, однако вычисляют их различно, даже на уровне подразделений. «Для объективного независимого мониторинга качества услуг нужны однозначно трактуемые показатели и хорошо проработанная методика их измерения и вычисления, доступная и контролирующим органам, и самим операторам, – отметил С. Архипов. – Сейчас вопрос лишь в том, чтобы собрать представителей отрасли связи и государства и выработать недостающую методику с должным уровнем детализации. Этот вопрос обсуждается не первый год, но, к сожалению, складывается впечатление, что не хватает воли или некоего инициатора, который смог бы собрать все эти предложения и в конечном счете подготовить такой документ».

В концепции Роскомнадзора предусматривается самостоятельный контроль качества абонентом, однако в московском пилотном проекте этот этап оказался обойденным. По словам Д. Пальцина, связано это с тем, что остался открытым вопрос оплаты трафика измерений. Между тем инструментарий такого контроля операторы уже активно осваивают. Как сообщил Юрий Ли, руководитель службы качества услуг пакетной передачи данных «ВымпелКома», компания сконцентрировалась на развертывании так называемого активного режима мониторинга качества, когда используются стандартные мобильные терминалы, на них устанавливается приложение, которое с определенной периодичностью проводит тестирование скорости, доступности, непрерывности и прочих показателей качества. «Наш опыт свидетельствует, что сравнительно небольшим количеством устройств можно обеспечить достаточно неплохое покрытие территории мониторинга, получить представление не только об общем состоянии сети, но, самое главное, о качестве сервиса в точке потребления услуги, – отметил Ю. Ли. – В проекте участвуют сотрудники компании, поэтому его география определяется географией их перемещений, однако мы планируем запуск проекта и для клиентов. При этом непосредственно за трафик измерений абонент платить не будет».

Ю. РОКОТЯН («ВымпелКом»), К. ПИШАЛЬНИКОВ («ЭР-Телеком»)

Как и ожидалось, полученные в рамках проекта результаты зависели от модели устройства, что объясняется аппаратными и программными ограничениями на уровне операционной системы. По словам Ю. Ли, при выборе устройства абонент зачастую руководствуется не его характеристиками с точки зрения качества радиопередающих трактов, а дизайном, операционной системой, популярностью той или иной марки, что отнюдь не свидетельствует о качестве самого устройства. К тому же нередко производители устройств больше заботятся о скорости выпуска продукта на рынок, чем о его качестве, – и в одиночку бороться с этой проблемой на глобальном уровне оператор не может, признает эксперт. Тем не менее именно распределенные измерители качества могут стать хорошим подспорьем в инициативах по измерению качества, по его саморегулированию на основе публикации результатов в открытых источниках, считает Ю. Ли.


Ю. ЛИ («ВымпелКом»)

Кто на новенького?

Дискуссии о качестве услуг в последние два года ведутся в основном вокруг голосовой мобильной связи и мобильного доступа в интернет. Соответствующие методики разработаны и для фиксированного ШПД и фиксированной телефонии. По словам Д. Пальцина, для измерений показателей на сетях фиксированной связи Роскомнадзору необходимо наладить взаимодействие с операторами этих сетей. «Если с мобильными операторами всё понятно – мы без взаимодействия поехали и померили, то здесь речь уже идет о размещении нашего измерительного оборудования на фиксированных сетях передачи данных», – пояснил Д. Пальцин. На это О. Скоков заметил, что уже разработанные методики для ШПД предусматривают механизмы и принципы измерений.

Между тем эта задача отчасти решается местными властями, указал В. Баранцев. Сам город, по его словам, является крупнейшим потребителем услуг связи, закупая их для школ, поликлиник, различных социальных служб – всего более 15 тыс. городских объектов, а также для эксплуатации отдельных крупных систем, как, например, городской системы видеонаблюдения. Это требует постоянной оценки качества услуг, поэтому ДИТ Москвы по своей инициативе наладил мониторинг качества каждого отдельного пакета услуг, в том числе изображений, поступающих с 145 тыс. камер видеонаблюдения, включив контроль за исполнением требований в госконтракты. И за их невыполнение операторам грозят штрафные санкции.

В свою очередь, операторов подталкивает к заботе о качестве конкуренция. Как подчеркнул Сергей Кунегин, начальник отдела управления качеством МГТС, именно под давлением конкуренции в области ШПД компания некоторое время назад приступила к модернизации сетей абонентского доступа по технологии GPON – по сути переводу всех квартир Москвы на оптические абонентские линии. Цель проекта – обеспечение клиентам качественной услуги широкополосного доступа. По словам Кирилла Пищальникова, директора по управлению сетью «ЭР-Телекома» (бренды «Дом.ru» и «Дом.ru Бизнес»), для оператора качество – элемент конкурентной борьбы, особенно на локальных рынках с сильными игроками (Новосибирск, Челябинск). Система оценки качества в компании основана на инструментальном контроле (полевые измерения, мониторинг) и регулярных (раз в полгода) опросах клиентов, где большой блок отведен качеству.


А. ТРОШИН («Манго Телеком»), Б. ЛАСТОВИЧ (МАС), В. СУДЬИН (Комиссия РСПП по телекоммуникациям и ИТ)

Очевидно, тема качества услуг связи не будет исчерпана и с введением госконтроля, если таковое произойдет, и с появлением единой для операторов системы мониторинга показателей, и с переходом абонентов на самоконтроль. «Проблему качества и их регулирования можно считать только открытой, поскольку, с одной стороны, нет предела совершенству, с другой – и операторы, и регулятор, и потребитель всегда в пути, – резюмировала Н. Кий. – При этом нужно стремиться к тому, чтобы качество было выгодно и приемлемо по затратам для всех участников рынка: и для регуляторов, и для бизнеса, и для потребителей. Тем более если учесть, что связь если не де-юре, то де-факто переходит в состав социально значимых услуг».

Лилия ПАВЛОВА

Пазл качества
в сетях нового поколения

Обеспечение качества телекоммуникационных услуг – задача многокомпонентная, которая обрастает дополнительными аспектами с переходом к новым сетям, объединенным общим брендом «интернет». Отправной точкой решения этой задачи может стать введение мониторинга качества предоставления услуг связи.

Борис ЛАСТОВИЧ,
эксперт Международной академии связи

Новые сети

Проблема качества предоставления потребителям услуг электросвязи и контент-сервисов сегодня одна из самых заметных на телекоммуникационном поле. Причин тому несколько. Первой я бы назвал беспрецедентные преобразования, новые тенденции как в мировом, так и в отечественном телекоме.

Давно ли мы были озабочены очередями на установку телефона и цифровизацией коммутаторов на сетях TDM? А сегодня на 100 жителей страны приходится 180 договоров на мобильную связь, причем пользователь имеет возможность получения услуг, и не только телефонии, у любого оператора, в любом месте планеты. Возросшие риски невыполнения нормативов, проблемы контроля качества связаны теперь не только с количественными изменениями, но и с изменением характера услуг. Так, владелец смартфона уже не может безоговорочно считаться абонентом своего оператора, а его терминал входить в состав сети, как это предусматривают рекомендации МСЭ-Т E.800, определяющие само понятие качества обслуживания в электросвязи.

Главная тенденция электросвязи на современном этапе уже не в технологическом и количественном развитии, а в переходе от отдельных для каждой услуги сетей к единой коммуникационной инфраструктуре, базирующейся на IP-протоколе, на основе которой предоставляются все услуги (и не только связи). Место голосовой телефонии как основной услуги электросвязи во всем мире уверенно занимает универсальный широкополосный доступ к глобальной информационной экосистеме (определение МСЭ).

При этом приходится учитывать, что к разным типам услуг (например, телефонии, мультимедиа, веб-услугам) предъявляются разные требования, которые уже не могут быть удовлетворены прежними способами. Необходимы специальные сетевые и организационные решения, новые подходы к обеспечению и контролю показателей качества предоставления разных услуг разным потребителям на одной сети.

Еще одна связанная с новыми тенденциями проблема заключается в том, что по традиции ответственность за качество делится между операторами в цепочке предоставления услуги. Но сети связи нового поколения – это сети с пакетной коммутацией (ШПД, Softswitch, IMS), работающие на IP-протоколах и имеющие «плоскую» архитектуру и самоорганизующееся программное управление. В таких сетях параметры качества привычными методами не локализуются, и непонятно, кто и в какой мере должен нести ответственность за их отклонение от нормативных значений. Дополнительную остроту проблеме придает быстрый рост мобильных широкополосных соединений, которые могут включать гибридные соединения с традиционными сетями и терминалами и значительное число транзитных узлов. Это отрицательно сказывается на качестве обслуживания и еще более размывает ответственность операторов.

К тому же в новой инфокоммуникационной среде конечной услугой, как правило, является не услуга связи, а разного рода приложения, контент, часто переданный в сеть сторонними провайдерами и реализуемый в виде услуги опять же за пределами сети, на терминалах, параметры которых оператору неизвестны. В таких условиях телекомоператоры не могут полностью управлять качеством того, что предоставляется потребителю.

Хотим мы это признавать или нет, но сети последующих поколений – назовем их для краткости и по смыслу новыми – давно стали нашей реальностью,

быстро эволюционируют и приобрели широкую известность под общим брендом «интернет».

Наличие универсального доступа к Сети во все большей степени определяет качество жизни населения, эффективность экономики и государственного управления, возможности реализации других преимуществ информационного общества. В России, по оценке аналитиков, в конце 2013 г. насчитывалось около 70 млн активных пользователей интернета. У нас самая большая интернет-аудитория в Европе, уже вдвое превышающая постоянно уменьшающееся количество абонентов ГТС/СТС. Среди активных интернет-пользователей почти 100% государственных организаций, включая органы власти и управления, около 98% бизнес-структур, а также школы, высшие учебные заведения, общественные структуры и т.д.

Помимо возможности посещения зоны .ru и всего глобального интернета, новые сети обеспечивают получение госуслуг и применение информационных технологий, в том числе в системах управления государством и сложных интеллектуальных технологических системах, работу платежных и иных банковских систем, использование облачных сервисов, автомобильных навигаторов, скайпа и многих других сервисов и приложений. Трудно также не заметить многомиллионные аудитории электронных СМИ, интернет-телевидения и социальных сетей.

Следующим этапом стало строительство в крупных городах частных сетей нового поколения на новых технологиях, таких, как «волокно в квартиру» или 4G, рассчитанных на предоставление универсального доступа миллионам пользователей. Их уже и к интернету не отнесешь.

И все это – при отсутствии внятной политики развития в рамках (или за рамками?) давно устаревшей системы регулирования.

Отставание госрегулирования

Второй причиной актуальности проблемы качества я бы назвал отставание в государственном регулировании сферы цифровых коммуникаций.

Действующая модель развития и управления, нормативная правовая база, в том числе закон «О связи», иные механизмы госрегулирования все еще ориентированы на традиционные сети, прежде всего на телефонную сеть общего пользования.

А сети связи нового поколения, реально работающие на государство, новую экономику, оказывающие услуги как минимум половине жителей страны, существуют как бы сами по себе, отдельно и независимо от традиционных сетей. Главным, если не единственным регулятором и стимулом развития для них остается рынок, коммерческие интересы владельцев. Бурное развитие интернета в нашей стране в 90-е и 2000-е годы, безусловно, обязано рынку, отсутствию административных сдержек. Но такое развитие имеет очевидный предел: ШПД распространяется и совершенствуется в основном в крупных городах. Судя по международным рейтингам, в России этот предел уже достигнут. Как и предел в регулировании: известные читателям журнала попытки изменить ситуацию путем традиционного администрирования, навязывания операторам невыгодных лицензионных условий сегодня представляются непродуктивными.

Я не разделяю мнения, что в борьбе за клиента бизнес сам устанавливает жесткие внутренние стандарты качества предоставляемых сервисов. Да, такое может быть, но только в условиях продуманного регулирования рынка и далеко не везде. На свободном рынке – равные для всех участников условия конкуренции, а уж тем более стимулы развития в интересах государства и социума сами сформироваться не могут.

Так что уровень качества обслуживания потребителей в телекоммуникациях должен определятся и поддерживаться прямыми или косвенными механизмами государственного регулирования. Это в полной мере относится и к техническому регулированию, обеспечивающему качество работы каждой сети в отдельности и сети страны в целом.

Но особого прогресса в этом направлении пока не просматривается.

Иллюстрацией могут послужить представленные в прошлом году Минкомсвязью России на общественное обсуждение предложения по созданию еще одного вида сетей общегосударственного масштаба – «мультисервисных». Предложения, фактически исключающие конкуренцию, не учитывающие наличие и массовое использование в стране именно мультисервисных по функционалу интернет-сетей. Но, главное, в очередной раз игнорирующие необходимость выработки основополагающих, стратегических принципов построения функционально единой, современной национальной сети связи Российской Федерации. С учетом которых только и можно что-либо предлагать в этой сфере.

Относительно качества эти принципы (которых нет) должны бы еще вчера определить обязательные для всех операторов нормативы и сетевые решения, гарантирующие, в частности, связность, устойчивость и качество работы функционально единой современной сети связи страны. Но при отсутствии исходных принципов невозможно оценить даже работоспособность предлагаемых решений.

Для действующих операторов такая неопределенность в регулировании влечет за собой риски для бизнеса, связанные с вероятностью спонтанных решений регулирующих и директивных органов. И примеров тому достаточно.

Цунами трафика

Наверное, самой насущной причиной повышения внимания к качеству обслуживания в электросвязи, касающейся каждого потребителя, является наблюдаемый сегодня резкий, взрывной рост трафика в сетях в результате неограниченного доступа, быстрого роста числа загрузок сервисов и приложений, особенно мультимедиа, в мобильных сетях. Растут риски их перегрузки, снижается качество предоставления услуг.

Сохранение качества хотя бы на прежнем уровне требует соответствующего росту трафика увеличения пропускной способности опорных, соединительных, магистральных линий, т.е. постоянного наращивания инвестиций телеком-операторов в развитие своей сетевой инфраструктуры. Однако эти инвестиции операторам не выгодны, так как повышая издержки, не приводят к адекватному росту доходов. Проблема усугубляется отсутствием в России развитой линейно-кабельной инфраструктуры, а также тем общепризнанным фактом, что в сложившихся условиях операторы уже не могут развивать свои транспортные сети только за счет собственных ресурсов.

Решения находятся в области совершенствования регулирования. Исходя из принципа сохранения открытости сетей, можно, к примеру, ввести механизмы перераспределения доходов контент-провайдеров, прежде всего OTT, учитывающие необходимость инвестиций в увеличение пропускной способности сетей. Или – следовать принципу ограниченного доступа, снижающего качество обслуживания для определенных категорий поставщиков контента и пользователей. Для этого потребуется установление еще одного принципа построения национальной сети – регулирования трафика с применением специальных общесетевых организационных, аппаратных и программных решений.

Как видим, и в этом случае регулятору необходимо прежде всего определиться с взаимоувязанными концептуальными принципами построения функционально единой национальной сети. Если же оставить все, как есть, то уже в ближайшие год-два можно ожидать коллапса сетей в виду быстрого роста количества смартфонов и планшетных компьютеров у населения, увеличения числа загрузок и онлайн-использования фильмов, сложных игр, карт и т.п.

Кстати, по данным МСЭ, доля трафика от голосовой телефонии в целом по сетям составляла на начало текущего года около 10%, а в сетях 3G – 1% и менее. Опубликованные в 2013 г. данные некоторых наших сотовых операторов подтверждают эти цифры и тенденции. Аналитики предсказывают в ближайшие годы переход голосовой телефонии (и видео) в число сервисов универсального доступа. Такое решение представляется особенно привлекательным для операторов строящихся новых сетей, таких, как фиксированные GPON или сотовые LTE.

Ослабление внимания к эксплуатации

Еще одна причина повышенного внимания к качеству – это отмечаемое многими специалистами снижение уровня эксплуатации сетей и обслуживания потребителей. Так, в системе «Ростелекома» уже проведено с десяток «оптимизаций» персонала. С этого начинает каждый новый руководитель, причем под увольнение все чаще попадают те, от кого напрямую зависит качество обслуживания потребителей: монтеры, кабельщики, среднее звено управления – организаторы эксплуатации. Однако о каких-либо организационных мероприятиях, которые позволили бы, соответственно, в разы поднять производительность труда оставшихся работников, говорить можно только гипотетически. Да и вряд ли это возможно в принципе.

Наши ведущие сотовые операторы, владельцы и топ-менеджеры которых заинтересованы прежде всего в сохранении рыночной капитализации своих компаний, стремясь сократить издержки в условиях стабили-

QoS и QoE. Границы отношений

В действующем Регламенте международной электросвязи (РМЭ) 1988 г. качество обслуживания рассматривается как *совокупный показатель характеристик услуги, определяющий степень удовлетворенности потребителя* (QoS). Это определение приведено в Рекомендациях МСЭ-Т E.800 и соответствует действующему стандарту ИСО-9000, являясь, на мой взгляд, главным критерием качества для любого вида обслуживания.

Эта концепция качества обслуживания является составной частью РМЭ и предусматривает, что национальные администрации связи должны «обеспечивать сотрудничество по созданию, эксплуатации и техническому содержанию сетей для достижения удовлетворительного качества обслуживания потребителей».

С 1апреля 2015 г. вступит в действие новый РМЭ, принятый на Всемирной конференции по международным телекоммуникациям в декабре 2012 г., однако концепция качества скорее будет уточнена, чем пересмотрена.

В последнее время сквозное качество, QoS, профессиональным сообществом все чаще рассматривается как качество обслуживания, предоставляемое коммуникационной сетью от стыка с провайдером до стыка с потребителем. А качество восприятия, QoE, выступает как качество сервиса, воспринимаемое конечным пользователем, и включает в себя всю совокупность эффектов цепочки предоставления конечной услуги (клиент, терминал, сетевая и сервисная инфраструктуры). Оно учитывает и качество контента, и субъективные факторы, такие, как ожидания пользователей.

В этой связи, по крайней мере на переходный период, до урегулирования взаимоотношений операторов и контент-провайдеров, представляется необходимым нормативное закрепление регулятором пределов ответственности телеком-операторов за качество обслуживания.

И сделать это нужно с учетом диверсификации бизнеса, изменения продуктовых линеек операторов. К примеру, операторы «большой четверки» предоставляют не только голосовую телефонию и широкополосный доступ, но и IPTV, и массу приложений, и иной контент. Должны ли они нести ответственность за качество восприятия своих конечных услуг?

зации развития, также не сильно отстают от «Ростелекома» в такой «оптимизации».

Вместе с тем передача эксплуатации сотовых сетей в аутсорсинг, появление между поставщиком и потребителем услуг еще одного хозяйственного звена со своими финансовыми интересами также, по мнению специалистов, не способствует повышению качества обслуживания. В результате складывается впечатление, что эксплуатация сетей массового пользования все больше сводится к банальному устранению повреждений в неопределенные сроки.

Изменение роли регуляторов

Не мы одни в мире сталкиваемся с такими проблемами. Но решать их можно по-разному. Не случайно в условиях формирования новой цифровой коммуникационной среды и консолидированного рынка ИКТ растет роль национальных регуляторов. Качество предоставления услуг на сетях сегодня в решающей степени зависит от их компетентности, адаптивности, независимости, понимания проблем и путей современного развития.

Уровень качества обслуживания потребителей в телекоммуникациях должен определятся и поддерживаться прямыми или косвенными механизмами государственного регулирования

В виду важности проблемы МСЭ ежегодно выпускает специальные обзоры и отчеты по транснациональным аспектам регулирования в сетевом сообществе. Мировой опыт совершенствования регулирования в сфере коммуникаций каждые два года обсуждается на глобальных симпозиумах МСЭ для регуляторных органов и обобщается в виде рекомендаций национальным регуляторам. В руководящих указаниях 13-го глобального симпозиума, проходившего в июле 2013 г. в Варшаве, в частности, сказано: «Резкий рост потока данных в результате свободного доступа к сетям и быстрое развитие новых услуг и приложений, таких, как облачные услуги и мобильные приложения, вкупе с постоянно увеличивающейся комплексностью рынков ИКТ ставят под вопрос традиционные роли и полномочия регуляторных органов, требуя пересмотра подходов к регулированию в цифровой экосистеме».

У нас вызывают понимание и уважение усилия Роскомнадзора по созданию отвечающей современным требованиям системы контроля качества предоставления услуг связи в России. Международная академия связи вместе с профильной комиссией РСПП участвует в подготовке предложений к проекту представленной Роскомнадзором Концепции создания системы контроля качества предоставления услуг связи в РФ.

При подготовке конкретных предложений МАС исходила из того, что глобальные перемены в электросвязи в сочетании с отсутствием в России внятной политики формирования новой инфраструктуры цифровых коммуникаций и нерешенностью вопросов регулирования затрудняют выработку сбалансированных системных решений в части определения нормативов качества.

Принятые решения должны быть просты, понятны и удобны операторам, абонентам, выполнимы органами контроля, носить универсальный характер, вызывать минимальные изменения в действующем законодательстве и отраслевых нормативных актах.

Поэтому мы рекомендуем прежде всего ввести в РФ отвечающий этим требованиям мониторинг качества предоставления услуг связи, как это сделано в большинстве стран мира. Учесть при этом международный опыт и внедрить ряд механизмов, предложенных в концепции Роскомнадзора.

Мониторинг должен осуществляться по субъективным критериям удовлетворенности пользователей предоставляемыми услугами. Но для его организации, для достоверности и эффективного использования полученных данных необходимо навести порядок в учете, отчетности, регламентах, контроле и измерении параметров качества, в применении адекватных целям контроля, понятных и справедливых действий надзорного органа в случаях выявления отклонений от нормы.

Организатором и основным заказчиком мониторинга может быть только наделенный соответствующими полномочиями (которых сегодня явно недостаточно) и действующий в пределах установленных регламентов государственный надзорный орган (в части контроля за качеством услуг связи) или регулятор в сфере национальных телекоммуникаций.

Инициатива ЦНИИС по созданию системы и портала контроля качества ИКТ-услуг и одобрительная реакция на нее операторов подтверждают своевременность нашего предложения и вполне соответствуют нашим идеям организации обратной связи операторов с потребителями. ИКС

Недооценка динамических техник обхода защиты информации обходится дорого

Ущерб от утечек данных, по данным опроса, проведенного по заказу McAfee, в среднем составляет порядка $1 млн. Основную роль в утечках играют динамические техники обхода защиты информации, поэтому игнорировать их – непозволительная роскошь.

Исследование, проведенное компанией Vanson Bourne по заказу McAfee (дочерней компании Intel Security) показало, что специалисты, ответственные за защиту конфиденциальных данных, зачастую не понимают сути динамических техник обхода защиты информации (AETs, advanced evasion techniques) и их роли в реализации постоянных угроз повышенной сложности (APTs, advanced persistent threats), неверно их интерпретируют, а также используют неэффективные средства защиты. В рамках исследования был организован опрос 800 управляющих ИТ-службами и менеджеров по безопасности в разных странах – США, Великобритании, Германии, Франции, Австралии, Бразилии и ЮАР.

Динамические техники обхода защиты информации представляют собой средства маскировки, предназначенные для незаметного проникновения в сети и переноса вредоносного содержимого. Такие методы впервые были обнаружены в 2010 г. специалистом по сетевой безопасности компании Stonesoft, которая в 2013 г. стала частью компании McAfee. AETs могут быть использованы в сетевой атаке для разбиения вредоносного кода на фрагменты, обхода межсетевого экрана или системы предотвращения вторжений (IPS), а затем, уже в сети, для сборки кода и продолжения атаки.

Профессор Эндрю Блит из Университета Южного Уэльса, давно изучающий распространение динамических техник обхода защиты информации и их воздействие на безопасность сети, заявляет: «Существование динамических техник обхода защиты информации – это факт. Особенно удручает то, что большинство управляющих ИТ-службами и специалистов по обеспечению безопасности сильно недооценивают AETs, называя их количество равным 329 246. На самом деле таких методов примерно в 2500 раз больше – около 800 млн».

Из этих 800 млн известных на сегодняшний день динамических техник обхода защиты информации лишь 1% может быть обнаружен межсетевыми экранами. Такие методы получили широкое распространение с 2010 г., и сейчас мы сталкиваемся с миллионами комбинаций и модификаций подобных техник, основанных на особенностях строения сетей.

Причина, по которой методы AETs не фигурируют в отчетах и недооцениваются, заключается в том, что некоторые платные тесты позволяют производителям настроить защиту против них. В результате оказываются возможными обнаружение и защита только от определенных методов AETs, в то время как множество других подобных методов, быстро обновляемых и изменяемых преступными сообществами, остается незамеченным.

«В погоне за обнаружением новых вредоносных программ большинство организаций совершенно упускает из виду динамические техники обхода защиты информации, которые помогают вредоносным программам преодолевать барьеры безопасности, – делится своим мнением Джон Олтсик, главный аналитик компании Enterprise Strategy Group. – AETs – это серьезная угроза, поскольку большая часть средств защиты не позволяет их обнаружить и оказать им противодействие. ИБ-специалисты и руководители предприятий должны осознать всю реальность этой растущей угрозы».

Около 40% ИТ-специалистов, ответственных за принятие решений, считают, что не располагают средствами обнаружения и отслеживания динамических техник обхода защиты информации в своей организации, а почти две трети таких специалистов в качестве самой трудной проблемы, возникающей при внедрении технологий по борьбе с AETs, называют необходимость убедить руководство в том, что подобные атаки действительно представляют серьезную угрозу.

Вместе с тем последние громкие случаи утечки данных показали, что преступники по-прежнему могут в течение долгого времени успешно скрывать свою деятельность. Опрошенные эксперты также подтверждают этот факт. 22% ИБ-специалистов признали, что в их сетях были случаи утечки данных. Около 40% респондентов, подтвердивших утечку данных, считают, что основную роль в этом сыграли динамические техники обхода защиты информации. Участники опроса, в организациях которых за последние 12 месяцев наблюдалась утечка данных, оценили ущерб в среднем в $931 006. По данным опроса, наименьшее количество случаев утечки данных (15%) наблюдалось в Австралии, но средняя оценка нанесенного ущерба была значительно выше – $1,5 млн. Потери для американских организаций в среднем превысили $1 млн. Наиболее серьезным оказался удар по сектору финансовых услуг: ущерб от каждой утечки данных составил более $2 млн независимо от страны.

«Хакеры знают сложные методы обхода защиты и постоянно их используют, – подчеркивает Пэт Калхун, генеральный управляющий по защите сетей компании McAfee. – Мы готовы предложить компаниям обучение сотрудников, которое, как мы надеемся, укажет им, на что следует обратить внимание, и поможет понять, что нужно для защиты от таких атак».

Материал подготовлен экспертами компании McAfee. Part of Intel Security.

Технологии в гонке вузов за рейтингом

Конкуренция в сфере высшего образования обостряется во всем мире. Современные технологии позволяют значительно и относительно быстро улучшить некоторые показатели, определяющие позиции университета в международном рейтинге.

Кевин ДАНСИТ, управляющий партнер, CorCordi Education Consultancy

Татьяна ТОЛМАЧЕВА, партнер, CorCordi Education Consultancy

Ситуацию можно сравнить с гонкой за первенство в преодолении самой высокой вершины планеты Эверест в начале 1950-х гг. Но кто определяет победителя этой гонки? Любые оценки и классификации вызывают, как правило, многочисленные споры и критику, однако три международных рейтинга лучших университетов мира получили общее признание. Это рейтинг британского издания Times Higher Education (THE), Шанхайского университета Jiao Tong (Академический рейтинг университетов ARWU) и QS World University Rankings.

От Финляндии до Новой Зеландии, от Великобритании до Китая университеты выделяют все больше ресурсов для улучшения своих позиций в международных рейтингах. Япония поставила амбициозную цель: к 2020 г. правительство намерено обеспечить вхождение в список топ-100 университетов мира не менее 10 японских университетов. Стратегический план развития Манчестерского университета (University of Manchester) предполагает привлечение культовых ученых для повышения репутации и качества исследований, что в свою очередь положительно скажется на позиции вуза в таблицах мировых рейтингов; к 2015 г. планируется принять на работу 5 лауреатов Нобелевской премии.

Между тем в таблицах лидирующих университетов мира российские вузы представлены слабо. Для изменения этой ситуации в 2013 г. была запущена федеральная программа повышения международной конкурентоспособности российских вузов и вхождения к 2020 г. пяти российских университетов в топ-100 высших учебных заведений мира. Однако важно понять, что быстрее добиться планируемых изменений университетам позволит только использование технологий. На сегодняшний день для сотрудников и студентов вуза это наиболее действенные инструменты, позволяющие преодолеть многие, если не все барьеры общения и взаимодействия: расстояние, специфику национальной и организационной структуры, язык – все, что определяет обособленность деятельности многих университетов мира, формируя «острова» знаний, опыта и экспертизы.

Технологии позволяют усовершенствовать процесс преподавания, обучения и проведения исследований, повысить эффективность систем управления, усилить международное сотрудничество и улучшить весь профиль университета. Кроме того, надлежащее и эффективное использование технологий стимулирует инновационную деятельность студентов, повышает шансы их трудоустройства и в конечном счете приносит значительную экономическую и социальную выгоду всей нации. Проанализируем, как и на какие операционные показатели деятельности вузов могут повлиять технологии.

Глобализация и российские вузы

Для повышения позиции университета в сфере создания и передачи знаний интернационализация сегодня является необходимым условием: способность университета к интеграции и его вовлеченность в глобальную сеть знаний, основанная на возможности соединять, передавать и взаимодействовать, – ключ к успеху в мировом масштабе. Хотя у России большая история выдающихся научных открытий во многих дисциплинах и под руководством ученых мирового уровня, не все открытия получили заслуженное признание в мире. Причиной такой ситуации является традиционно низкая интеграция значи-

Табл. 1. Университеты развивающихся стран: выборочный сравнительный анализ QS World University Rankings

Университет	№ в рейтинге «Развивающиеся рынки»	№ в мировом рейтинге	Индекс академической репутации	Индекс репутации среди работодателей	Соотношение «преподаватели – студенты»	Индекс цитирования научных статей	Доля иностранных преподавателей	Доля иностранных студентов	Баллы
Hong Kong University (Гонконг)	1	26	99,4 № 28	93,1 № 48	94,7 № 60	51,7 № 239	100,0 № 19	98,7 № 26	88,6
МГУ (Россия)	9	120	84,1 № 83	64,8 № 173	99,9 № 17	6,3 № 664	8,7 № 594	37,3 № 352	63,9
Университет нефтяных и минеральных ресурсов им. короля Фахда (Саудовская Аравия)	22	216	44,0 № 265	55,4 № 242	84,7 № 113	7,7 № 626	100,0 № 12	61,6 № 201	49,9
Индийский институт технологий (Дели)	23	222	51,3 № 215	86,8 № 75	35,9 № 467	63,3 № 157	1,3 № 781	1,5 № 801	49,4

тельной части российских университетов в мировую систему высшего образования.

Анализ рейтинга университетов развивающихся стран, подготовленного по методике QS, показывает, что даже всемирно известный российский университет МГУ занимает далеко не лидерские позиции в глобальном рейтинге, например, по индексу цитирования научных статей (которым оценивается активность и качество научно-исследовательской деятельности), по доле иностранных преподавателей в преподавательском составе и доле иностранных студентов в числе обучающихся (см. табл. 1). И это притом, что МГУ занимает достаточно высокие позиции по таким показателям, как индекс академической репутации и соотношение профессорско-преподавательского состава и численности обучающихся.

Проблему МГУ нельзя назвать уникальной. В самом деле, у всех российских университетов, как правило, очень низкий уровень охвата международной аудитории, а набор международных преподавателей и студентов невелик. Кроме того, результативность научных исследований, которая измеряется индексом цитирования научных статей в ведущих англоязычных рецензируемых журналах, и в самом деле довольно низка. Это не означает, что профессорско-преподавательский состав не активен в научно-исследовательской деятельности – причина в том, что результаты исследования не публикуются в изданиях, которые учитываются метриками, а потому не имеют достаточного международного признания.

Если оценить негативное влияние этих показателей на позиции университета, то можно увидеть, что их суммарный вес потенциально доходит до 30% всех метрик, используемых методологией рейтинга QS (см. табл. 2). Кроме того, не стоит забывать, что эти три показателя косвенно оказывают влияние и на индекс академической репутации, и на индекс репутации среди работодателей, а значит, суммарный коэффициент может достигать 50%.

Таким образом очевидно, что успешная стратегия интернационализации имеет решающее значение для российского университета, нацеленного на улучшение своих позиций в международных рейтингах. Такая стратегия должна быть интегрирована во все аспекты деятельности вуза, включая разработку образовательных программ, организацию научно-исследовательской деятельности, обеспечение управления обучением и формирование сильной управленческой команды.

Эффективная стратегия интернационализации обеспечивает совместные международные исследования, результат которых – публикации в соавторстве с международными учеными в ведущих изданиях (выявленных в ходе соответствующего библиометрического анализа). Она также предполагает различные формы транснационального образования, в том числе

Табл. 2. QS-рейтинг ведущих университетов мира

Вес показателя, %	Показатель	Метод оценки
40	Индекс академической репутации	Репутационный опрос среди мирового академического сообщества
10	Индекс репутации среди работодателей	Репутационный опрос среди работодателей
20	Соотношение профессорско-преподавательского состава и численности обучающихся	Анализ данных, предоставляемых вузами, государственными организациями, агентствами, и открытых источников
20	Индекс цитирования научных статей (на 1-го преподавателя)	Данные баз Web of Science (Thomson Reuters); Scopus (Elsevier и Google Scholar)
5	Доля иностранных преподавателей в преподавательском составе	Расчет на основании данных, предоставленных вузом
5	Доля иностранных студентов в числе обучающихся	Расчет на основании данных, предоставленных вузом

Примечание: методология QS в отношении азиатских и латиноамериканских университетов имеет свою специфику

совместные с международными партнерами образовательные программы, которые в некоторых случаях позволяют получить двойной диплом. Помимо того, открытые онлайн-курсы могут не только обеспечить качество международного образования российским студентам, но также содействовать легкой и значительной интернационализации студентов в классе. Набирающие популярность программы международного обмена преподавателями и студентами – еще одна форма, позволяющая улучшить международный профиль университета и одновременно повлиять на его позиции в рейтинге ведущих вузов.

Технологический акселератор

В простом и предельно широком смысле научные исследования – это процесс сбора данных и информации, их изучение, обобщение и осмысление с целью производства новых знаний. В современных условиях в большинстве случаев научно-исследовательская работа стимулируется национальными амбициями государства и университетов – стремлением развивать и поддерживать высокий профиль и статус в области международных знаний и ноу-хау. Это достигается расширением границ знаний и развитием инноваций, полезных для всего международного сообщества.

Сам процесс проведения исследований и продвижение их результатов равно важны. Ключевыми факторами успеха в любой научно-исследовательской деятельности являются:

- обеспечение команде исследований наибольшей эффективности сбора данных, анализа и экспериментов;
- использование действенных инструментов для продвижения и распространения результатов научно-исследовательской работы (например, журнальных публикаций, изданий книг, презентаций с конференций) для создания репутации мирового уровня.

Технологии поддерживают процесс проведения исследований и распространение результатов научно-исследовательской работы. Технологии могут обеспечить и улучшить все аспекты исследовательской деятельности, например:

- предоставить более широкий доступ к глобальной базе знаний;
- расширить исследовательские связи и вовлечь в процесс исследований более широкое сообщество (взаимодействие);
- создать среду для работы виртуальной исследовательской команды;
- обеспечить управление информацией;
- стимулировать создание глобальной репутации (через построение цифровой идентификации, онлайн-присутствия, участие в социальных сетях, участие в конференциях посредством видеомостов и пр.);
- построить платформу для эффективного распространения результатов научно-исследовательской работы;
- поддерживать личное профессиональное развитие и рост исследователей.

Для успеха российских исследовательских университетов очень важно сделать акцент на увеличении числа публикаций, появившихся в результате транснационального исследовательского взаимодействия. По оценке ведущего исследователя в области науки о данных Мартина Шомшора (Digital Science), более 40% всех опубликованных в 2013 г. исследований появились в результате транснационального исследовательского взаимодействия (в 1996 г. – только 25%). Из них на долю исследователей из США приходится около 30%, Китая – 10%. Россия заметно отстает от США,

Табл. 3. Задачи и технологические решения

Задачи университета	Технологии (приложения) для решения
Усовершенствовать процессы исследований и повысить эффективность распространения их результатов	▸ ПО, сайты и приложения для управления информацией и для работы с документами (например, Zotero, Reference Manager, Evernote, Diigo, Springpad, Instapaper, StumbleUpon) ▸ Академические социальные сети (например, Mendeley) ▸ Библиометрические и наукометрические инструменты (ПО и приложения): BibExcel, Publish, Perish, Paject, CiteSpace
Расширить исследовательские связи, повысить эффективность взаимодействия, построить виртуальную образовательную среду	▸ Технологии взаимодействия и передачи видео- и голосовых данных, обеспечивающие эффект присутствия: веб-конференции, видеоконференции, телепрезентации ▸ Онлайн-взаимодействие: wiki, twitter, социальные сети ▸ Системы записи занятий Lecture capture ▸ Открытые онлайн-курсы
Повысить качество обучения и вовлеченность студентов в процесс обучения	▸ Интерактивные доски ▸ ПО для создания презентаций и средств визуализации информации (например, PowerPoint) ▸ Системы голосования в классе (Promethean, iClicker) ▸ Технологии для образовательной методики «перевернутый класс» (Flipping the classroom) ▸ Подкасты ▸ Обучающие игры: DuoLingo, Ribbon Hero, ClassDojo, Goalbook, World Peace Game, Brainscape, Socrative 101 ▸ Технологии обучения на планшетных компьютерах ▸ ПО и приложения трекинга и оценки знаний (Socrative, Edmodo, ClassDojo, GradeXpert, Accelerus), ПО для управления процессом обучения (Mindflash, Administrate, eLeAP, Firmwater LMS, Thinking Cap LMS, ILMS)

Германии, Великобритании и Китая в распространении результатов транснациональной исследовательской деятельности. В самом деле, удельный вес этого показателя в России, Бразилии и Индии намного ниже, чем в таких небольших странах, как Бельгия, Израиль, Сингапур и Тайвань.

Эффективное транснациональное взаимодействие требует более широкой активности исследовательского сообщества, расширения исследовательских связей и выстраивания виртуальных исследовательских команд. Достижение этой цели ставит перед университетами ряд задач, с которыми можно справиться с помощью определенных технологических решений (см. табл. 3).

Можно привести много примеров использования университетами по всему миру технологий для решения своих бизнес-задач, и их число растет, поскольку со временем приходит понимание всех предоставляемых ими преимуществ. Для многих университетов ключевым фактором успеха является возможность через создание виртуальной образовательной среды привлекать студентов, обучающихся удаленно. Нередко такая возможность позволяет привлекать международных партнеров к совместным программам или программам с двойными дипломами. В других случаях отдельные университеты и консорциумы университетов запускают онлайн-проекты (например, Coursera, edX в США, FutureLearn в Великобритании, Open2Study в Австралии), предлагая массовое обучение (часто бесплатное и, как правило, без выдачи каких-либо сертификатов и дипломов). Даже такой престижный университет, как Гарвардская школа бизнеса (HBS), запускает в июне 2014 года несколько своих программ дистанционного обучения. К участию привлечены такие культовые профессора, как Майкл Портер и Клейтон Кристенсен.

Технологии оказывают заметное влияние и на традиционные учебные заведения. Сегодня полные программно-аппаратные решения Lecture capture, включающие запись, реформатирование, вещание, обмен и архивирование, позволяют университетам использовать методику «перевернутого класса» (Flipping the classroom). Благодаря ей студенты получают доступ к обязательным обучающим материалам до занятия, а аудиторное время посвящено практическим заданиям для закрепления теоретического материала, изученного дома самостоятельно, и развитию на его основе практических навыков.

Комплексное воздействие глобализации и стремительные технологические изменения в свою очередь значительно меняют кампус XXI века. Он становится более независимым. Полностью подключенный к интернету по проводным и беспроводным сетям, кампус уже не ограничен физическими стенами. Исследователи эффективно ведут совместную научно-исследовательскую работу в режиме реального времени, не чувствуя региональных и международных границ, комфортно располагаясь в своих кабинетах и лабораториях. Центром интерактивного образовательного процесса становятся электронные библиотеки. И хотя сегодняшнему университету еще далеко до нарисованного будущего, технологии уже сейчас кардинально, быстро и безповоротно меняют мир, трансформируя бизнес-модели образования.

■ ■ ■

Университеты должны быть готовы принять технологический вызов. Те, которые этого не сделают, безвозвратно устареют и станут невостребованными. Эту мысль подтверждает и создатель теории подрывных инноваций, один из соавторов книги «Инновационный университет: изменение ДНК высшего образования изнутри» Клейтон Кристенсен, который считает, что в следующие 10–15 лет 25% вузов или совсем умрут, или вольются в другие университеты.* Как считают авторы, уже сейчас традиционные вузы демонстрируют штаммы сломанной бизнес-модели, отражающие спрос и ценовое давление, несвойственные раннее высшему образованию. Подрывные инновации (среди которых, например, массовые открытые онлайн-курсы) со временем приведут к полной трансформации индустрии. И не стоит забывать, что именно технологии позволяют обеспечивать их внедрение и реализацию. ИКС

Успешная стратегия интернационализации имеет решающее значение для российского университета, нацеленного на улучшение своих позиций в международных рейтингах

* C. Christensen, M. Horn. Innovation Imperative: Change Everything Online Education as an Agent of Transformation: New York Times, 01/11/2013).

Защита данных в медицине
Все ли учтено?

Часть 2. Часть 1 см. «ИКС» №5' 2014, с. 50

Врачебная тайна ассоциируется в первую очередь с долгом перед тем, кто обратился за медицинской помощью. Однако в современных условиях ответственность за сохранение секретов становится практически обоюдной.

Леонид БАРАНОВ

Границы защиты

Рассмотрим вполне обыденный для наших дней сценарий: пациент Z устанавливает на свой смартфон из Google Play приложение Diabet. При этом он осуществлял поиск соответствующих лекарственных препаратов в поисковых системах и электронных магазинах (что, скорее всего, нашло отражение в cookies), просматривал соответствующие материалы и сделал несколько закладок в браузере. Немного позже он обсуждал свои проблемы на форумах соответствующей тематики и несколько раз обменивался электронной почтой – отправлял и получал данные исследований и рекомендации, назначенные лечащим врачом, – с людьми, страдающими аналогичным недугом. В результате с некоторыми стал перезваниваться. Сколько шансов у него сохранить свои данные в тайне? Задумывается ли он, да и в его ли силах определить и контролировать возможные границы распространения этой информации? Кроме того, где и по чьей вине в какой-то момент может стать общедоступным исследование, подписанное врачом X, остается только догадываться.

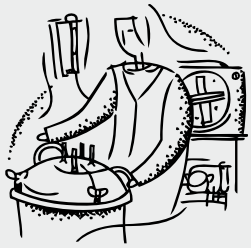
Но стоит ли гадать, кого по крайней мере могут попытаться привлечь к ответственности, окажись данные там, где никто не ожидал, да и вообще совершенно не хотел видеть? Для медицинских организаций строят модели угроз и считают риски. А кто возьмется делать это для себя?

От кого мы скрываем собственную медицинскую информацию?

От работодателя? Там, где необходимо, существует проверка на профессиональную пригодность с учетом особенностей профессии и условий работы, а там, где нужды в этом нет, такие сведения никому не интересны. От «компетентных органов»? Они имеют право доступа – при необходимости и в объеме своих полномочий – к любой информации; причем рамки закона соответствующим образом корректируются: совсем недавно органы прокуратуры получили право узнавать врачебную тайну граждан без их согласия. От самого себя? Но по запросу (и по закону) нам обязаны предоставить любые сведения, касающиеся собственного здоровья, включая те, которые раньше раскрывать считалось недопустимым. Так от кого же? Кто и с какой целью становится заинтересованным лицом? И всегда ли наши страхи оправданы? Ведь даже в сообщении под заголовком «Хакеры получили персональные данные нескольких тысяч пациентов» основ-

От сокрытия – к сохранению

Согласно Большой медицинской энциклопедии, понятие врачебной тайны уходит в глубь веков и, похоже, появляется одновременно с врачеванием. Поначалу она была частью «таинственного обряда», акта, выполняемого жрецами древнего Египта и Индии и носящего религиозный характер. Когда роль врача в обществе освобождалась от жреческих традиций, врачебная тайна, возможно, стала следствием гуманистической миссии врача, желания не навредить больному (понимая под этим не только физический, но и моральный и материальный ущерб). Уже в «Клятве Гиппократа» (по разным источникам, V–IV вв. до н.э.) есть строки, непосредственно относящиеся к сохранению полученной информации: «Что бы при лечении (а также без лечения) я ни увидел или ни услышал касательно жизни людской из того, что не следует когда-либо разглашать, я умолчу о том, считая подобные вещи тайной».



В «Факультетском обещании врача России» (XIX–XX вв.) были, в частности, такие строки: «Обещаю [...] свято хранить вверяемые мне семейные тайны и не употреблять во зло оказыва-

ным акцентом может быть беспокойство по поводу того, что незаконным путем удалось получить полные сведения о 126 кредитных картах.

Кстати, необходимо отметить, что отдельные случаи законного сокрытия персональных данных носят достаточно спорный характер с этической точки зрения. Например, п. 2 ст. 15 Семейного кодекса РФ гласит: «Результаты обследования лица, вступающего в брак, составляют врачебную тайну и могут быть сообщены лицу, с которым оно намерено заключить брак, только с согласия лица, прошедшего обследование». При этом п. 3 той же статьи недвусмысленно обозначает уровень возникающих при этом рисков: «Если одно из лиц, вступающих в брак, скрыло от другого лица наличие венерической болезни или ВИЧ-инфекции, последнее вправе обратиться в суд с требованием о признании брака недействительным».

Защищать или не защищать?

Этот вопрос далеко не нов. Например, еще в начале XX века нарком здравоохранения Н.А. Семашко предлагал отказаться от врачебной тайны, мотивируя это тем, что болезнь – не позор, а несчастье. Правда, впоследствии он отказался от этой идеи и признал ее ошибочной. Учитывая перемены, произошедшие за почти 100 лет, возможно, такая идея уже выглядит не столь революционной, как прежде. Сейчас сформировалось совершенно другое общество, гораздо более открытое и толерантное – достаточно взглянуть на рекламу, зачастую изобилующую интимными подробностями использования гигиенических средств, не говоря уж о совершенно специфичной информации, считавшейся просто неприличной в эпоху, когда у нас «секса не было». Но кто теперь обращает на это внимание? Широкое, публичное и подробное освещение получают такие темы, как гомосексуальные отношения, запрет абортов, суррогатное материнство. Шокирует ли это общество сейчас и можно ли это было представить еще 50 лет назад?

Речь, конечно, не идет о том, чтобы передать медицинские данные в публичный доступ, размещая их, например, на сайтах медицинских учреждений. Но, возможно, следовало бы основной фокус сместить с обеспечения их, по сути, секретности на защиту от несанкционированного изменения и предумышленной фальсификации, которые, кстати, могут нанести гораздо больший ущерб как моральному, так и физическому здоровью человека, чем разглашение. В самом деле, сколько вреда может принести пилот самолета или водитель транспортного средства, допуск которых к работе был осуществлен на основе сфальсифицированных данных? И какой убыток возможен от необоснованного (вследствие тех же фальсификаций) денежного или лекарственного обеспечения? А ведь злоумышленные действия теперь уже возможны со стороны не только медицинского, но и инженерного персонала. Между тем, обеспечить целостность данных никак не менее сложная задача, чем обеспечить их конфиденциальность.

Секреты на виду

Вспомним, что, согласно определению врачебной тайны, к ней относятся, в частности, сведения о факте обращения гражданина за оказанием медицинской помощи и состоянии его здоровья. Но ряд заболеваний (например, легкие переломы конечностей, простудные заболевания) является публично демонстрируемым и идентифицируемым, а скрыть «факт обращения за оказанием медицинской помощи» во время регистрации в медицинской информационной системе при записи на прием в поликлинике невозможно. И если прежде необходимые сопутствующие документы (например, паспорт) обрабатывались в регистратуре за перегородкой, то сейчас человек принародно вводит ряд данных в инфомат, а подчас обращается за помощью (публичной, кстати) к сотруднику медицинской организации или просто к более подготовленным в сфере информационных технологий соседям по очереди. Стоя рядом с инфоматом, сейчас при желании можно получить любые персональные данные, в первую очередь – пожилых людей, что фактически нарушает врачебную тайну и организационно, и технологически. А наши покупки в аптеке? Это абсолютно публичный акт, и по названию отпущенных препаратов (предназначенных иной раз для лечения или профилактики недугов в весьма интимных сферах жизни) легко установить, что именно беспокоит человека. Вроде бы привычные ситуации, а вот с позиции закона медицинское учреждение обязано хранить тайну обращения.

Кстати, иной раз бытующее мнение, согласно которому «раньше» данные никак не защищались, ошибочно. Напротив, данные медицинского характера на бумажном носителе были очень хорошо защищены: хранились в специальных помещениях с ограниченным доступом, не выдавались на руки пациентам даже в пределах медицинского учреждения, из кабинета в кабинет переносились медицинской сестрой и т.д. Защита обеспечивалась комплексом организационных мер.

Теперь же каналы поступления первичных данных в информационные системы (запись через интернет) не являются закрытыми и не имеют никакой защиты. И хотя, согласно новой редакции закона (ФЗ «Об основах охраны здоровья граждан в Российской Феде-

емого мне доверия».

«Присяга врача Советского Союза» содержала формулировку: «Получая высокое звание врача и приступая к врачебной деятельности, я торжественно клянусь [..] хранить врачебную тайну».

В наше время, согласно действующему законодательству, в «Клятве врача России» также есть строки: «.. клянусь [..] хранить врачебную тайну».

рации»), из статьи, определяющей понятие медицинской тайны убрали строки «Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений», это не означает, что конфиденциальность по-прежнему не должна быть обеспечена.

Получается, что сегодняшнее положение дел в сфере защиты персональных данных пациентов, врачебной тайны начинает напоминать работу некой спецслужбы, насыщенной секретами, одна часть сотрудников которой (персонал медицинских учреждений) со всей ответственностью должна относиться к их охране, тогда как другая (пациенты) не имеет понятия о том, как эти секреты сохранять – может выносить их за стены учреждений, да и вообще совершенно свободно ими распоряжаться, подчас вообще не признавая никаких секретов или о них не задумываясь.

Теперь каналы поступления первичных данных в информационные системы (запись через интернет) не являются закрытыми и не имеют никакой защиты

Без вины виноватые

А ведь пациент имеет полное право вообще отказаться от предоставления своих персональных данных, что в отдаленной перспективе может привести к непредсказуемым последствиям. В самом деле, далеко не все люди бывают последовательны в своих действиях – кто в силу характера, кто по воле обстоятельств. Соответственно, в разных медицинских учреждениях для получения одной и той же медицинской услуги «информированное согласие пациента» в одних случаях будет подписано, а в других – нет, т. е. может быть осознанно востребовано получение медицинской услуги без предоставления своих данных.

Таким образом, вполне вероятна ситуация, когда конфиденциальная, с точки зрения пациента (как субъекта персональных данных), информация может появиться в общем доступе из источника, которому он дал право ею распоряжаться, но ответственность за этот факт он возложит на другой источник, который добросовестно сохранял его данные, но тем не менее будет вовлечен в разбирательства в связи с их утечкой.

Кроме того, хотя персональные данные одновременно могут принадлежать их носителям, инфраструктуре передачи, инфраструктуре хранения и непосредственно медицинской организации (причем, как правило, не одной), ответственность за их утечку, вполне возможно, будет возлагаться только на последнюю. Разрешение подобных споров может быть довольно непростой задачей и, пусть косвенно, серьезно влиять на работу медицинских учреждений.

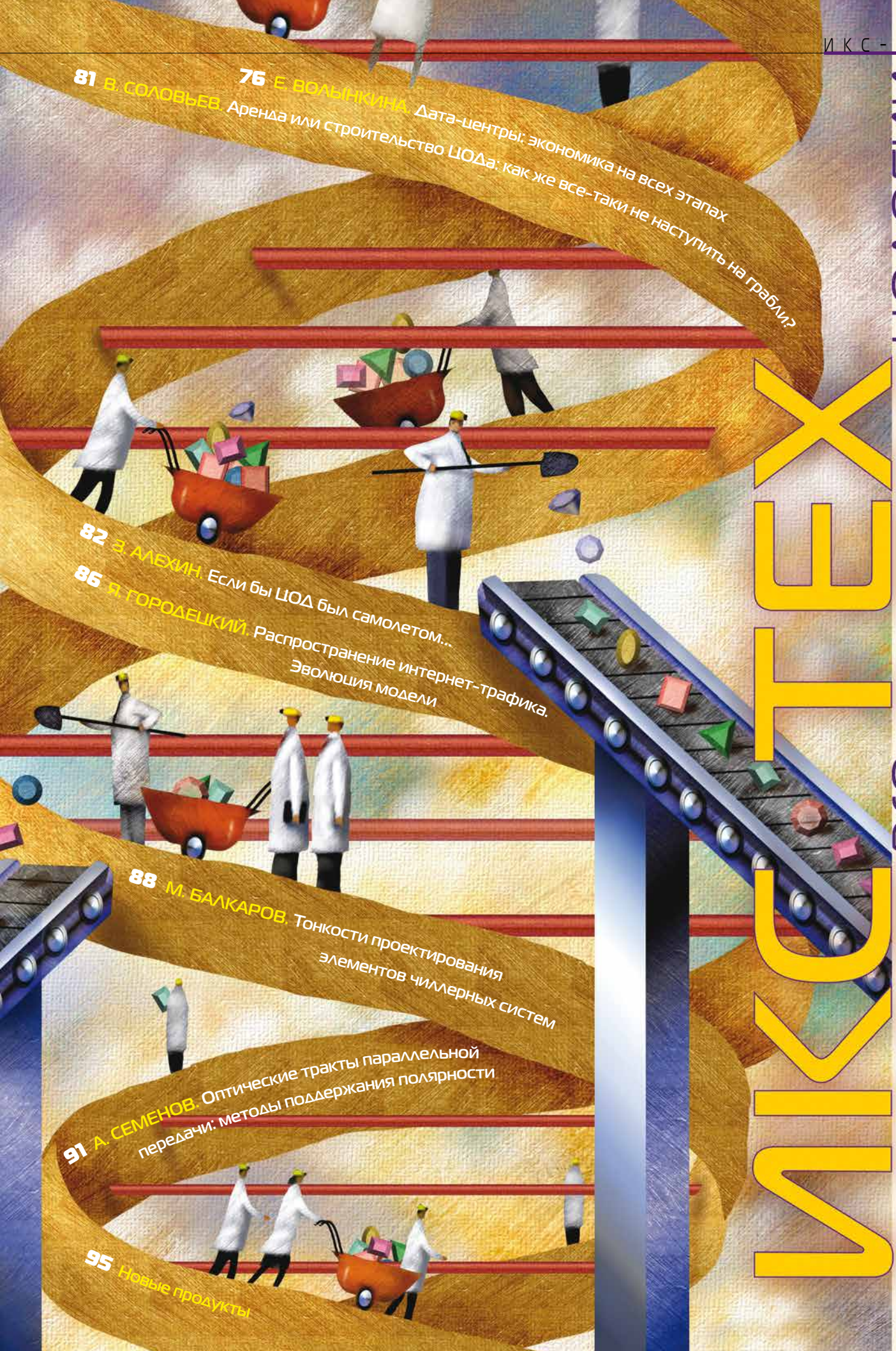
■ ■ ■

Итак, все ли учтено в медицине в области защиты персональных данных? По размышлении получается, что все «под контролем» (хотя, возможно, в силу сложности и объема еще не все сделано) только в области, охватывающей медицинские учреждения. И даже здесь о защите данных приходится рассуждать с оговорками и уточнениями. Причем, не оттого, что кто-то недобросовестно выполняет свои обязанности, а потому что информационные границы пытаются поставить самой ж и з н и, которой чуждо прокрустово ложе правил и инструкций по самой сути. Человеку свойственно делиться своими бедами, опираться на чужой опыт, искать советов в трудных ситуациях и находить положительные примеры. Более того, иногда только сообща решаются проблемы, непосильные одиночкам. И новые условия жизни, жизни в информационном обществе, дают для этого колоссальные возможности. Круг заинтересованных лиц практически больше не имеет организационных и географических рамок. Старая поговорка «слухами земля полнится» в информационном обществе приобретает новый контекст и становится уже «слухами Земля полнится», и этого нельзя не замечать.

В конечном счете, что мы так настойчиво пытаемся скрыть от окружающих? Недостатки здоровья? Но у кого их нет? И как тогда расценивать Паралимпийские игры, где, несмотря на ограниченные возможности участников, разворачиваются события, приковывающие внимание миллионов болельщиков и по накалу страстей ни в чем не уступающие играм Олимпийским, в которых участвуют спортсмены, символизирующие, по идее, образцы человеческого здоровья?

Возможно, общество уже созрело для того, чтобы пусть постепенно, но последовательно менять свое отношение к тому, что болезнь – это не позор, а несчастье, и найдет лучшее применение гигантским средствам на обеспечение секретности того, что практически одномоментно может стать секретом Полишинеля. ИКС

ИКС pro технологии



Дата-центры экономика на всех этапах

Евгения ВОЛЫНКИНА

В создании экономически эффективного дата-центра важно продумать все – и электропитание, и охлаждение, и ИТ-оборудование, и кабельное хозяйство, и системы мониторинга, и даже заглушки на серверных стойках. Все инновации вендоров оцениваются сейчас с экономической точки зрения.

Любой дата-центр – это по сути большой калькулятор, с помощью которого компания должна зарабатывать деньги. Компоненты этого калькулятора, особенности его проектирования, сборки и настройки стали предметами обсуждения на 2-й международной конференции Data Center Design & Engineering (DCDE), организованной журналом «ИКС» (→ также см. с. 24-25).

Товар лицом

Проектирование и строительство дата-центра – дело непростое не только из-за сложности самого объекта, но и из-за большого числа участников этого процесса: консультантов, проектировщиков, подрядчиков, заказчиков и инвесторов. И все они должны иметь максимально полную информацию не только о своем участке проекта и своих системах, но и о том, что делают «смежники». Это позволит и минимизировать ошибки «на стыках», и создать гармоничный проект, имеющий заявленные характеристики. Понятно, что все участники проекта не могут быть специалистами и по архитектуре, и по строительству, и по инженерным системам. Для заказчиков дата-центров, как отмечает Александр Овчинников («АДМ Партнершип»), проектная документация часто выглядит грудой чертежей с непонятными символами. А от заказчика зависит судьба всего проекта, так что в интересах проектировщика представить свой продукт в максимально наглядной форме. Современные системы автоматизированного проектирования в принципе имеют функции, позволяющие выполнять качественную визуализацию всех конструкций в 3D, по которой заказчик может понять, что же в итоге он получит – корпуса с проездами и дорогами, фасады зданий, внутренние помещения с инженерными системами, ИТ-оборудованием и коммуникациями. А инженерам-проектировщикам эта 3D-картина поможет определить, не совершили ли они каких-то ошибок, не пересеклись ли где-то воздуховоды и лотки для кабелей, пройдет ли трубопровод через отверстие в перекрытии и т.д. По мнению специалистов, подробная объемная модель здания позволяет на 90% уменьшить количество ошибок, возникающих на этапах создания рабочей документации и начала строительства.

Системы визуализации разрабатывают под свои нужды и производители оборудования для дата-центров. Такая система создана, например, компанией Panduit, которая специализируется на построении СКС. Как объяснил Александр Андреев (Panduit), это ПО нельзя назвать полноценной системой промышленного моделирования, его задача – создать предварительный трехмерный дизайн дата-центра на основе самых общих данных о параметрах будущего ЦОДа, полученных от заказчика. Тем не менее, система позволяет сэкономить немало времени: в одной комнате у компьютера могут собраться представители пяти-шести поставщиков отдельных систем и буквально за два-три часа согласовать проект дата-центра с размещением шкафов, серверов, коммутационного оборудования, кондиционеров, трубопроводов, кабелей, лотков и пр., после чего каждый поставщик может заняться подробной разработкой своей части проекта (в «обычной» жизни на согласование такого проекта может уйти несколько месяцев).

Модульная мода

Однако сейчас вендоры все чаще предлагают заказчикам «нарисовать» ЦОД из готовых кубиков-модулей. Причем эти модули делаются не только из легких каркасных конструкций, но и из железобетона – такие, например, предлагает компания M+W Group. По внешнему виду такой модульный ЦОД сложно отличить от «капитального». Во всем остальном эти модули имеют те же преимущества, что и их легкие собратья: стандартные размеры и комплектацию, заводское произ-

водство, быстрое проектирование, доставку на место, установку и ввод в эксплуатацию, возможности масштабирования и по горизонтали, и по вертикали. Причем, несмотря на железобетонное исполнение, модуль M+W Group по своим весу и размерам позволяет доставлять его на место обычным грузовым транспортом. Есть уже инсталляции, где из таких модулей собран дата-центр общей площадью 1000 кв. м.

За крупные модульные ЦОДы берется и компания Emerson Network Power. Ею разработаны 10 типовых решений модульных дата-центров SmartMod с разными вариантами систем охлаждения от фреоновых до адиабатических. Заявленный коэффициент PUE не превышает 1,5. Самый маленький SmartMod с четырьмя серверными стойками мощностью 7,5 кВт каждая помещается в контейнере размером 2900 × 2300 × 6100 мм. Более крупный его собрат размером 3000 × 3300 × 12500 мм, в котором установлены семь стоек по 8 кВт, уже работает в Санкт-Петербурге в интересах «Газпрома». Есть и модели, предназначенные для систем высокой плотности, вплоть до 30 кВт на стойку. А самый большой объект, собранный из контейнеров SmartMod, сейчас возводится в Швеции, его общая потребляемая мощность составляет 15 МВт.

Свое слово на уже довольно тесном рынке модульных ЦОДов собирается сказать и российская компания Green MDC. Как заявил ее генеральный директор Федор Клименко, в своих разработках Green MDC постаралась использовать плюсы и исключить минусы решений других вендоров. К последним он относит высокую удельную стоимость и большие сроки поставки для классических модульных ЦОДов, неудобство эксплуатации и низкую энергоэффективность контейнерных дата-центров. Поэтому поставка модульного Green MDC осуществляется за 12 недель, перед транспортировкой его можно разобрать на компоненты, а в его начинке используются давно проверенные решения. Есть варианты для установки в помещениях и на улице, с 12 и 24 стойками, с разными системами охлаждения, в том числе с использованием фрикулинга. И по энергоэффективности модули Green MDC выглядят вполне достойно: заявленный среднегодовой PUE составляет 1,24.

Модульный принцип давно взят на вооружение и производителями систем ИБП для ЦОДов. При относительно малых мощностях они обходятся дороже, чем моноблочные, но на уровне 500 кВт ценовая разница уже невелика. Например, конек компании ABB – модульные системы ИБП с децентрализованной параллельной архитектурой. Если централизованная архитектура предполагает наличие общих блоков – центрального процессора, панели управления, статического байпаса, батарей, – то в децентрализованной каждый модуль системы – законченный ИБП, а общим элементом является только силовой шкаф. Благодаря такой конструкции в системе нет единой точки отказа, ее легко обслуживать, потому что сами модули легкие и их можно менять в горячем режиме. Реализовано все это во флагманской модульной системе Conceptpower DPA 500 с максимальной мощностью стойки 500 кВт и модулями по 100 кВт каждый. Всего можно установить в параллель до шести таких стоек, получив систему мощностью 3 МВт. Системы семейства Conceptpower DPA могут оснащаться также модулями мощностью 24, 32 и 40 кВт.

Модульные ИБП для дата-центров выпускает и компания Entel. Как рассказал Валерий Суханов («Гулливер»), компактные модульные системы Entel IPX, мощность которых может варьироваться от 15 до 120 кВА с шагом 15 кВА, уже установлены в России в нескольких

корпоративных ЦОДах. Причем в одной из инсталляций выбор заказчика был обусловлен сильными ограничениями на площадь, выделенную под ИБП. Около полугода назад на рынке появились гибко масштабируемые системы Entel IPS-M, мощность которых можно наращивать от 3 до 480 кВА с помощью модулей мощностью 3, 5, 6, 10, 15 и 20 кВА. А самой последней разработкой компании является ИБП Entel IPC с силовыми модулями мощностью 33,5 кВА, из которых можно собрать систему с максимальной мощностью 600 кВА при резервировании N+3.

Динамика vs статика ИБП

Долгое время создатели ЦОДов смотрели на динамические ИБП как на экзотику, потому что они были экономически оправданы лишь при высоких мощностях, до которых не дотягивали многие российские дата-центры. Но когда среди ЦОДов появились достаточно мощные объекты, ДИБП стали реально востребованы. Например, компания «Евро-Дизель» недавно выпустила новую серию ДИБП NO-BREAK KS7e мощностью от 2250 до 2750 кВА, которые фактически имеют 100%-ю доступность. Достигается это за счет автоматической

смазки всех подшипников без полной остановки системы, использования необслуживаемого электромагнитного сцепления и отсутствия необходимости в проверке соосности благодаря моноблочной конструкции. Кроме того, производитель гарантирует 100%-й пуск дизельного двигателя этого ДИБП, потому что двигатель предварительно прогрет и смазан и, кроме того, проходит регулярное тестирование по заданному пользователем расписанию. При нагрузке 30% КПД ДИБП NO-BREAK KS7e составляет 92%. Можно также отметить компактный дизайн этой системы: ее размеры – 9,3 × 2 × 2 м, тогда как системы предыдущего поколения имели длину от 9,95 м. При равной мощности ДИБП NO-BREAK KS7e занимают на 40–60% меньше места, чем статические ИБП.

На компактность, надежность и простоту обслуживания своих дизельно-роторных ИБП (ДРИБП) обращает внимание и компания Hitec Power Protection. ДРИБП Hitec сейчас имеют мощность от 300 до 3000 кВА, что позволяет использовать их в самых разных ЦОДах. Таких объектов в России уже 10, и мощность самого крупного – 10 МВт. Как отметил Рене Лацина (Hitec), при использовании классических систем с ДГУ и статическими ИБП упомянутые компоненты обычно поставляются разными производителями, и это часто создает определенные проблемы, в частности необходимость согласовать выбор ДГУ не только с нагрузкой, но и со статическими ИБП. Кроме того, такая система имеет много переключателей и модулей управления, функционирование которых зависит друг от друга, а в ДРИБП Hitec все основные энергетические элементы собраны на одной раме и соединены простой соосной механической связью. Большим достоинством ДРИБП является их способность поддерживать одновременно работу и ИТ-нагрузки, и системы охлаждения. Причем, в ДРИБП вероятность запуска двигателя равна фактически 100%, т.к. в случае проблем с аккумулятором стартера сигнал на запуск приходит с резервной батареи или напрямую от кинетического модуля, который работает всегда.

Столь же высокая надежность требуется системам бесперебойного электроснабжения, работающим на ответственных объектах и мероприятиях, таких, например, как недавние Олимпийские игры в Сочи. Ситуация – как в ЦОДе: заказчик требует 100%-й доступности. Как рассказал Василий Лапшин («Абитех»), в Сочи–2014 для обеспечения электропитания всей инфраструктуры (учитывая ИТ- и телекоммуникационную нагрузки) на 32 объектах горного и прибрежного кластера, главном вокзале Сочи и в аэропорту Адлер были задействованы около 1500 ИБП производства GE мощностью от 700 ВА до 500 кВА. Общая суммарная мощность всех систем бесперебойного электропитания составила более 16 МВА – как у крупного дата-центра. Только одних аккумуляторных батарей в их составе было более 5500 штук. Конечно, уследить за таким хозяйством можно только с помощью системы мониторинга, которая круглосуточно каждые 60 секунд производила опрос более 300 критичных ИБП. Всего за время игр было зарегистрировано 1137 аварийных ситуаций, но ни одной потери нагрузки не было. В таком режиме, но только месяцами и годами, приходится работать системам электропитания многих ЦОДов.

Фрикулинг и не только

Ну а в секторе систем охлаждения вендоры активно продвигают системы фрикулинга, которые, по сути, уже стали массовыми. В разряде экзотики пока находятся только системы с адиабатическим охлаждением воздуха. Примером такого решения является новая система адиабатического прецизионного кондиционирования Mirage компании NordVent, которая, по словам генерального директора ее российского представительства Андрея Миляева, является первым в мире серийным образцом решения, работающего на эффекте охлаждения воздуха за счет адиабатического охлаждения воды. Система Mirage позволяет работать в режиме фрикулинга до температуры +29°C на улице, т.е. включать резервную систему компрессорного ох-

лаждения придется крайне редко. Уже есть инсталляция восьми таких систем мощностью 125 кВт каждая в ЦОДе в Амстердаме, где потребляемая мощность ИТ-нагрузки составляет 750 кВт. По подсчетам NordVent, система Mirage такой мощности должна окупаться за три года.

Более многочисленными инсталляциями могут похвастать системы прямого свободного охлаждения для дата-центров AMD 2000 CWU-D компании Stulz. Компания HTS, которая является официальным поставщиком прецизионного оборудования Stulz в России, уже имеет целый список реализованных проектов в дата-центрах мощностью от 200 до 900 кВт. Правда, у системы AMD 2000 не столь широкий диапазон работы в режиме фрикулинга – до +24°C, но в российском климате это означает достаточно эпизодическое включение компрессорных холодильных машин.

Однако в стремлении использовать передовые решения не стоит забывать о мерах, которые не требуют больших затрат, но позволяют заметно повысить эффективность любой системы охлаждения дата-центра за счет разных технологий оптимизации воздушных потоков. Максимальный эффект дает предотвращение перемешивания воздуха из холодных и горячих коридоров с помощью заглушек и уплотнений. Компанией Minkels разработаны специальные пластиковые заглушки для серверных и телекоммуникационных шкафов, а также пенные уплотнители для кабельных вводов, позволяющие обеспечить комфортную работу оборудования внутри стоек. По словам Константина Кондобы (Minkels), комплекс всех этих мер часто позволяет повысить КПД системы охлаждения на 80–90%(!).

От мониторинга до управления

Безотказные системы электропитания и высокоэффективные системы охлаждения, конечно, необходимы в ЦОДах, но чтобы все это оборудование работало с заявленными характеристиками, необходимы системы мониторинга и управления. От нештатных ситуаций никто не гарантирован, но чтобы минимизировать последствия, важно вовремя заметить небольшие изменения в работе оборудования, которые могут рано или поздно привести к его выходу из строя. В современных крупных ЦОДах, где много потенциальных точек отказа, необходима централизованная система мониторинга. Как отметил Александр Нилов (Rittal), в одной 19-дюймовой стойке нужно контролировать влажность и температуру воздуха, фиксировать появление огня, дыма, открытие двери, попытки взлома или порчи. А если таких стоек сотни и тысячи? С их мониторингом должна справиться предлагаемая Rittal система CMC III с шиной обмена данными CAN-Bus, которая поддерживает используемые в ЦОДах разнородные датчики. Данные системы мониторинга CMC III можно использовать в высокоуровневом ПО для управления всей ИТ-инфраструктурой дата-центра RiZone.

Отдельной системы мониторинга требует кабельная инфраструктура ЦОДа. Схемы коммутации оборудования в дата-центрах очень сложны и «склонны к изменению», поскольку в любом ЦОДе периодически появляется новое оборудование и убирается старое. Все это отражается на кабельных подключениях, информацию о которых нужно поддерживать в актуальном состоянии, что, учитывая количество кабелей в ЦОДе, очень непросто. Штрихкоды на оборудовании уже давно используются в дата-центрах, а для аналогичной маркировки кабельных разъемов компания TE Connectivity предлагает использовать технологию CPID (Connection Point Identificator): в вилку каждого соединителя встраивается чип, в котором записана вся информация о данном кабеле. Благодаря этим чипам программно-аппаратный комплекс Quareo в реальном времени фик-

сирует все изменения в СКС ЦОДа, что упрощает и модернизацию, и обслуживание сети.

Еще одна система, которая должна быть в любом дата-центре, – система обнаружения пожара. Но, как отметил Геннадий Бахмутский («Пожтехника»), лучше выявлять не сам пожар, а его самые ранние предпосылки – тогда убытки от простоя, потери оборудования и данных могут оказаться нулевыми. Однако традиционные системы обнаружения пожара из-за низкой чувствительности оптических камер зачастую начинают бить тревогу, когда пожар уже разгорелся. Поэтому «Пожтехника» предлагает использовать в ЦОДах аспирационные системы нового поколения VESDA-E, которые по своей чувствительности в 1000 раз превосходят традиционные датчики. Они могут обнаружить даже слабые выделения дыма при перегреве электронных плат и кабелей. На этом этапе проблему сможет решить ИТ-администратор, просто заменив кабель, плату или сервер.

Ну а в крупном ЦОДе уместна будет комплексная система управления инфраструктурой DCIM (Data Center Infrastructure Management). Например, в DCIM-систему StruxureWare for DC компании Schneider Electric входит система мониторинга окружающей рабочей среды и энергосистем с видеонаблюдением и сбором соответствующих данных, инструменты управления электроснабжением, ИТ-оборудованием и его конфигурациями, средства бизнес-планирования дата-центра для отслеживания изменения его нагрузки и понимания дальнейшего развития, инструменты динамической оптимизации охлаждения и компьютерного моделирования воздушных потоков, которые позволяют выявить горячие зоны в серверном зале и потенциальные проблемы в ЦОДе. Зарубежные аналитики считают, что мировой рынок DCIM-систем в ближайшие годы будет расти со скоростью как минимум 40% в год, но, по мнению Андрея Ивашова (Schneider Electric), на российском рынке таких темпов ждать не приходится, потому что большинство наших заказчиков пока при расчете бюджетов обращают внимание только на критически важные для ЦОДа системы электропитания, охлаждения и контроля доступа. Однако для владельцев крупных дата-центров важно не только построить свои площадки, но и эффективно эксплуатировать их в течение достаточно длительного времени, и со временем они должны понять, что правильное управление ЦОДом мощностью 1МВт позволит сэкономить в год столько средств, что хватит на зарплату всему персоналу дата-центра.

Своя версия DCIM-системы есть и у компании RiT Technologies. Ее комплекс CenterMind контролирует параметры окружающей среды и работу системы электроснабжения, автоматически определяет топологию сети, идентифицирует в ней все сетевые устройства и контролирует соединения между ними, отслеживает все события, происходящие в СКС, в том числе обнаруживает подключение к корпоративной сети неавторизованных устройств, автоматизирует процессы перемещения, добавления или изменения всех доступных ресурсов сети. Стоит отметить возможность использования системы CenterMind для мониторинга и управления не только ЦОДа, а вообще ИТ-инфраструктуры предприятия, включая распределенные корпоративные ИТ-среды компаний, имеющих удаленные филиалы.

Последние штрихи

После внедрения DCIM-системы наступает время задуматься о том, как наиболее эффективно распорядиться имеющимися ИТ-ресурсами для обслуживания пользователей. Компания KEMP Technologies считает, что помогут в этом ее аппаратные и виртуальные устройства балансировки нагрузки KEMP LoadMaster, которые обеспечивают высокий уровень доступности, масштабируемость и оптимизацию доставки приложений. По словам руководителя представительства компании в России и СНГ Кирилла Зигизмунда, для решения проблем доступности приложений, работающих в ЦОДе, использование этого балансировщика более экономически выгодно, чем установка дополнительных серверов. LoadMaster может распределять нагрузку между несколькими ЦОДами, он отправляет запросы пользователя только на доступные серверы и приложения, уменьшает сетевые задержки и даже выполняет некоторые функции системы предотвращения вторжений. Что немаловажно, настройку этого балансировщика может выполнить любой администратор. В свете постоянных жалоб наших компаний на дефицит квалифицированных ИТ-кадров такой подход может только приветствоваться.

Таким образом, для построения дата-центров всех видов и размеров, их оснащения вполне передовой инженерной и ИТ-инфраструктурой, последующей ее эксплуатации и эффективного использования на благо своего бизнеса и бизнеса клиентов на рынке есть все необходимое. Это явный рынок покупателя, так что последнему нужно только не лениться: разбираться в предложениях вендоров, сравнивать и считать предстоящие затраты, и желательно не на один год вперед. ИКС

Аренда или строительство ЦОДа

как же все-таки не наступить на грабли?

Как правильно проанализировать экономическую эффективность инфраструктурных проектов? Если не учитывать неравноценность денег во времени, результаты анализа могут быть в корне неверны.

Владимир СОЛОВЬЕВ, директор по информационным технологиям, Финансовый университет при Правительстве РФ, докт. экон. наук, профессор

Предложения облачных сервисов становятся все более экономически привлекательными, и инстинкт самосохранения подталкивает моих коллег – CIO – к анализу эффективности своих проектов и сравнению различных вариантов их реализации.

Все большее внимание при этом уделяется классическому вопросу: арендовать или купить (построить), однако при выборе оптимального варианта часто допускаются ошибки.

Errare humanum est

От ошибок не застрахованы не только обычные ИТ-директора, но и признанные гуру. Вот, например, уважаемый автор в апрельском номере «ИКС»* сравнивает экономику строительства или аренды ЦОДа без учета ценности денег во времени и, естественно, получает результаты, прямо противоположные реальности.

Перейдем к конкретике.

Автор сравнивает строительство и аренду на примере одной стойки в центре обработки данных уровня Tier III и двух стоек в ЦОДе уровня Tier II.

Капитальные расходы на строительство одной стойки в ЦОДе уровня Tier III принимаются равными $100 000, а операционные расходы почему-то включают в себя только плату за электроэнергию, которая при постоянном электропотреблении на уровне 7,5 кВт•ч и тарифе 0,12 долл./кВт•ч за десять лет владения ЦОДом составит

7,5 кВт•ч × 24 ч/сут. × 365 сут./г. × 10 лет × 0,12 долл./кВт•ч = $78 840.

На самом деле операционные расходы гораздо больше, поскольку помимо платы за электричество включают еще по крайней мере стоимость аренды помещения, расходы на персонал и на амортизацию оборудования. Но давайте, как и автор, пренебрежем всеми расходами, кроме расходов на электричество, считая их равными в собственном и арендуемом ЦОДе.

Тогда суммарные расходы на эксплуатацию стойки в построенном ЦОДе уровня Tier III составят $100 000 + $78 840 = $178 840.

Если же мы будем арендовать стойку в аналогичном ЦОДе, то при арендной плате $2000 в месяц расходы за 10 лет составят 2000 долл./мес. × 12 мес./г. × 10 лет = $240 000.

Из этого автор делает вывод, что строить ЦОД уровня Tier III выгоднее, чем арендовать.

Далее автор сравнивает строительство и аренду стойки в центре обработки данных уровня Tier II. Оценивая расходы на строительство в расчете на одну стойку в $70 000, а месячную арендную плату в $1300, автор рассчитывает суммарные расходы за десять лет:

- $70 000 + $78 840 = $148 840 при строительстве;
- $1300 × 12 × 10 = $156 000 при аренде.

Опять получается вывод, что строительство выгоднее.

Сначала покритикую автора по мелочам – с точки зрения заказчика, работающего в Российской Федерации, использование доллара в качестве расчетной валюты выглядит странным. Еще более странен расчет долларового тарифа: автор берет рублевый тариф 3,60 руб./кВт•ч и переводит его в доллары по курсу 30 руб./долл. (на момент написания данной статьи доллар стоил 36,08 руб. – разница больше 20%).

Кроме того, непонятно, зачем в случае с Tier II автор анализировал не одну стойку, а две.

Ценность денег во времени

Теперь перейдем к самому главному – к неравноценности денег во времени, которая не учтена в расчете. Если ее учесть, результаты будут прямо противоположными!

Действительно, сумма x сегодня – это не то же самое, что сумма x через месяц: если сегодня есть свободные деньги, их можно инвестировать, разместив, например, на банковском депозите, если же денег сегодня не хватает, то можно получить кредит. При этом на банковский депозит через заранее оговоренные периоды начисляется процент, точно так же процент берется за пользование кредитом. Таким образом, при процентной ставке i сумма x сегодня эквивалентна сумме x(1 + i) через месяц. Через два месяца сегодняшние x руб. будут стоить x(1 + i)2 руб., а через n мес. – x(1 + i)n руб. Аналогично сумма y, уплачиваемая через n мес., эквивалентна сумме y/(1 + i)n, уплачиваемой сегодня**.

Если платежи за серверную стойку осуществляются ежемесячно в начале каждого месяца в сумме x руб., всего платежей n, а годовая процентная ставка i делится между месяцами равномерно, то современная ценность всего этого потока платежей равна

*Мартынюк А. Аренда ЦОДа или строительство? Грабли для CIO // «ИКС» № 4'2014, с. 66. Также на портале: www.iksmedia.ru.

**Подробнее о стоимости денег во времени можно прочитать, например, в Википедии: http://ru.wikipedia.org/wiki/Дисконтированная_стоимость или в книге Соловьев В.И. Финансы предприятий и домашних хозяйств. М.: Вега-Инфо, 2010. – http://visoloviev.ru/booksmath/Fin2010.pdf.

NPV = x + x/(1 + i/12) + x/(1 + i/12)2 + x/(1 + i/12)3 + ... + x/(1 + i/12)n – 1.

Вспомнив формулу для суммы первых n членов геометрической прогрессии с начальным элементом b1 = x и знаменателем q = 1/(1 + i/12), получим, что ценность рассматриваемого потока платежей равна

NPV = x [1 – 1/(1 + i/12)n]/[1 – 1/(1 + i/12)] = x[1 – (1 + i/12)–n](1 + 12/i).

В Microsoft Excel для расчета современной ценности такого потока платежей* используется функция

-ПС(<процентная ставка>;<число периодов>;<размер платежа>;;1).

Здесь минус перед формулой нужен потому, что в Excel вычисляется величина, противоположная NPV, последняя единица в формуле означает, что платежи осуществляются в начале каждого периода (если они производятся в конце периодов, вместо единицы нужно поставить ноль), в качестве процентной ставки за месяц, как правило, берется 1/12 годовой процентной ставки.

Для оценки суммарной стоимости владения стойкой в построенном центре обработки данных к капитальным затратам в размере $100 000 нужно прибавить не сумму всех операционных расходов, а их современную ценность – NPV.

Вычислим современную ценность потока ежемесячных платежей за электроэнергию в размере x = 7,5 кВт•ч × 24 ч/сут. × 30 сут./мес. в течение 10 лет (т.е. 120 мес.) при годовой процентной ставке i = 0,12 (и соответственно месячной ставке 0,12/12 = 0,01):

-ПС(0,12/12;120;7,5 × 24 × 0,12;;1) = $45617,60.

Таким образом, стоимость десятилетнего владения построенной стойкой будет равна $145617,60.

Современная ценность потока ежемесячных арендных платежей в размере x = $2000 в течение 10 лет (120 мес.) при годовой процентной ставке i = 0,12 (и соответственно месячной ставке 0,01):

-ПС(0,12/12;120;2000;;1) = $140 795,05,

т.е. аренда получается дешевле покупки!

Совершенно аналогично для ЦОДа уровня Tier II современная ценность операционных расходов при строительстве равна $45 617,60, вкупе с $70 000 капитальных затрат получаем

$70 000 + $45 617,60 = $115 617,60.

Современная ценность потока арендных платежей равна -ПС(0,12/12;120;1300;;1) = $91 516,79 – в этом примере аренда не просто дешевле строительства, а более чем на 20% дешевле.

Вопрос полезности перевода капитальных затрат в операционные вообще довольно тонкий. Идея такого перевода совсем не в том, что держать оборудование на балансе невыгодно, а в том, что если требования к ресурсам меняются, то при аренде можно заказывать ровно столько ресурсов, сколько нужно, а при покупке нужно купить ресурсов столько (или почти столько), сколько требуется при пиковых нагрузках, т.е., как правило, больше, чем нужно в среднем. Именно поэтому операционные расходы выгоднее: если мы разносим мороженое по пляжу, то нанимать персонал и арендовать тележки для перевозки мороженого только на летний период выгоднее, чем постоянно держать персонал в штате и тележки на балансе.

Если же количество нужного персонала и оборудования не изменяется в течение долгого времени, то выгоднее персонал нанять на постоянную работу, а оборудование приобрести и поставить на баланс.

Аналогично университетам часто бывает выгоднее не приобретать в собственность лицензии на программное обеспечение учебного процесса, а арендовать их: число студентов ежегодно меняется, и арендовать можно ровно такое количество лицензий, которое требуется.

В общем случае, естественно, выгодно арендовать те ресурсы, которые используются не постоянно и не на полную мощность.

Конечно же, и в случае вычислительных мощностей ЦОДов арендовать можно только то, что реально нужно, и потребности в арендуемом оборудовании не будут постоянно находиться на пике, поэтому взять в аренду можно столько стоек, сколько необходимо, и арендная плата будет еще меньше.

При сравнении вариантов сорсинга инфраструктурных решений учет прогноза потребности в эластичности ресурсов так же необходим, как и учет неравноценности денег во времени! ИКС

*В финансовой науке и практике такие потоки равных платежей с постоянной периодичностью называют рентами, а если платежи ежегодные – то аннуитетами.

Заурбек АЛЕХИН,
независимый консультант

Если бы ЦОД был самолетом...

Требования, предъявляемые обычно к центрам обработки данных, не уникальны. Сходными требованиями оперируют, например, в гражданской авиации. Попробуем сопоставить ЦОД с самолетом и понять, насколько наработки в области авиации применимы к созданию и эксплуатации дата-центров.

Основное требование к ЦОДу (точнее, к его инженерной инфраструктуре) сводится к тому, что объект должен обеспечивать работу размещенного в нем ИТ-оборудования и сохранность данных. Для этого основные инженер-

ные системы (в том числе электроснабжение и охлаждение) должны бесперебойно функционировать сами и поддерживать надежное функционирование предоставляемых ЦОДом услуг.

Как обстоит дело с соблюдением подобных требований в других областях? Какие методы используются? Как анализируется текущее состояние и обеспечивается эксплуатация? Ответы на эти вопросы могут помочь взглянуть на проблемные точки строительства и эксплуатации дата-центров со стороны и в итоге повысить надежность работы этих сложных объектов.

ЦОД и самолет: построение аналогий

Предназначение. Итак, будем сравнивать ЦОД с гражданским самолетом. Самолет предназначен для перевозки пассажиров из точки А в точку Б. При этом пассажиров следует удобно разместить, создать комфортные климатические условия, включая подачу чистого воздуха, предоставить воду, питание и т.д. И, безусловно, обеспечить безопасность перелета.

Инженерная инфраструктура дата-центра (включая машинный зал) предназначена для размещения ИТ-оборудования, предоставления электропитания, поддержания необходимых климатических условий (по крайней мере температуры и влажности). Конечно, полного совпадения нет, но если рассматривать ИТ-оборудование как пассажиров, а самолет – как инфраструктурный объект, определенные аналогии прослеживаются.

Ограничения по массе, объему, нагрузке. Фюзеляж всякого самолета имеет ограничения как по объему, так и по прочности. Количество кресел, а значит, и пассажиров строго ограничено. Кроме того, жестко лимитируется общая полезная нагрузка (вес). Причина простая: иначе не взлетит.

Если говорить о ЦОДе, то его машинные залы всегда ограничены по площади, фальшпол рассчитан на определенный вес размещаемого на нем оборудования, все инженерные системы имеют ограничения по мощности и другим характеристикам (это наиболее актуально для электроснабжения и охлаждения). Так что в данном аспекте аналогия с самолетом очевидна.

Четкие правила доступа. Чтобы попасть на борт самолета, необходимо не только предварительно купить билет, но и своевременно прибыть в аэропорт, пройти регистрацию, предполетный досмотр и посадку в самолет. Кроме того, каждый пассажир должен соблюдать правила авиаперевозок. Как, впрочем, и сама авиакомпания.

Наличие ограничений по безопасности в ЦОДе тоже не удивляет. Более того, здесь это одно из наиболее важных требований. В ЦОД никого просто так не пускают, для размещения техники необходимо согласовать и подписать договор, изучить и соблюдать правила допуска в помещения, установки, демонтажа и перемещения оборудования и т.д. Оговариваются и периоды посещений объекта. То есть в этой части совпадение почти полное.

Несколько классов обслуживания. «Экономический», «бизнес», «первый» – это наиболее часто используемые названия классов авиаобслуживания. Хотя фантазии у маркетологов авиакомпаний достаточно для того, чтобы увеличить количество этих классов в разы, но нам для понимания достаточно будет этих трех.

Что такое классы обслуживания, чем они различаются и что дают пассажиру? В действительности речь идет о различном объеме дополнительных удобств и/или услуг. Не более того. Следует помнить, что основная задача пассажирского самолета – перемещение пассажира из точки А в точку Б. И само перемещение независимо от класса обслуживания происходит совершенно одинаково: все пассажиры за одно и то же время будут перемещены из одного аэропорта в другой. За что же платят любители повышенных классов? За комфорт в ходе полета, индивидуальное обслуживание, дополнительные удобства, за более приятное окружение, за несколько большую безопасность, ну и, безусловно, за престиж.

А что же ЦОД? Как выглядит бизнес-класс по-цодовски с точки зрения потребителя его услуг? Примерно так же. Это может быть отдельный модуль или зал («первый класс») или выгородка в общем зале («бизнес-класс») или стойка в ряду ей подобных («эконом-класс»). Еще можно расширить для клиента допустимый временной диапазон для посещения и работы на объекте, предоставить выделенного менеджера для сопровождения. Все это принято именовать VIP-сервисом. Суть особо не меняется, и ЦОД успешно вписывается в предложенную модель.

Наличие службы летной эксплуатации (экипаж). Чтобы самолет взлетел, экипаж просто необходим. Кто-то должен вывести самолет на полосу, поднять в воздух, осуществлять контроль и корректировку маршрута в ходе полета и, конечно, совершить посадку. Кроме того, кто-то должен выполнять большое число незаметных для пассажиров операций в ходе полета, включая контроль различных параметров, их регулирование, связь с диспетчерами, реагирование на ситуацию в салоне и т.д.

ЦОДы пока тоже без дежурного персонала работать не могут. Конечно, мера ответственности, требования, да и напряженность работы дежурной смены ЦОДа отличаются от задач экипажа самолета, но в целом картина похожая: у ЦОДа есть свой экипаж, и он несет ответственность за «полет».

Постоянный контроль критичных систем. Самолет – очень сложный объект, содержащий большое количество разных систем, функционирование многих из которых критично для безопасности полета. Поэтому в ходе полета следует контролировать состояние систем и при необходимости принимать меры. Именно этим объясняется такое количество разнообразных приборов на самолетах прошлых поколений. В настоящее время приборов стало меньше, хотя количество контролируемых параметров возросло. Просто изменился способ визуализации, и значения параметров стали выводить на мониторы в более компактном и консолидированном виде.

ЦОД – тоже сложная система и тоже имеет свой обязательный набор параметров, подлежащих постоянному контролю. У любого современного ЦОДа есть тот или

иной вариант системы мониторинга, во многих работают развитые, передовые системы управления. Назначение этих систем вполне соответствует летным аналогам – контроль параметров для своевременного реагирования в случае достижения или превышения пороговых, предельно допустимых значений.

Сопровождение и обслуживание в полете («экипаж салона»). Бортпроводники – неотъемлемая часть гражданской авиации. Многие считают, что их основная функция – создание максимального комфорта пассажирам. В действительности же их ключевая задача – обеспечение выполнения пассажирами правил техники безопасности и оказание им помощи в случае любых чрезвычайных происшествий. А обслуживание – задача скорее вторичная, хотя и более заметная.

Вот с «бортпроводниками» в ЦОДах, честно говоря, не очень. Кстати, может быть, и напрасно – нам всем стоит подумать на эту тему. Тем не менее основная функция – контроль соблюдения внутренних правил объекта как собственным персоналом, так и представителями заказчиков и сервисных подрядчиков – силами дежурной смены все же реализуется.

Техническое обслуживание и плановый ремонт. ТОиР – важнейший элемент эксплуатации воздушных судов. Всякий самолет в обязательном порядке проходит предполетную подготовку перед каждым рейсом. Кроме того, широкий спектр профилактических и ремонтных мероприятий осуществляется в соответствии с графиком технического обслуживания в течение всего времени использования воздушного судна.

Оборудование инженерной инфраструктуры ЦОДа тоже подлежит регулярному техническому обслуживанию. Так что особой новизны в постановке задачи нет. В том, что касается реализации, дело обстоит несколько хуже. Конечно, то или иное обслуживание наиболее критичных систем проводится, но насколько оно соответствует требованиям и рекомендациям, не всегда очевидно. Особенно если учесть, что и сами рекомендации присутствуют в актуальном виде далеко не всегда – нормативные документы по этой теме отсутствуют.

Взлет и посадка. Для исполнения своего основного предназначения самолет должен покинуть пункт вылета и каким-то образом прибыть в пункт назначения. Взлет и посадка – наиболее важные этапы всего процесса, несущие в себе огромные риски. Более того, поднявшись на борт самолета, все пассажиры и экипаж фактически соглашаются с тем, что через какое-то время придется совершать посадку. И изменить это обстоятельство уже будет нельзя ни при каких условиях.

В сфере ЦОДов прямой аналогии взлету и посадке нет. Можно, конечно, искусственно довести модель до более или менее полного соответствия. Но для целей нашей статьи это не только не обязательно, но даже вредно. Поэтому оставим ситуацию как есть.

Резюме. Итак, нам удалось обозначить широкий набор соответствий и даже прямых совпадений между самолетом и дата-центром.

Нам также удалось найти по крайней мере одно существенное различие, связанное с необходимостью принятия определенного решения, которое несет в себе заметные риски, – это решение о взлете. Тем не менее, несмотря на определенный фатализм такого решения, редко кто из пассажиров всерьез над ним задумывается. Почему? Ответ очевиден: потому что все уверены в том, что взлетевший самолет сможет сесть и успешно выполнить свою миссию по перемещению пассажиров из точки А в точку Б.

Конечно, катастрофы с самолетами случаются. Но в целом безопасность авиаперевозок настолько высока, что мы, особенно не задумываясь, выбираем этот вид транспорта для путешествий. Почему?

О надежности самолетов

Как указывается в энциклопедии по авиации, *«надежность авиационной техники – это свойство летательного аппарата в целом и (или) его частей (конструкции, бортового оборудования, двигателей и др.) выполнять заданные функции, сохраняя значения эксплуатационных показателей в установленных пределах, соответствующих режимам и условиям использования, технического обслуживания, ремонта, хранения и транспортировки»**.

То есть самолет надежен настолько, что пассажиры могут не бояться за свою безопасность. На его надежность оказывает влияние как уровень надежности отдельных частей, так и особенности формирования из них единого изделия. При этом одна из особенностей состоит в том, что, несмотря на возможные отказы отдельных элементов, работоспособность всего изделия должна сохраняться на допустимом уровне. Для этого компоненты, потенциально подверженные отказам, резервируются.

Поскольку обеспечить полную безотказность всех деталей невозможно, происходящие отказы должны быть легко выявляемы и контролируемы, в первую очередь экипажем. Для наиболее опасных отказов предусматриваются способы предотвращения их отрицательного воздействия, включая изменение параметров работы отдельных агрегатов либо активацию аварийных систем.

Все происходящее на борту самолета регистрируется при помощи систем сбора полетной информации. И, наконец, обеспечивается эксплуатационная технологичность, т.е. создаются все условия для установления причин неисправностей, их устранения и предупреждения проявления.

Уровень надежности летательного аппарата и отдельных его компонентов оценивается рядом количественных показателей, характеризующих безотказность, долговечность и сохраняемость**. Помимо этого применяются комплексные показатели, отражаю-

---

*Авиация: Энциклопедия М.: Большая Российская энциклопедия, 1994.

**Сохраняемость – свойство изделия, устройства, сооружения непрерывно сохранять (в заданных пределах) значения установленных для них показателей качества во время и после хранения и при транспортировке; сохраняемость – одна из составных частей надежности.

щие готовность к вылету, регулярность и безопасность полетов, совершенство технического обслуживания.

С целью обеспечения надежности авиационной техники было создано целое научное направление. В качестве базы были применены количественные методы расчета и анализа, а также инженерные методы обеспечения надежности при создании и испытании изделий. В дальнейшем были сформированы комплексные программы обеспечения надежности, опирающиеся на научные методы проектирования, испытаний и эксплуатационной оценки надежности. Это позволило глубоко исследовать причины появления неисправностей и разработать технологии создания изделий с заданным и контролируемым уровнем надежности.

Управление надежностью осуществляется на всех стадиях жизненного цикла самолета. Так, на стадии проектирования:

- разрабатываются принципиально новые схемные решения, в том числе предусматривающие резервирование;
- выбираются оптимальные для последующего надежного функционирования рабочие режимы и условия работы;
- применяются специально создаваемые материалы с необходимыми характеристиками;
- формируются механизмы контроля при производстве и эксплуатации, способные обеспечить как диагностику, так и прогнозирование технического состояния.

На стадии производства используются передовые технологии и эффективные методы контроля.

Проведение специальных, ориентированных на проверку уровня надежности, испытаний как отдельных систем, так и построенного летательного аппарата в целом – еще одна важная стадия жизненного цикла.

На стадии эксплуатации:

- отслеживаются условия и режимы работы;
- обязательно выполняются предусмотренные профилактические работы;
- обеспечивается эксплуатационный контроль работоспособности;
- постоянно проводится анализ и устранение причин выявляемых отказов.

Как это все работает

Конечно, ключевой момент – наличие научных методов и обоснований. Но не менее важны и другие компоненты.

В первую очередь должно быть обеспечено **исполнение установленных требований и рекомендаций**. Для этих целей сформирована нормативная база надзорных органов (в настоящее время это Госавианадзор), а также система отраслевых и государственных стандартов. Так, только действующих отраслевых авиационных стандартов в настоящее время более 8000 (!).

Отдельно следует обратить внимание на **эксплуатационные документы,** которые в обязательном порядке разрабатываются и поддерживаются в актуальном состоянии для каждого самолета. Причем, как по летной, так и по технической эксплуатации.

Следующий элемент – **инфраструктура для осуществления проектирования, разработки, изготовления и испытания** авиационной техники. Сложно переоценить ее масштабы, особенно если учесть, что в современном пассажирском самолете количество деталей достигает нескольких миллионов.

Далее – **эксплуатационная инфраструктура.** Она тоже огромна. Всего в мире насчитывается более 40 тыс. аэропортов и отдельных взлетно-посадочных полос. Многие аэропорты осуществляют разнообразное техническое обслуживание.

И, наконец, **люди.** Практика показывает, что люди – наименее надежный и предсказуемый элемент. Для обеспечения надлежащего его уровня в нашей стране имеется не только Единый квалификационный справочник персонала организаций воздушного транспорта, но и целостная система подготовки и переподготовки таких специалистов.

Все перечисленное связано в единую комплексную систему, результатом функционирования которой и является возможность пользоваться авиационным транспортом, не опасаясь за свою жизнь.

А что если... Счастье возможно

Из сказанного выше следует, что в настоящее время в нашей стране существует и эффективно работает некая модель, которая обеспечивает высокий уровень надежности функционирования весьма сложной системы (самолета). При этом сколько-нибудь серьезных споров о целесообразности исполнения требований, сформулированных в рамках данной модели, не слышно.

В то же время надежность функционирования ЦОДов до сих пор под вопросом. Более того, говорить здесь о каком угодно варианте уверенности вообще пока не приходится. Мы в самом начале пути.

Закономерен вопрос: может быть, стоит воспользоваться наработками, имеющимися в авиационной отрасли, и применить их для отрасли ЦОДов? Результаты будут не только полезными, но и наконец-то дадут ответ на постоянно возникающие вопросы о реальной надежности создаваемых и/или уже существующих объектов.

Таким образом можно будет обеспечить полную прозрачность всего жизненного цикла ЦОДа и наличие подтвержденных научными расчетами значений параметров объекта, включая оценку его безотказности, ремонтопригодности, готовности и надежности. Также станет возможным осознанно управлять этими параметрами в соответствии с обоснованными потребностями и имеющимися возможностями конкретного потребителя услуг или владельца объекта.

Какой ценой можно достичь этого счастья?

Конечно, задача не простая, и определенные усилия приложить придется. Наиболее серьезного напряжения потребует **создание научной основы эксплуатации ЦОДа,** включая создание полноценной модели ЦОДа, описывающей все его элементы и взаимодействия, для проведения дальнейших расчетов и вычислений. Однако основные техники можно будет не изо-

бретать с нуля, а воспользоваться уже готовыми из практики других отраслей. Так, многие системы ЦОДа и происходящие в них процессы имеют те или иные аналоги в летательных аппаратах. А ввиду всеобъемлющего характера обеспечения надежности можно не сомневаться в наличии соответствующих научных разработок по ним.

Следующим шагом будет **формирование собственной нормативной базы.** Конечно, речь не идет о тысячах документов, но сегодня фактически нет ни одного. Это уж точно неприемлемо. С большой вероятностью удастся использовать уже имеющиеся документы, и не только из области авиастроения. Основные усилия придется направить на изучение имеющейся нормативной базы и определение ее применимости к ЦОДам.

Далее, предстоит сформировать **условия, при которых использование созданных нормативных документов будет необходимым для участников отрасли.** Вероятно, это наиболее сложный элемент. Но его удастся пройти легко в случае, если научные разработки будут качественными и смогут обеспечить необходимый уровень надежности, поскольку иметь уверенность в стабильности функционирования ЦОДа заинтересованы практически все потребители его услуг.

На фоне уже существующей модели обслуживания ЦОДов и снабжения их оборудованием создание **системы поставщиков,** готовых гарантировать качество услуг и надежность своей продукции в соответствии с жесткими требованиями и нормативами, не должно вызвать особых сложностей. Конечно, это потребует определенных усилий от всех участников и, вероятно, приведет к росту стоимости их продукции, но совокупный положительный эффект оправдает затраты как поставщиков, так и потребителей соответствующей продукции и услуг.

Последнее по счету, но не по важности – решение кадрового вопроса. Задача сложная, поскольку сегодня отсутствует система подготовки персонала для ЦОДов, но понятная и вполне реализуемая.

■ ■ ■

Изложенный выше подход и план сложны и не предполагают быстрого получения результата. Слишком уж многое предстоит сделать. Но поставленная цель тоже не сиюминутная, а ее достижение будет представлять ценность еще долгие годы.

Дорогу осилит идущий... ИКС

Распространение интернет-трафика

эволюция модели

Рост и изменение состава интернет-трафика трансформируют схемы его распространения и взаимоотношения между операторами, контент-провайдерами. На рынке появляются и растут новые игроки – IX и CDN. Как будет рынок меняться дальше?

Ярослав ГОРОДЕЦКИЙ,
генеральный директор,
CDNvideo

Призрак коммунизма

С момента возникновения интернета постоянно видоизменялись как состав интернет-трафика, так и схема его распространения. Лично я хорошо помню времена, когда люди пользовались Gopher вместо WWW, а непременным атрибутом договора между интернет-провайдером и клиентом было предоставление доступа к новостным группам Usenet.

В те времена российский интернет был устроен довольно просто. Для обеспечения зарубежной интернет-связности операторы побогаче строили собственные каналы на Запад, а победнее – покупали их у первых. Российская же связность была бесплатной: существовала московская точка обмена, где все российские операторы связи бесплатно обменивались трафиком («пирились»). Любой начинающий оператор сразу мог подключиться к этой точке обмена трафиком и получить бесплатно доступ ко всем российским интернет-ресурсам. Существовал практически цифровой коммунизм – для операторов действовал принцип «от каждого – по способности, каждому – по потребности».

Конечно, это не могло продолжаться долго – «звериный оскал капитализма» сделал свое дело, и в 2003 г. возникла ОПГ (отдельная пиринговая группа операторов), которая собрала на свои сети наиболее популярный российский контент и стала брать деньги с остальных операторов за доступ к нему. Одновременно операторы, входящие в ОПГ, строили магистральные интернет-каналы по всей России. Чтобы получать больше доходов, надо было их наполнить контентом. Стимулируя его локальное производство, операторы ОПГ стали предоставлять контент-провайдерам бесплатный доступ к своим сетям. Кстати, так возник чисто российский феномен бесплатного трафика для контент-провайдеров, который во многом способствовал развитию в России собственных сильных интернет-сервисов («Яндекс», Mail.ru и пр.). На межоператорском рынке в рамках от-

дельно взятого государства на несколько лет воцарилась бизнес-модель, при которой магистральные операторы продавали трафик операторам ШПД, а те, в свою очередь, – своим абонентам. Она очень похожа на бизнес-модель, работавшую в то же время на глобальном рынке, при которой операторы Tier 1 продавали свою связность всем.

Ветер перемен

Но, несмотря на стройность, логичность и иерархичность вышеописанной модели, она подверглась серьезному давлению со всех сторон и сейчас существует в гораздо более сложном окружении, чем раньше. С одной стороны, сами магистральные операторы связи стали выходить на рынок широкополосного доступа и конкурировать там с местными операторами связи, т.е. со своими же клиентами по IP-транзиту. Как следствие, местные операторы начали искать пути снижения зависимости от магистральных операторов связи. На существующий со стороны местных операторов связи спрос наложилось предложение. Появились новые игроки, так или иначе интегрировавшие значительные контент-ресурсы и предложившие местным операторам связи получать эти ресурсы напрямую, т.е. в обход магистральных операторов связи. К таким новым игрокам относились локальные и распределенные точки обмена трафиком (IX) и сети доставки контента (CDN). Расскажем подробнее об этих игроках, их бизнес-моделях, а также о доле трафика, которую они могут сэкономить местному оператору.

Локальные точки обмена трафиком

В регионах России локальные точки обмена трафиком стали развиваться примерно на рубеже 2007–2008 гг. Первые официальные точки обмена трафиком появились в виде проекта расширения деятельности московской точки обмена трафиком MSK-IX. Якорным клиентом этого проекта стал «Яндекс», заинтересованный в улучшении скорости доступа к своим ресурсам из регионов России. Параллельно в регионах возникали и местные точки обмена трафиком, в которых концентрировались местные ресурсы.

Сейчас в России точка обмена трафиком есть практически в каждом городе с населением больше 500 тыс. человек. Правда, активно работают далеко не все из них. Московская точка обмена трафиком (MSK-IX) пропускает свыше 1 Тбит/с и находится на 4-м месте в мире по объему пропускаемого трафика. Через нее, по оценкам экспертов, можно получить около четверти российского интернет-трафика. Региональные IX такими показателями похвастаться не могут – они пропускают от силы несколько десятков гигабит трафика. Вероятно, это связано с высокой концетрацией российского контента – в регионах не так много локального контента, а московские ресурсы, за исключением «Яндекса», предпочитают другие локализации.

Распределенные точки обмена трафиком

К 2010 г. в России появились распределенные точки обмена трафиком. Если бизнес-модель локальных точек обмена была заимствована Россией из мировой практики, то распределенные точки обмена – чисто российский феномен. Фактически они служат средством доступа к ряду популярных ресурсов (например, «ВКонтакте») по всей территории России. Таким образом, распределенные IX – нечто среднее между локальными точками обмена трафиком, предоставляющими связность в рамках города, и полноценными операторами связи, обеспечивающими полную связность.

Наиболее популярными распределенными точками обмена трафиком являются DataIX и W-ix. По оценкам экспертов, с их помощью можно получать также около четверти российского интернет-трафика, львиную долю которого составляет трафик «ВКонтакте».

Подключение как к локальным, так и к распределенным точкам обмена трафиком тарифицируется, стоимость платежей обычно в несколько раз ниже, чем стоимость услуг IP-транзита, но квант тарификации при этом гораздо грубее (обычно он кратен гигабитам или десяткам гигабит).

Сети доставки контента

На распределение трафика в интернете существенно влияют сети доставки контента (CDN). С их помощью можно локализовать контент, запрашиваемый клиентами, внутри сетей операторов связи, установив внутри сети кэширующие серверы, на которых находится часто пользователями контент. Это экономит трафик на магистральных каналах связи и ускоряет общую удовлетворенность пользователей качеством работы в интернете.

В России существует два крупных коммерческих оператора CDN, агрегирующих контент сотен клиентов, – это NGENIX и CDNvideo. Собственные CDN строят также некоторые крупные контент-провайдеры – это, в частности, ivi, Megogo и Google. Все они предлагают операторам возможность установки кэширующих серверов, каждый из которых способен сэкономить по нескольку процентов магистрального трафика.

Светлое будущее?

Таким образом, российские региональные операторы связи уже могут получать около половины интернет-трафика через точки обмена трафиком и через CDN, т.е. минуя сети магистральных операторов связи. В основном, это трафик видеосервисов (его получают как через IX, так и через CDN) и P2P-трафик, получаемый через IX (через CDN P2P-трафик не ходит). Есть все предпосылки к дальнейшему росту трафика видеосервисов, ведь люди все реже пользуются торрентами для просмотра кино, заменяя их на OTT-видеосервисы типа Netflix и ivi. По оценкам операторов связи, доля P2P-трафика в России составляет пока около 60%, но падает и продолжит падать – в Европе доля P2P-трафика сейчас – около 40%, а в США – всего 12%, там он практически вытеснен OTT-видеосервисами, которые используют CDN как средство доставки трафика. Вероятно, то же самое через несколько лет произойдет и в России.

Скорее всего, те OTT-видеосервисы, которые вытеснят P2P, будут использовать коммерческие или собственные CDN для распространения трафика, поэтому

доля трафика, распространяемого через CDN, может достичь 50–60%, как сейчас на Западе. Таким образом, основная доля интернет-трафика будет зарождаться в сети локального оператора связи и там же потребляться. Если эти прогнозы верны, основной точкой развития в ближайшие несколько лет станут интеллектуальные сети широкополосного доступа, способные предоставлять пользователю всю полноту контента из локального кэша с заданными параметрами качества, несмотря на то что он может быть связан с глобальным интернетом лишь относительно узким «бутылочным горлышком». Впрочем, это не удивительно – люди не любят искать контент и, в основном, смотрят то, что им предлагают. Так, более половины интернет-трафика порождается настройками по умолчанию компьютеров и других устройств. Вполне логично закэшировать этот и другой популярный контент в сети провайдера, лишний раз не загружая магистральные каналы связи. ИКС

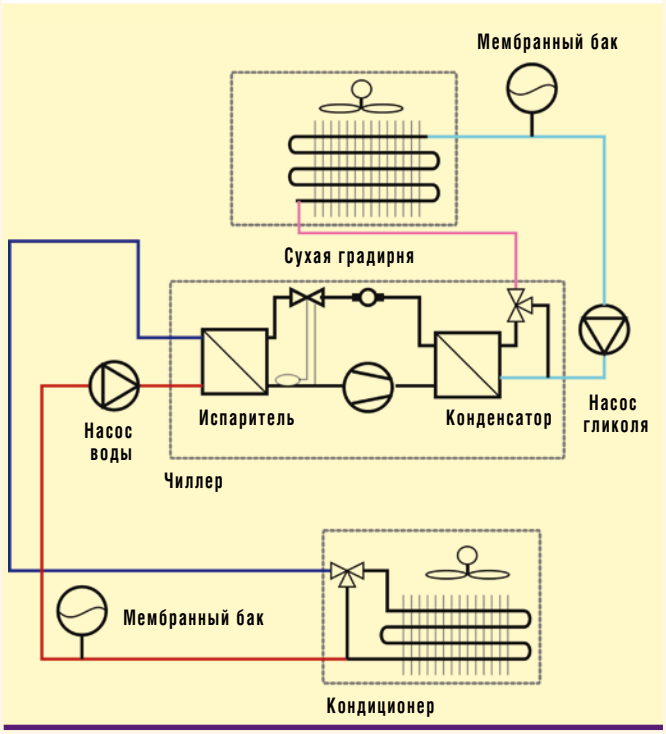
Тонкости проектирования элементов чиллерных систем

Михаил БАЛКАРОВ

Основной недостаток чиллерных систем – оборотная сторона их же достоинств: системы очень гибкие, поэтому при проектировании легко допустить ошибки.

Напомню, чиллерные системы, или, в отечественной терминологии, системы на охлажденной воде (один из вариантов показан на рис. 1), – это системы, использующие для охлаждения холодную жидкость. Она, в свою очередь, производится чиллером – по сути, обычным кондиционером, только с испарителем, отбирающим тепло у жидкости, а не у воздуха. В зимний период жидкость может охлаждаться напрямую, за счет холодного внешнего воздуха.

Рис. 1. Схема чиллерной системы



Типичный диапазон температур применяемой жидкости – 5–20°C. Помимо воды могут использоваться растворы этилен- и пропиленгликолей. Проходя через теплообменники кондиционеров, жидкость нагревается на 5–15°C и возвращается в чиллер.

Сам чиллер может быть как гликолевой схемы, что типично для систем с фрикулингом, так и воздушной. Размещаться он может либо в помещении, либо на улице (в этом случае обычно в виде моноблока, объединенного с теплообменником). Необходимыми элементами системы являются насосы для циркуляции воды по внутреннему и внешнему контурам и расширительные баки, обеспечивающие стабильность давления при изменениях температуры жидкости. Трехходовой клапан в кондиционерах управляет температурой теплообменника «вода–воздух», и, следовательно, производительностью кондиционера. Впрочем, клапан может быть и двухходовым, без байпаса. В этом случае схема содержит внешние элементы балансировки и обычно использует насос переменной производительности или еще один контур с собственным насосом переменной производительности.

Цель статьи – обратить внимание на ряд вопросов, вызывающих затруднения на практике.

Трубы

Сечение труб выбирается исходя из скорости потока около 1 м/с. На небольших отрезках этим правилом можно пренебречь. К примеру, если фланцы близко расположенного оборудования имеют меньший диаметр или необходимо выполнять нормативы по экранированию. Тем не менее скоростей выше 3 м/с следует избегать в любом случае, поскольку при них уже возможна механическая коррозия труб. Не рекомендуются и скорости намного ниже 1 м/с – в основном из-за роста стоимости труб и особенно арматуры. Кроме того, слишком низкая скорость чревата образованием воздушных пробок. Минимально допустимой обычно считается скорость 0,6 м/с.

Материалы труб сегодня могут быть самыми разнообразными. Углеродистая или нержавеющая сталь, медь, различные варианты пластика и металлопласта. К несомненным достоинствам пластика и меди, помимо очевидной коррозионной устойчивости, относится высокая гладкость внутренней поверхности, которая уменьшает гидравлическое сопротивление системы. Для труб малого диаметра из металлопласта широкое распространение получили обжимные элементы в виде тонкой металлической гильзы, которые при монтаже запрессовываются на трубе клещами.

Оцинкованные трубы нельзя применять в системах с гликолем – присадки моментально разъедают цинк и при этом расходуются.

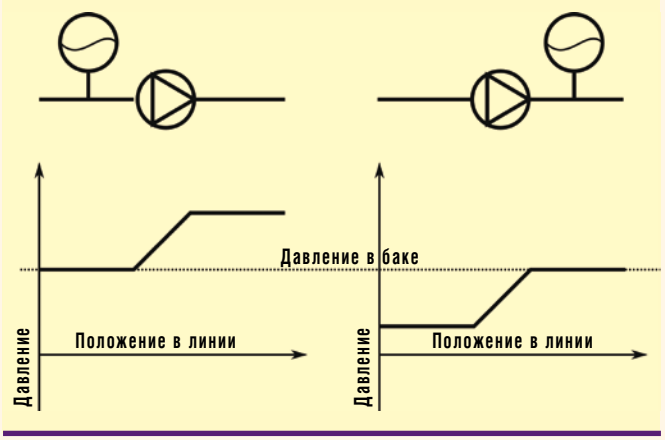
Между разнородными металлами обязательно должна быть предусмотрена гальваническая развязка, иначе не избежать проблем с коррозией.

Также обязательно нужно учитывать коэффициент температурного расширения материала труб, при необходимости устраивая эластичные фланцы или петли для его компенсации. Наибольшие проблемы в этом отношении вызывают некоторые пластики.

Исходя из опыта, рекомендую металлопласт покупать самый дорогой: только единицы производителей в мире выпускают трубы, которые не расслаиваются через несколько лет эксплуатации.

Несмотря на определенную эластичность металлопластовой трубы, минимальный радиус изгиба (используйте специальный инструмент), к примеру, у дюймовой – 30 см. Поэтому для низкого фальшпола в месте поворота потребуется применять специальный угловой фитинг.

Рис. 2. Изменение давления в работающей системе в зависимости от места установки мембранного бака



Впрочем, подвод воды в серверные может осуществляться и сверху, успешный опыт эксплуатации таких решений есть. Основная проблема в этом случае – традиционная водобоязнь. На практике же вероятность повреждения сплошной металлопластовой трубы минимальна, а заключение ее во вторичный лоток или короб практически полностью устраняет даже гипотетическую опасность протечки. Единственная проблема, с которой действительно пришлось столкнуться, – образование, а

Как избежать ошибок при проектировании систем холодоснабжения

Виктор ГАВРИЛОВ,
технический директор,
«АМДтехнологии»

При разработке систем холодоснабжения ЦОДа на базе холодильных машин зачастую допускаются серьезные ошибки, которые могут сильно повлиять на работоспособность системы в целом. Так, выбирая моноблочный чиллер со встроенным гидравлическим модулем, заказчик нередко считает, что получит законченное изделие, готовое к эксплуатации, которое нужно просто подключить к системе трубопроводов, но забывает о проведении гидравлического расчета. В результате свободного напора насоса, встроенного в чиллер, может оказаться недостаточно для преодоления гидравлического сопротивления сети. Большинство производителей могут укомплектовать холодильную машину насосами с необходимыми для конкретного проекта характеристиками, но для этого надо предварительно выполнить гидравлический расчет и указать при заказе оборудования требуемый свободный напор насоса.

Следует также обращать внимание на тип уплотнения насоса. Оно должно быть рассчитано на работу с гликолем. Ошибки встречаются и при выборе диаметра магистральных трубопроводов. Иногда при этом руководствуются присоединительными размерами трубопроводов холодильной машины. Это неверно – необходимый диаметр магистрального трубопровода определяется гидравлическим расчетом, исходя из допустимой скорости движения жидкости. Не стоит забывать и об обязательной установке на входе в чиллер грязевых фильтров с надлежащим размером ячейки фильтрующего элемента. Отсутствие или неверный подбор фильтра может привести к загрязнению испарителя и снижению холодопроизводительности машины.

На начальном этапе проектирования нужно выбрать гидравлическую систему с постоянным или переменным расходом. От этого будет зависеть выбор типа балансировочных клапанов: статических либо динамических, применение трех- или двухходовых клапанов. Система с постоянным расходом проще в проектировании и эксплуатации, однако системы с переменным расходом позволяют дополнительно снижать затраты на электроэнергию при частичной загрузке ЦОДа.

Все упомянутое – лишь малая часть нюансов, которые могут возникнуть при проектировании системы холодоснабжения и которые необходимо учитывать. Для получения работоспособной, энергоэффективной системы с высоким уровнем надежности следует выбирать профессиональные инжиниринговые компании, работающие на рынке строительства центров обработки данных.

затем падение вниз капель конденсата при повреждениях теплоизоляции. Поэтому лоток под трубами – обязательный элемент при таком подводе. Вместо лотка можно использовать дешевые тонкие пластиковые трубы большого диаметра, разборные пластиковые короба или же обертку из палаточной ткани со шнуровкой.

Собственно, качественная теплоизоляция труб и остальных элементов системы обязательна при любом варианте прокладки. Иначе образование луж конденсата и интенсивная коррозия металлических деталей при определенных условиях гарантированы. Единственные элементы системы, где от этого правила можно отказаться, – герметичные шкафы.

Системный эффект

Рассматривая гидравлику, нельзя обойти вниманием так называемый системный эффект. Он заключается в изменении падения давления потока за счет взаимного влияния близко расположенных последовательных элементов. В общем случае это явление вредное, хотя для жидкости оно обычно уменьшает суммарное падение давления по сравнению с падением на каждом из элементов в отдельности. Приведем несколько примеров из практики, в которых именно системный эффект приводил к проблемам.

- После поворота подающей трубы большого диаметра с заметным расходом давление и, следовательно, расход на близко расположенном отводке практически отсутствуют.
- Центральные насосы в группе, объединенные на коллекторе недостаточного диаметра, запирают крайние, в итоге расход получается значительно меньше формальной суммы производительностей.
- Ближайшие к концу линии насосы слива конденсата при недостаточном диаметре труб запирают дальние. При обратном порядке включения все на удивление может работать нормально. Как легко догадаться, эта проблема может возникнуть в любых системах кондиционирования, не только чиллерных. Поскольку конденсат может появиться даже в системах охлаждения, ориентированных на его отсутствие.

Мембранный бак

Мембранный (расширительный) бак представляет собой герметичную емкость с эластичной диафрагмой, с одной стороны присоединенную к магистрали теплоносителя, а с другой накачанную газом под давлением. Он выполняет ряд функций.

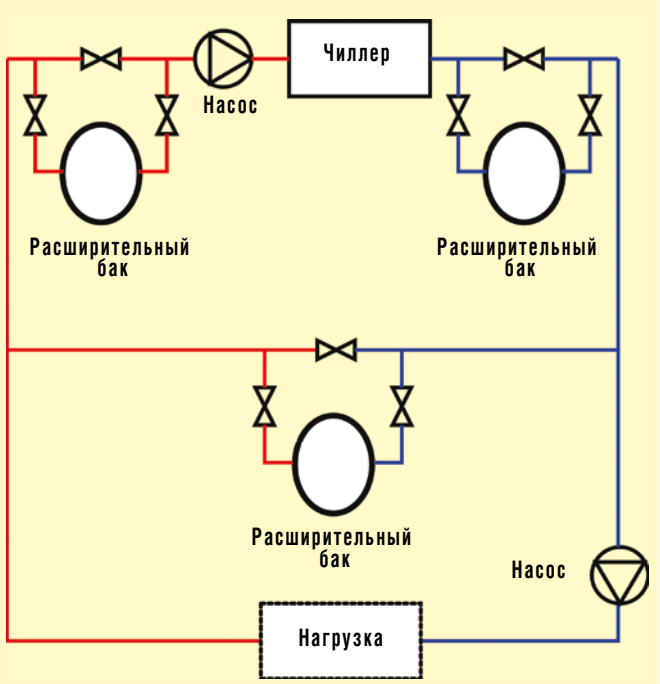
- Поддержание стабильного давления при изменении температуры жидкости в системе. При отсутствии возможности расширения с ростом температуры давление в жидкости нарастает очень быстро.
- Поддержание избыточного давления в системе. Именно для этого мембранный бак достаточно часто устанавливают сверху. В этом случае достаточно 1,5 бар, чтобы во всей системе давление с гарантией было выше атмосферного и в результате уплотнения оставались герметичными, а насосы работали без проблем. Тем не менее при некотором увеличении объема и рабочего давления его вполне можно располагать внизу.
- Компенсация скачков давления при запуске насосов. С этой целью бак устанавливается сразу на выходе насосов. Отмечу, что такой подход, как правило, нерационален – гораздо целесообразнее использовать либо несколько мелких насосов, включаемых по очереди, либо насосы с плавной регулировкой оборотов, либо же специализированные компенсаторы гидроударов, представляющие собой компактный цилиндр с поршнем внутри.

Объем бака зависит от общего объема системы, проектных давлений и температур, а также концентрации раствора гликоля, поскольку у разных концентраций растворов разные коэффициенты теплового расширения. Для нормального функционирования бак должен быть накачан газом под необходимым давлением, а в проекте системы, разумеется, должны быть приведены расчеты его объема с указанием проектных температур и давлений.

Мембранный бак является условно нулевой точкой системы – в норме давление в месте его установки при включении и выключении насосов не меняется. С этим, в частности связана нецелесообразность его расположения после насосов: работающие насосы при расположении бака после них не повышают давление в системе, а, наоборот, понижают перед собой (рис. 2, предполагается, что насосы и баки используются идентичные), что может привести к ранее упомянутым проблемам с низким давлением.

Накопительный бак – это емкость или набор емкостей проектного размера, обеспечивающие требуемый запас жидкости для непрерывной работы при пропадании основного электроснабжения.

Рис. 3. Варианты расположения накопительного бака в чиллерной системе



Еще одна задача бака – поддержка работы при выключенном чиллере, если нагрузка на систему слишком мала относительно его возможностей регулирования мощности. Чиллер по принципу работы тоже является компрессорной холодильной машиной и, следовательно, не может работать долгое время на нагрузке, отличной от номинала, а после выключения снова сразу включиться. Разумеется, минимальный объем накопительного бака в системе должен обеспечивать 5 мин работы. Впрочем, во многих системах такое время достигается просто за счет объема жидкости непосредственно в трубах. Производители чиллеров в документации обычно указывают минимально допустимый объем системы. Собственно, чем больше бак, тем точнее поддерживается заданная температура воды.

В баке также происходит отделение растворенных газов за счет малой скорости движения жидкости. По этой же причине – иногда неожиданно для проектировщиков и службы эксплуатации – бак является фильтром тонкой очистки. В нем оседают вся ржавчина и прочие взвеси, собираемые в системе. Поэтому обязательно следует предусматривать сливной кран на днище бака и воздухоотделитель на его крышке. Как, впрочем, требуется устанавливать и байпасную линию, позволяющую отключать бак от системы на время чистки.

Бак может располагаться как перед чиллером – для улучшения работы при малой нагрузке и лучшего выделения растворенных газов, так и после, что обеспечивает значительно большее время автономной работы. В обоих вариантах требуется интенсивное перемешивание воды в баке, для того чтобы обеспечивать именно инерционность, а не просто временную задержку. Однако оптимальная схема подключения – параллельно чиллерам, при этом конструкция бака, наоборот, должна исключать перемешивание. Все эти варианты изображены на рис. 3.

Баки, а также их опорные стойки должны быть тщательно теплоизолированы.

Емкость бака в первом приближении должна соответствовать штатному расходу воды системы на требуемое время автономии. Если же инсталляция не позволяет применять баки большого объема, то можно установить льдогенератор. Это устройство с отдельным маленьким чиллером, создающее в баке запас льда. Он может оказаться полезным и для компенсации краткосрочных пиковых нагрузок, к примеру в жаркие летние дни, или в случае разницы дневного и ночного тарифов на электроэнергию. Вместо генерации льда можно использовать охлаждение до низких температур запаса раствора гликоля, но это менее эффективно с точки зрения объема и веса установки.

Еще одно применение накопительного бака – замена жидкости без остановки системы. Баки осекаются, сливаются и моются. После чистки баки заполняются водой и снова подключаются к системе. По истечении удвоенного времени автономной работы на баках раствор в системе достаточно равномерно перемешается. В зависимости от полученной в итоге концентрации раствора процедуру можно повторить. В итоге система окажется заполненной почти чистой водой. После этого для гликолевого контура в баки-накопители заливается раствор более высокой концентрации в расчете на разбавление чистой водой, уже находящейся в трубах. ИКС

Оптические тракты параллельной передачи

методы поддержания полярности

Одновременное использование параллельной передачи и классических двухволоконных схем обусловливает необходимость поддержания правильной полярности многоволоконных оптических трактов. Таковая обеспечивается корректным выполнением проекта на основе стандартной серийной элементной базы или специальных разработок.

Андрей СЕМЕНОВ,
директор по развитию,
RdM Distribution,
докт. техн. наук

В современных ЦОДах широкое распространение получила оптическая техника, причем при скоростях обмена данными на уровне десятков гигабит в секунду применяется схема параллельной передачи по нескольким волокнам. Однако по меньшей мере до 2020 г. наряду с параллельной многоволоконной передачей в дата-центрах будет продолжать использоваться классическая двухволоконная схема. Переход от двухволоконной к параллельной передаче должен происходить бесшовно и осуществляться без замены линейного кабеля. Это обстоятельство заставляет обращать особое внимание на обеспечение корректного подключения друг к другу приемника и передатчика сетевых интерфейсов на разных концах линии. Комплекс встающих при этом вопросов носит название задачи поддержания правильной полярности.

Особенности поддержания полярности

Корректное подключение приемников и передатчиков разных концов линии двухсторонней связи может быть обеспечено разными путями. Главное средство решения этой задачи – реверсирование отдельных це-

Табл. 1. Исполнение элементной базы для реализации разных методов подключения в случае формирования дуплексных оптических трактов

Метод подключения	Элемент группового соединителя		Дуплексный коммутационный шнур
	Кабельная вилка	Розетка	
A	A	A	Один прямой (A-to-B), один обращенный (A-to-A)
B	B	B	Прямой (A-to-B)
C	C	A	Прямой (A-to-B)

пей передачи сигнала в шнурах и кабелях стационарных линий. Это осуществляется двумя основными способами.

Первый способ – прямое физическое скрещивание отдельных цепей передачи сигналов в кабельном изделии: концы световодов заклеиваются на различные посадочные места вилок соединителей. Характерный признак такого решения – волокна в вилках разъемных соединителей на разных концах при одинаковой пространственной ориентации имеют различную нумерацию.

Второй способ не меняет раскладки световодов в наконечнике вилки, он основан на том, что стандартные для ЦОДа оптические соединители LC и MPO строятся по симметричной схеме, т.е. содержат проходную розетку и две вилки, вставляемые в ее гнезда. Это дает возможность добиться эффекта скрещивания за счет обычного разворота на 180° вокруг продольной оси одного из гнезд розетки, а вместе с ним и вставленной в него вилки, что эквивалентно изменению порядка следования волокон.

Необходимость дополнительно сосредоточиться на обеспечении правильной полярности для двухволоконных трактов возникает из-за массового использования в кабельных системах ЦОДов стационарных линий, ориентированных на схему параллельной передачи. При организации линейных трактов используются оптические соединители группового типа. Их внедрение резко увеличивает количество физически возможных вариантов соединения цепей передачи сигнала, что должно быть учтено при выборе схемы организации связи. Ситуацию несколько облегчает то, что подключение вилки к розетке возможно только в одном положении, заданном кодирующим выступом на вилке и вырезом на розетке.

Указанные особенности и достигнутый уровень техники однозначно указывают на то, что обеспечение правильной полярности возможно и на основе серийной элементной базы. Существенными дополнительными условиями становятся корректное выполнение проекта построения СКС и соблюдение правил эксплуатации кабельной системы.

Что говорит стандарт

Необходимость дополнительных мер по поддержанию правильной полярности трактов параллельной передачи была осознана еще при создании первых многоволоконных разъемных соединителей. На нормативном уровне способы решения данной задачи были впервые зафиксированы в американском стандарте ANSI/TIA-568-B.1-7. Этим документом были введены три метода обеспечения корректности построения цепей распространения сигнала от передатчика к приемнику, обозначаемые буквенными индексами A, B и C. Главные различия этих методов заключаются в исполнении отдельных компонентов, последовательное соединение которых образует тракт. При этом часть компонентов оказывается одинаковой (табл. 1 и 2), что уменьшает номенклатуру поставляемой продукции.

Табл. 2. Нумерация световодов в вилках 12-волоконных соединителей типа MPO в зависимости от типа коммутационного шнура (вид на торцевую поверхность, «ключ вверх»)

Тип шнура	Конец	Номера световодов											
	Ближний	1	2	3	4	5	6	7	8	9	10	11	12
B	Дальний	12	11	10	9	8	7	6	5	4	3	2	1
A	Дальний	1	2	3	4	5	6	7	8	9	10	11	12
C	Дальний	2	1	4	3	6	5	8	7	10	9	12	11

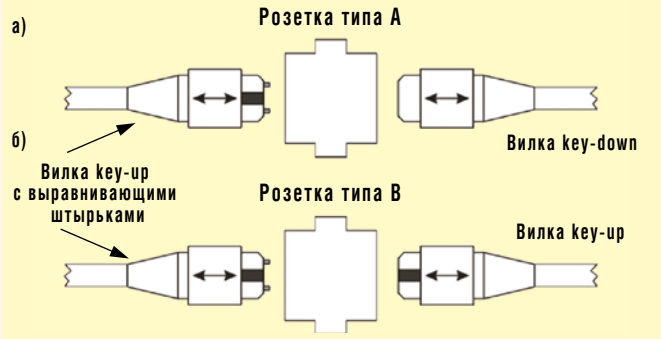
Практическая ценность стандарта ANSI/TIA-568-B.1-7 увеличивается тем, что положения нормативной части этого документа могут без ограничений распространяться на дуплексную схему организации связи.

Ни один из перечисленных методов не является предпочтительным. Тем не менее анализ табл. 1 показывает, что для текущей эксплуатации оптической подсистемы целесообразно обращение к методу B. Основное его достоинство – максимально полная универсализация элементной базы пользовательских компонентов, т.е. шнуровых изделий и интерфейсов коммутационных панелей. Этим определяется его наибольшее распространение на практике.

Стандартные обозначения отдельных компонентов тракта

В действующей нормативной базе учитывается использование в составе тракта симметричных групповых оптических соединителей, вилки которых могут соединяться друг с другом в двух положениях: нормальном и обращенном.

Рис. 1. Варианты соединения вилок разъемов MPO в проходной розетке: а) конфигурация типа A; б) конфигурация типа B



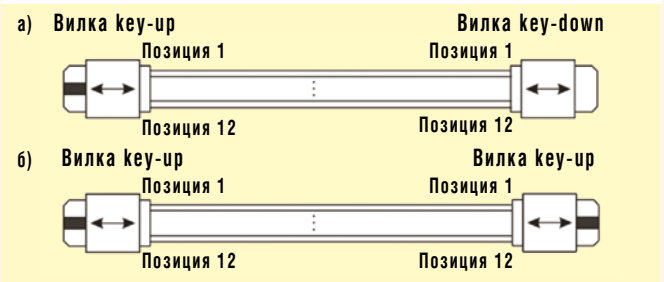
Вилка имеет единственное исполнение. За счет этого конкретный тип соединения во многом определяется разновидностью применяемой розетки. Сама розетка позволяет подключать к ней вилку только в одном положении. В стандартах она обозначается англоязычными терминами key up («ключ вверх») и key down («ключ вниз»), отражающими несимметричную форму поперечного сечения вилки и ее положение в розетке в рабочем состоянии.

Для конкретизации понятий «верха» и «низа» считается, что волокна вилок стандартных соединителей при взгляде на торцевую часть их наконечников располагаются вдоль горизонтальной прямой линии. Возможность ее вертикальной ориентации, в отличие от офисных СКС, в действующих редакциях стандартов для ЦОДа не предусмотрена.

В дуплексных изделиях типа LC несимметричность появилась из-за исполнения фиксатора в виде односторонней внешней рычажной защелки. В групповом изделии MTP/MPO эта конструктивная особенность введена в дизайн корпуса формированием на одной из сторон вилки ключевого выступа. В обоих случаях защелка и выступ взаимодействуют с соответствующим пазом розетки.

Панельный компонент разъема с расположением вырезов под направляющие компоненты вилок на противоположных сторонах гнездовых частей корпуса обозначается как розетка типа А (рис. 1а) и предназначен для обращенного соединения (key up to key down). Соответственно, аналогичные изделия с расположением вырезов на одинаковых сторонах корпуса относятся к типу В. В этом случае вилки включаются в розетку в развернутом на 180° относительно друг друга положении (рис. 1б), обеспечивая реверсирование волокон.

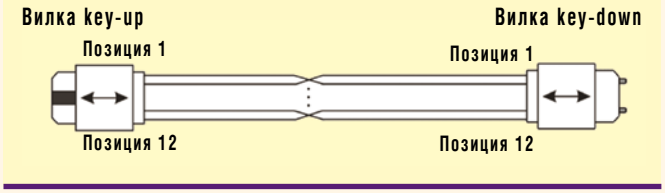
Рис. 2. Разновидности многоволоконных оптических коммутационных шнуров:
а) шнур типа В (key-up to key-down); б) шнур типа А (key-up to key-up)



Многоволоконные коммутационные шнуры первоначально были представлены двумя разновидностями (тип А и тип В, рис. 2). В шнуре типа А вилки ориентированы ключевыми выступами в противоположные стороны, для вилок шнура типа В принята одинаковая ориентация. Соответственно меняется нумерация волокон (табл. 2).

Стандарт ANSI/TIA-568-C.3 вводит третий тип коммутационного шнура – С (рис. 3). Вилки в нем ориентированы, как в шнуре А, а различие состоит в применении внутреннего скрещивания волокон каждой пары,

Рис. 3. Многоволоконный оптический коммутационный шнур типа С



что вообще представляет собой характерный отличительный признак изделий группы С.

Транковые кабели с точки зрения раскладки волокон в вилках не отличаются от коммутационных шнуров, что позволяет распространить на них систему обозначений, которая изначально была принята для последних.

При работе на скоростях до 10 Гбит/с включительно по традиционной двухволоконной схеме необходимы дуплексные коммутационные шнуры. Обращенный (нескрещенный) шнур обозначается как «шнур А–В» (A-to-B), нормальному прямому шнуру с внутренним скрещиванием волокон присваивается обозначение «шнур А–А» (A-to-A) (рис. 4а и 4б соответственно).

Метод А

При реализации метода А в линейной части используются транковый кабель и розетки типа А. Последовательность подключения симплексных коннекторов разветвительного шнура к розеткам коммутационного устройства на обоих сторонах стационарной линии одинакова. Очевидное преимущество этого метода в том, что на всех коммутационных панелях с пользовательской стороны сохраняется однотипная ориентация и нумерация розеток коммутационных портов.

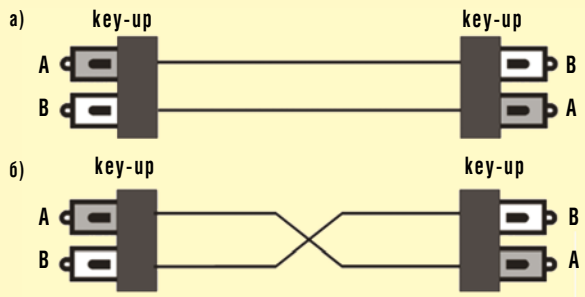
Метод А для дуплексной схемы передачи сигнала предполагает применение прямого и обращенного коммутационных шнуров на разных концах тракта. В системах параллельной оптики вилки транкового кабеля устанавливаются на него в оппозитном положении, т.е. key down и key up. Восстановление ориентации сигнала осуществляется за счет применения на разных концах тракта различных коммутационных шнуров: типа А и типа В.

Метод В

Метод В отличается наиболее сложной структурой стационарной линии. В качестве пользовательского интерфейсного компонента стационарной линии используются розетки типа В. Они устанавливаются с разных сторон тракта в положениях key up и key down. В линейной части применяется транковый кабель типа В со скрещенными световодами.

Выбор ориентации направляющего выреза розетки для конкретного коммутационного устройства (при возможности ее изменения) находится в компетенции системного архитектора. Положение выреза вверх целесообразно применять в коммутационных устройствах, устанавливаемых в зонах более высокой ступени иерархии инфраструктуры аппаратного зала. В случае одинаковых значений этого параметра, что харак-

Рис. 4. Основные разновидности дуплексных оптических коммутационных шнуров:
а) шнур типа A-to-B (прямой шнур); б) шнур типа A-to-A (обращенный шнур)



терно для резервных линий, используется обычное правило «восток – запад».

При реализации метода B отдельные вилки разветвительного шнура одного из концов стационарной линии подключаются к внутренней части розеток концевой панели в инверсном направлении. При такой раскладке в пределах стационарной линии происходит тройное обращение сигнала каждой пары световодов, а соответствующие им розетки на разных концах стационарной линии меняются местами при приеме и передаче сигнала. Вилки транкового кабеля устанавливаются на него с одинаковой ориентацией. Сам кабель не имеет внутреннего скрещивания отдельных световодов. Коммутационные шнуры относятся к обращенному типу. Сильная сторона этой конфигурации – применение однотипных коммутационных шнуров на разных сторонах тракта.

Метод C

Метод C реализуется, когда формируемая линия изначально предназначена для поддержки дуплексной схемы передачи сигнала. В его основу положено применение однотипных дуплексных шнуров типа A-to-B на разных концах тракта. Для правильного распределения сигнала по отдельным розеточным модулям дуплексного соединителя используются розетки типа A, а также транковый кабель типа C, скрещивание ленты световодов которого достигается разворотом одной из вилок MTP/MPO на 180°. Характерной особенностью линейного изделия данной разновидности является то, что внутри него каждая пара световодов дополнительно скрещивается.

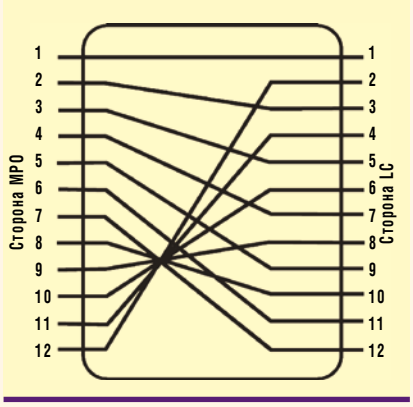
Отдельные вилки разветвительного шнура подключаются к внутренней части розеток одной из концевых панелей в «прямом» направлении. При такой раскладке в пределах стационарной линии происходит одинарное обращение сигнала каждой пары световодов. При этом сами розетки каждой пары на разных концах стационарной линии не меняются местами при приеме и передаче сигнала и имеют одинаковую ориентацию ключевых вырезов (тип B).

Оригинальные разработки

Методы A – C носят общий характер и инвариантны к исполнению оконечных участков стационарных линий. Это открывает перспективы улучшения технико-экономических характеристик решения за счет специализации и устранения функциональной избыточности.

Функцию адаптера, обеспечивающего правильную полярность, можно легко возложить на кассеты модульного типа, широко применяемые в параллельной оптике. Подобное решение было доведено до уровня серийного продукта в двух довольно схожих вариантах: в обоих применяется принудительное разделение световодов на приемные и передающие с последующим объединением в составе 12-волоконной ленты. Основное различие решений – в количестве 12-волоконных лент линейного кабеля, задействованных в процессе формирования стационарной линии.

Рис. 5. Разветвительная кассета Corning



Основной целью нововведений является устранение главного недостатка стандартных методов A – C, невозможности добиться полностью симметричной структуры оптического тракта в общем случае его использования как для дуплексной, так и для параллельной передачи.

Решение компании Corning Cabling Systems базируется на одной 12-волоконной ленте и известно как «универсальный системный метод» (Plug & Play Universal Systems Method). Схема внутренней разводки реализующей его кассеты изображена на рис. 5. Решение на основе двух 12-волоконных лент, одна из которых работает только на прием, а вторая – исключительно на передачу, внедрено швейцарской компанией Reichle & De-Massari. Оно также не предусматривается действующими редакциями нормативных документов и продвигается на рынке под названием метода S.

Оба метода позволяют применять на концах линии однотипные коммутационные шнуры.

■ ■ ■

Наличие набора стандартизованных компонентов для создания стационарных линий и трех структур, формируемых на их основе, позволяет обеспечить правильную полярность многоволоконных оптических трактов при сохранении высокой проектной гибкости решения в целом. Для поддержания правильной полярности высокую эффективность показали также специальные разработки.

В качестве основного типа транкового кабеля целесообразно применять изделия типа B; обращение к ним заметно упрощает как построение, так и эксплуатацию кабельной системы за счет возможности использования однотипных коммутационных шнуров в СКС, охватывающих все зоны ЦОДа. ИКС

Онлайн-ИБП большой мощности

Модели серии Vanguard – VRT-6000 и VRT-10K мощностью 6 и 12 кВА соответственно – ИБП с двойным преобразованием (характеризуются нулевым временем переключения на аккумуляторы), предназначенные для защиты серверного, сетевого, телекоммуникационного оборудования, которое устанавливается в стандартную 19-дюймовую стойку и требует высокого качества электропитания.

Модели выпущены в стоечном варианте, блок ИБП и батарейный модуль имеют высоту 3U каждый. Максимальное время батарейной поддержки в стандартной комплектации составляет 15–10 мин соответственно. Увеличить показатель можно за счет подключения дополнительных аккумуляторных блоков. Доступны батарейные блоки со встроенными выходными розетками (4 × IEC320 C13 + 4 × IEC320 C19) или дополнительным зарядным устройством.

ИБП серии VRT имеют коэффициент мощности, равный 0,9, обеспечивают синусоидальную форму выходного напряжения и допускают «горячую» замену АКБ.

Поддерживаются режим высокой эффективности и функция аварийного отключения EPO (например, для пожарной сигнализации). Модели оснащены многофункциональным ЖК-дисплеем с меню на русском и английском языках, а также портами USB и RS-232 и внутренним слотом SNMP-карты для организации удаленного управления и мониторинга.

Powercom: +7(495) 651-6281

Комплект для высокоскоростного подключения абонентских устройств

HD Kit Ethernet – кабельное HD-решение, обеспечивающее передачу данных между абонентским терминалом (ONT) и мультимедийными устройствами со скоростью до 100 Мбит/с, представлено в двух комплектациях.

Вариант для самостоятельной установки абонентом состоит из катушки с 20-метровым ультратонким (диаметром 2,3 мм) кабелем «витая пара» категории 5e, двух абонентских розеток под стандартный разъем RJ45, а также двух ультрагибких патч-кордов длиной 2 м каждый. Для подключения абонентского устройства не требуется никакого дополнительного инструмента: розетки оснащены прокалывающими зажимами с цветовой маркировкой. Кабель крепится к стене клеем, степлером или стандартными пластиковыми клипсами.

Вариант для компаний-инсталляторов, которые производят подключение абонента к сети, содержит катушку с кабелем «витая пара» категории 5e длиной 70 м, шесть абонентских розеток под разъем RJ45 и шесть ультрагибких патч-кордов.

Представительство ACOME в России: +7 (921) 904-2015

Дисплеи для видеостен

TH-47LFV5W и TH-55LFV5W – дисплеи диагональю 47” и 55” соответственно. Соотношение сторон – 16:9. Дисплеи снабжены D-LED подсветкой и антибликовым покрытием. Поддерживаемое разрешение – FullHD 1920 × 1080, углы обзора по горизонтали и вертикали – 178°. Контрастность – 1400:1, динамическая контрастность – 500 000:1. Время отклика – 10 мс.

Настраиваемая яркость изображения (500–800 кд/кв. м) дисплеев позволяет использовать их как внутри помещений, так и на витринах, освещаемых ярким солнцем. Благодаря возможности вертикальной установки и тонкому шву между соседними панелями (5,3 мм) могут применяться для построения видеостен. Управление может осуществляться удаленно через веб-браузер.

Энергопотребление – 220 Вт. Дисплеи сохраняют работоспособность в температурном диапазоне 0–40°C при влажности 10–90% (без образования конденсата). Время наработки на отказ около 60 тыс. часов (при условии уменьшения яркости до половины максимального значения).

Panasonic: +7(800) 200-2100

Реклама в номере

АБИТЕХ
Тел./факс: (495) 234-0108
www.abitech.ru . . . с. 77

АМДТЕХНОЛОГИИ
Тел.: (495) 963-9211
Факс: (495) 225-7431
E-mail: info@amd-tech.ru
www.amd-tech.ru . . с. 89

ИК ГУЛЛИВЕР
Тел/факс: (495) 663-2172
E-mail: info@ikgulliver.ru
www.ikgulliver.ru . . с. 79

SONY ELECTRONICS
Тел.: (495) 258-7667
Факс: (495) 258-7650
www.pro.sony.eu . . с. 13

STONESOFT
Тел.: (495) 787-9936
www.stonesoft.com . . с. 67

Указатель фирм

Учредители журнала «ИнформКурьер-Связь»:

ЗАО Информационное агентство «ИнформКурьер-Связь»:
127273, Москва, Сигнальный проезд, д. 39, подъезд 2, офис 204; тел.: (495) 981-2936, 981-2937.

ЗАО «ИКС-холдинг»:
127254, Москва,
Огородный пр-д, д. 5, стр. 3;
тел.: (495) 785-1490, 229-4978.

МНТОРЭС им. А.С. Попова:
107031, Москва, ул. Рождественка, д. 6/9/20, стр. 1;
тел.: (495) 921-1616.

Подпишись на журнал «ИКС»

Подписчики журнала гарантированно получают*:

- Доступ к электронной версии журнала «ИКС» в день его выхода

Оформляйте подписку:

- В редакции — по телефону: +7 (495) 785 1490 или e-mail: podpiska@iksmedia.ru
- Каталог Роспечать — индекс 73172, 71512
- Каталог Пресса России — индекс 12417
- Объединенный каталог — индекс 43247
- Список альтернативных агентств: http://iksmedia.ru в разделе подписка.

Специальные условия при оформлении подписки для корпоративных клиентов! Подробности по телефону отдела распространения: +7 (495) 785 1490

Тел.: +7 (495) 785 1490 • E-mail: podpiska@iksmedia.ru

* оформившие подписку через редакцию или альтернативное агентство

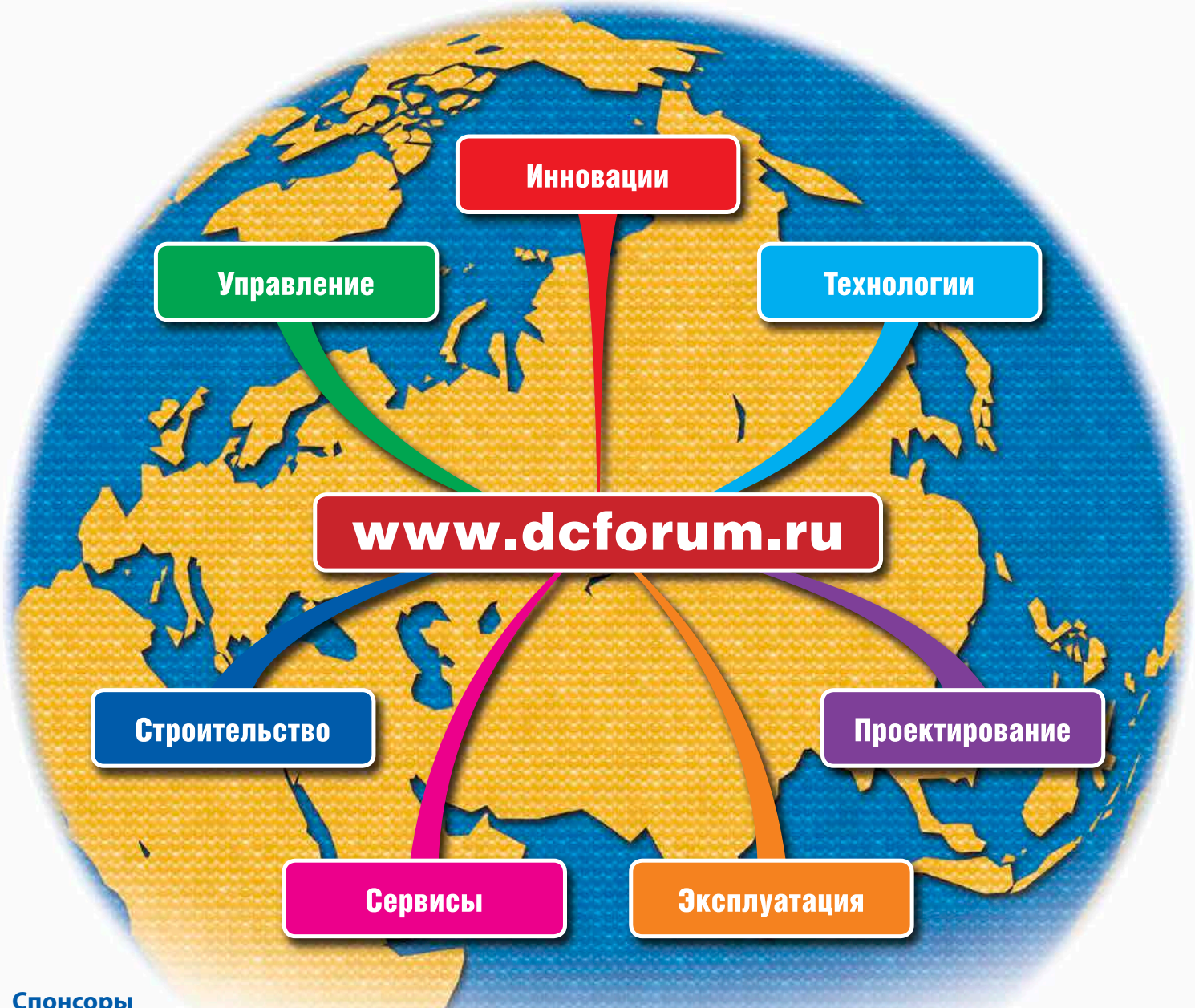
Телеком • ИТ • Медиа **www.iksmedia.ru**

9-я международная конференция

ЦОД

4–5 сентября 2014
Москва, Центр Digital October

IX DATA CENTER FORUM



Спонсоры и партнеры

Schneider Electric
DataPro
R-Style
Brand-Rex
KASPERSKY lab
linxdatacenter
ПОЖТЕХНИКА
HTS HOSSER TELECOM SOLUTIONS
EMERSON Network Power
АБИТЕХ абсолютная техника
DELTA Smarter. Greener. Together.
RITTAL
ТРЕЙД ГРУПП
Raritan Know more. Manage Smarter.
lattelecom
телекомбиржа
Uptime Institute