

ИКС

издается с 1992 года

№ 11 • ноябрь • 2013

Подмосковье дает зеленый сигнал	6
Осеннее обострение-2013	24
Базаданныхмания	67
Конец вечных вопросов про ЦОДы	72

ИТ-здоровье

ТЕМА НОМЕРА



НОВЫЙ

www.iksmedia.ru ←

мобильная версия на Google Play

16^я МЕЖДУНАРОДНАЯ ВЫСТАВКА И ФОРУМ **ССТВ' 2014**

28-30 января 2014 • Москва, Крокус Экспо



Цифровое кабельное, спутниковое и эфирное ТВ • IPTV • OTT
Мобильное ТВ • Multiscreen • Smart TV • HDTV • ТВ контент
Мобильные мультимедийные коммуникации
Мультисервисные сети • Спутниковая связь

www.cstb.ru

18+

Организатор

MIDexpo
МЕЖДУНАРОДНЫЕ ВЫСТАВКИ И ФОРУМЫ

Генеральный партнер



Поддержка



Стратегический партнер



Золотой спонсор



Генеральный
информационный партнер



Генеральный
интернет-партнер



Реклама

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. Емельяников,
Ю.Б. Зубарев (почетный председатель),
Н.Б. Кий, А.С. Комаров, К.И. Кукк,
Б.А. Ластович, Г.Е. Моница, 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.А. Краснушкина – ek@iks-media.ru

Дизайн и верстка
Д.А. Поддьяков, 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
expro@iks-media.ru
С.С. Агуреева – подписка
podpiska@iks-media.ru

Журнал «ИнформКурьер-Связь» зарегистрирован
в Министерстве РФ по делам печати, телерадио-
вещания и средств массовых коммуникаций
25 февраля 2000 г.; ПИ № 77-1761.
Мнения авторов не всегда отражают точку зрения
редакции. Статьи с пометкой «бизнес-партнер»
публикуются на правах рекламы. За содержание
рекламных публикаций и объявлений редакция
ответственности не несет. Любое использование
материалов журнала допускается только
с письменного разрешения редакции и со ссылкой
на журнал.

Рукописи не рецензируются и не возвращаются.

© «ИнформКурьер-Связь», 2013

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

Реклама МЕГАФОН Редакция пользуется
услугами
сети «МегаФон-Москва»

Тел.: (495) 502-5080
№ 11/2013 подписан в печать 01.11.13.
Тираж 15 000 экз. Свободная цена.
Формат 64x84/8

ISSN 0869-7973

12+



Пока абоненты, потирая руки, готовят план побега от поднадоевшего оператора (признаться, я отношусь к их числу), чтобы вкусить огрехи в работе его конкурента, – противостояние регулятора и бизнеса усиливается. И порой переходит из подковерной борьбы в публичную перепалку.

Ситуация напоминает революционную: верхи хотят, но не могут; низы не могут, а еще больше не хотят.

Речь, конечно, об МНР, на внедрение которого, как выясняется, по хорошему требуется несколько месяцев, а то и лет. Но точно не «на следующий день после утверждения нормативной правовой базы». Наши поставщики услуг, конечно, напрягутся и справятся за несколько месяцев: вот Новый год, Олимпиаду с 8 Марта переживут – и сделают в лучшем виде.

А тем временем падает удовлетворенность абонентов операторами мобильной связи. 7,4% – таковы общие потери сотовиков в доверии пользователей. Это падение до уровня 2007 года, ниже только кризисный 2009-й. Аналитики EPSI Rating в качестве причин называют отсрочку отмены мобильного рабства и снижение качества связи. Я бы добавила к этому разочарование клиентов в мобильном интернете – реальность разительно отличается от обещаний ТВ-рекламы: в итоге рейтинг МТС у абонентов упал более всего, у «Мегафона» – менее.

Долю тех, кто намерен сменить поставщика услуг, операторы оценивают невысоко, в несколько процентов. Аналитики – в разы больше. С ними стоит согласиться. По впечатлениям недовольных недостаточно. И люди захотят попробовать перейти к другому оператору из простого любопытства: как там, где нас нет?

Как всегда, в многосоставном процессе не найдешь правых и виноватых. Но регулятор, обещавший подготовить правовое поле МНР в марте, до конца не справился с этим делом еще в четвертом квартале, менял коней на переправе в приказах еще в сентябре, а с оператором базы данных перенесенных номеров определился только в первой декаде октября.

Сотовики, хоть и пытаются увидеть в МНР бизнес-преимущества, больше находят объективных и субъективных причин почему «нет» – не сегодня, не завтра, пусть на будущий год. И демонстрируют редкое единство, согласие и понимание с полувзглядом.

Бизнес, конечно, победит, потому что он больше, часто квалифицированное, а главное – мотивированное.

А абонентам деваться некуда – они рабы, хоть и на мобильном поводке. Юрьев день hi-tech-времен откладывается, скорее всего, на полгода: в политике с регулятором операторы настаивают на 1 июня.

До встречи.
Наталья Кий,
главный редактор

1 КОЛОНКА РЕДАКТОРА

6 НОВОСТИ

6 АКТУАЛЬНЫЙ КОММЕНТАРИЙ

М. ЮРГЕЛАС. «Мы даем зеленый сигнал»

8 ЛИЦА

9 ПЕРСОНА НОМЕРА

Дж. КУДРИЦКИ. Странствующий жизнелюб из большого бизнеса

КОМПАНИИ

12 Новости от компаний

СОБЫТИЯ

20 Планы КПССные

24 Осеннее обострение-2013

28 Кому полезны открытые данные?

30 Как регулировать стагнацию

32 Сильнодействующее средство от адептов корпоративной мобильности

СУБЪЕКТ ФЕДЕРАЦИИ

33 Ю. ФЕДОРОВА. Вечная мерзлота сохраняет мамонтов и монополистов

На портале IKS MEDIA

34 Блог, еще раз блог!

36 КАЛЕНДАРЬ СОБЫТИЙ



9

Дж. КУДРИЦКИ.

Странствующий жизнелюб из большого бизнеса



24

Осеннее обострение-2013



38 ТЕМА

ИТ-ЗДОРОВЬЕ: информатизация и высокие технологии в медицине

Фокус

40 Все только начинается

42 Р. САФРОНОВ. Наладить сотрудничество всех заинтересованных сторон

44 О. СИМАКОВ. Тектонические сдвиги будут заметны не сразу

Модель

45 Г. ЛЕБЕДЕВ. Информатизация не должна нарушать порядок работы врача

46 Б. ПОДДУБНЫЙ. От манифеста – к результату

Позиция

47 М. ЭЛЬЯНОВ. Главная проблема – нет правил игры

48 Г. СИЗОНЕНКО. Темпы есть, а системности нет

49 М. ДЕГТЕРЕВА. Главная задача информатизации пока не решена

Сценарий

50 М. НАТЕНЗОН. Россия – классическая страна для теле-медицины



62 ДЕЛО

Экономика и финансы

- 62 А. ЗАЙЦЕВА. Снова в «зеленой» зоне



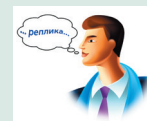
Горизонты

- 64 А. ГОЛЫШКО. Очередные задачи
Телекома. К новому сдвигу парадигмы



Реплика

- 67 М. ЕМЕЛЬЯННИКОВ. Базаданныхмания



Рубежи обороны

- 68 В. НОСОВА. Мобильная защита
для начинающих
70 Р. ЮСУПОВ. Защита по-русски



71 «ИКС» ргоТЕХнологии

- 72 Е. ВОЛЫНКИНА. Подопроектирование и подострой-
тельство: конец вечных вопросов
77 М. БАЛКАРОВ. Liebert PDX: и инновации, и традиции
78 В тренде – комплексные решения для ЦОДов
80 А. ПАВЛОВ, Д. БАСИСТЫЙ. Выбираем площадку
для ЦОДа. Правила и риски. Ч. 1
84 И. ГРАНКОВ. Ситуация под контролем
88 Я. ГОРОДЕЦКИЙ. SDN: прорывная технология
или маркетинговый пузырь?
90 А. СЕМЕНОВ. Оборудование интерактивного управле-
ния: расширение функциональных возможностей
93 Новые продукты

- 51 А. СМЕРНОВ. Разрыв между возможностями и реаль-
ностью

- 51 Е. РЯБЧИКОВА. Здравоохранение – перспективный
рынок для телекома

Ракурс

- 52 Врачебная тайна эпохи интернета

- 52 М. ЕМЕЛЬЯННИКОВ. Мечты об инфобезопасности
в здравоохранении

- 53 А. САБАНОВ. Защита от дилетантов

- 53 А. ПРОЗОРОВ. Требований инфобезопасности
слишком много

Подробности

- 54 Ф. КИДАЛОВ. Требуются реалистичные комплексные
решения

- 55 А. ЛИТВИНОВИЧ. Требуется стандарт

- 55 И. СКОБЕЛЕВ. Требуется единая платформа

Дискуссионный клуб «ИКС»

- 56 Разносторонний треугольник: пациент, врач и государство

Бизнес-партнер

- 60 К. ЕРМАКОВ, А. МОРОЗОВ. Трансформаторные ИБП
в медучреждениях: надежность прежде всего



1 EDITOR'S COLUMN

6 NEWS

6 COMMENT OF TODAY

M. YURGELAS. "We give a green light"

8 PROFILES

9 PERSON OF THE ISSUE

J. KUDRITSKI. Travelling businessman with zest for life

COMPANIES

12 Company news

EVENTS

20 Plans of CPSU

24 Autumn flare-up-2013

28 Who will benefit from open data?

30 How to regulate the stagnation

32 Anticorporate mobility adherers remedy

REGION OF FEDERATION

33 Y. FEDOROVA. Ever frost saves mammoths and monopolists

On IKS MEDIA portal

34 Blog, and once again blog!

36 CALENDAR OF EVENTS



J. KUDRITSKI. Travelling businessman with zest for life



24

Autumn flare-up-2013



38 COVER STORY

IT-HEALTH: informatization and high technologies in medicine

Focus

40 It's just the beginning

42 R. SAFRONOV. To establish collaboration of all concerned parties

44 O. SIMAKOV. Tectonic shifts will not be visible at once

Model

45 G. LEBEDEV. Informatization shouldn't disturb the doctor's work process

46 B. PODDUBNYI. From manifest to result

Position

47 M. ELIANOV. Main problem is the lack of game rules

48 G. SIZONENKO. There is movement, but there is not consistency

49 M. DEGTEREVA. Main informatization task isn't solved yet

Scenario

50 M. NATENZON. Russia is the classic country for telemedicine

51 A. SMIRNOV. The gap between capabilities and reality

1. IKS is the leading business inter-industry publication for new converged Telecom-Media-Technologies market – essential information source about market trends and analysis for your investment and strategy policies.
2. Our readers are the leaders of business community – your chance to talk to the market leaders directly through IKS publications and www.iksmedia.ru and share your views on the most popular topics.
3. Effective distribution channels – personalized subscriptions and focused distribution at key industry events.
4. Wide range of MarCom services – PR, ads, sponsorships, direct marketing, special projects on demand – round tables, pre-sale events.



YOUR SUCCESS IS OUR GOAL!

Contact us for 2013 editorial calendar!

- 51 E. RIABCHIKOVA. Healthcare is the perspective market for telecom

Angle

- 52 Patient confidentiality of the internet age
 52 M. EMELIANNIKOV. Dreams about infosecurity in healthcare
 53 A. SABANOV. Defense from amateur
 53 A. PROZOROV. There are too many infosecurity requirements

Details

- 54 F. KIDALOV. Realistic complex solutions are required
 55 A. LITVINOVICH. Standard is required
 55 I. SKOBELEV. United platform is required

"IKS" discussion club

- 56 Scalene triangle: patient, doctor, government

Business partner

- 60 K. ERMAKOV, A. MOROZOV. Transformer UPS for medicine: reliability first

62 BUSINESS

Economy and finances

- 62 A. ZAYTSEVA. In the "green" zone again

Horizons

- 64 A. GOLYSHKO. Foremost tasks of Telecom. To new paradigm's shift

Retort

- 67 M. EMELIANNIKOV. Databasemania

Defense lines

- 68 V. NOSOVA. Mobile defense for beginners
 70 R. YUSUPOV. Defense in the Russian style

71 «IKS» proTECHnologies

- 72 E. VOLYNKINA. Data center design and data center building: the end of perennial questions
 77 M. BALKAROV. Liebert PDX: both innovations and traditions
 78 There are the complex solutions for data centers in the trend
 80 A. PAVLOV, D. BASISTYI. To choose the place for data center. Rules and risks. Part I
 84 I. GRANKOV. Situation under the control
 88 I. GORODETSKIY. SDN: breakthrough technology or marketing bubble?
 90 A. SEMENOV. Interactive management equipment: functionality enhancement
 93 New products

«Мы даем

ЗЕЛЕНЫЙ СИГНАЛ»

актуальный
комментарий



После появления Новой Москвы область стала напоминать по форме хорошо гнутую подкову. Может быть, оно и к счастью. Но подмосковные информатизаторы шутят, что теперь «по контуру нет целостности».

В соответствии с госпланом Московская область должна за пятилетку перемахнуть с 20-го места по информатизации на 5-е. Что означают три строчки в рейтинге в год, рассказывает **Мария ЮРГЕЛАС**, министр государственного управления, ИТ и связи Московской области.

– Мария, большая часть вашей профессиональной деятельности до 2013 г. была связана с ИТ-бизнесом. Какой опыт взяли с собой на госслужбу, от чего пришлось отказаться?

– Первое – я резко поменяла свое мнение о чиновниках. Раньше с госсектором я была знакома со стороны бизнеса, по совместным проектам. Но только когда пришла на государственную службу, стал ясен колоссальный уровень ответственности и огромный объем работы – признаюсь, в бизнесе я столько не работала. Как следствие – необходимо расставлять приоритеты. Чтобы управлять огромной территорией, ты должен балансировать между темпами социального развития и задачами госвласти.

Кроме того, что ты публичный человек, ты должен заниматься и операционной деятельностью. У тебя должно быть стратегическое видение развития региона по своему направлению на период три-пять лет. Ты должен понимать, что все твои решения будут иметь непосредственное воздействие на жителей, а их в Московской области 7 миллионов. В бизнесе ты всегда ориентирован на результат, заточен на реализацию конкретного проекта. Максимум, что может быть, – не получишь прибыль. На госслужбе помимо собственно результата в цифрах и фактах есть последствия для людей, управления, бизнеса на твоей территории. Степень ответственности возрастает.

Да и размер поля деятельности совершенно иной. Московская область – крупнейший регион с точки зрения населения, географического и политического расположения, территории, числа муниципальных образований (их больше, чем где-либо в России, – 360). Соответственно сложность управления, требуемый уровень квалификации возрастают. Ты «между»: между муниципальной властью и федеральной властью. Это новый тип проблем и задач.

– В чем специфика информатизации Подмосковья? Отчего субъект Федерации центра стра-

ны к 2012 г. оказался на 20-м месте в рейтинге регионов по информатизации?

– Специфика такова, что в 2012–2013 гг. в расчете на душу населения финансирование программ внедрения ИКТ в области составило 0,7 тыс. руб. – против 6,6 тыс. и 4,7 тыс. руб. соответственно в Москве и Петербурге и, представьте, в 2–3 раза ниже, чем в Хабаровском и Камчатском крае. Кроме того, за прошлый год на посту руководителя ИТ и связи Подмосковья сменилось три человека. Разумеется, ситуацию надо исправлять. Выход мы видим в системном подходе к развитию единой ИКТ-инфраструктуры органов власти и к построению государственных информационных систем, в формулировании единой информационной политики и создании единой архитектуры ИС, унифицированной нормативной базы. Этим целям должна служить госпрограмма «Эффективная власть» и ее профильная подпрограмма «Развитие ИКТ для повышения эффективности процессов управления и создания благоприятных условий жизни и ведения бизнеса в Московской области на 2014–2018 гг.».

Прежде всего мы централизовали у себя финансовые ресурсы. В 2012–2013 гг. бюджет Министерства государственного управления, ИТ и связи не достигал и половины ИКТ-бюджета региона – остальная часть была «размыта» по другим ведомствам, что привело к серьезным различиям в обеспеченности техникой и системами, недостаточной координации и централизации в развитии ИТ. На период 2014–2018 гг. все, что связано с информационными технологиями (неважно, отнесенными к образованию, здравоохранению, культуре, транспорту или другим отраслям), объединено в госпрограмме по развитию ИКТ. Общий объем финансирования мероприятия составит 15,277 млрд руб. до 2018 г., из них в распоряжении профильного ведомства и Московского областного центра ИКТ будет находиться около 11 млрд руб. Я являюсь координатором этой программы. Несу за нее ответственность.

– Каковы приоритеты?

– Понятно, что бюджета всегда не хватает, а у нас бюджет социально ориентирован. В первую очередь мы развиваем информатизацию в образовании,

здравоохранении, не забываем культуру, модернизируем базовую инфраструктуру, т.е. обновляем компьютерный парк для 9 тыс. человек. Последний раз это делали в 2007–2009 гг., как понимаете, для ПК это древность.

Чтобы поднять уровень информатизации области, мы ведем рейтинг глав муниципальных образований по выполнению поручений губернатора в сфере ИТ, участвуем во всех «пилотах», во всех начинаниях в этой сфере, которые проводит Минкомсвязь. Нам необходимо повысить использование СМЭВ, которое сейчас в области рекордно низкое – только 8% госорганов включены в систему; в следующем году этот показатель должен составить 75%. Доля обращений граждан за госуслугами тоже невелика – 5%; к 2015 г. должна увеличиться до 25%.

Планомерно внедряем межведомственные системы – мы их называем «системы общего пользования». Например, в систему ЖКХ объединяются данные Министерства стройкомплекса и ЖКХ, муниципалитетов, сведения о тарифах и ценах, наконец, портал, который будет разработан и создан в интересах жителей. То есть по сути создаем виртуальный единый расчетно-кассовый центр ЖКХ и, конечно, единую информационную систему. До конца года для Министерства экономики Московской области будет создана единая система сбора и анализа социально-экономических показателей муниципалитетов и прогнозирования.

– Очевидно, что для достижения таких темпов роста ИТ-сферы понадобятся дополнительные инвестиции, помимо бюджетных. Как договариваетесь с бизнесом и видите его интересы?

– Привлечение инвестиций – одна из основных наших задач, иначе у нас будет недостаточно средств для того, чтобы вкладывать в социальную сферу. Поскольку в компетенции нашего министерства не только ИТ и связь, но и государственное управление, то мы отвечаем за снижение административных барьеров для бизнеса. Чтобы бизнес был заинтересован приходить в Московскую область, вкладываться, развивать предприятия, создавать рабочие места и в итоге платить налоги.

– С Москвой конкурировать в этом смысле сложно...

– А здесь не Москва является нашим главным конкурентом, а – Калуга. Губернатор Калужской области привлек значительный объем инвестиций. Потому что он объявил предпринимателям, что от их желания открыть в регионе бизнес и сделать инвестиции до подписания контракта – дистанция в десять минут, решения принимает на личном уровне. Иными словами, созданы такие условия, что даже крупные западные производители пришли в Калугу строить заводы.

Мы должны воспользоваться нашими уникальными условиями близости к столице, можем предложить лучшие условия, чем Калуга, знаем и видим претендентов. Но соседи уже начали – в этом их преимущество.

В области есть территории, где экономически невыгодно прокладывать оптоволокно, а уровень проникновения ШПД, прежде всего в школах, мы не считаем удовлетворительным. Сейчас говорим с «Ростелекомом» и ключевыми мобильными операторами о том, что готовы способствовать выделению земли, предоставлению зданий и сооружений для установки вышек и другого оборудования, т.е. готовы снижать барьеры входа и развития связи на территории области. Наша цель – чтобы операторы покрывали связью прежде невыгодные для них участки.

Мы пришли из бизнеса и понимаем, что бизнес надо чем-то заинтересовать. Мы как правительство готовы способствовать снижению административных барьеров. Мы даем зеленый сигнал. Но ждем ответных шагов.

– Как повлияло и еще повлияет на развитие ИТ в области формирование Новой Москвы?

– Конечно, есть серьезные потери в доходной части. С другой стороны, область держит курс на тесную интеграцию с Москвой. Много жителей Подмосковья работают в столице, москвичи живут на подмосковных дачах. Поэтому много общих тем: строительство дорог-развязок, легкое метро, единый проездной билет... Часть нынешних подмосковных министров пришли из правительства Москвы, поэтому мы находим общий язык, внедряем обкатанные в столице и уже каustomизированные решения.

– Понятие «эффективность власти, управления» входит в название госпрограммы Московской области и профильной подпрограммы, касающейся ИКТ. Как определяется это понятие, чем измеряется, ведь известно, что даже эффективность внедрения ИТ с трудом поддается счету?

– До перехода на трехлетний бюджет в области было много целевых программ. Мы решили объединить их по общему признаку, по показателям, которых необходимо достичь. Эффективное управление в целом невозможно без эффективного управления следующими ресурсами: финансами, имуществом, кадрами – с помощью современных технологий. Поэтому в нашем понимании эффективная власть – это как раз эффективное управление всеми ресурсами с помощью современных технологий.

В госпрограмму «Эффективная власть» вошли программы Министерства финансов, Министерства имущественных отношений, кадровой службы, а также программа по информатизации и качеству госуправления. По каждой программе есть свои показатели: в финансах – сбалансированный бюджет социальной направленности, в имущественной сфере – изыскание земель для предоставления инвесторам. Мой основной показатель по информатизации – повышение в рейтинге, а по госуправлению – снижение административных барьеров, препятствующих развитию бизнеса. Так что у эффективной власти есть свои измерители.

Беседовала **Наталья КИЙ**

Энтузиазм профессионалов – движущая сила информатизации здравоохранения в России (см. ТЕМУ НОМЕРА → с. 38–61 ←). Гости нашей рубрики доказывают это каждый день.



**Мария
ДЕГТЕРЕВА,**

директор,
государственное
учреждение
здравоохранения
особого типа
Владимирской
области
«Медицинский
информационно-
аналитический
центр»

Родилась 1 июля в Горьком, среднюю школу оканчивала в Коврове Владимирской области. В 1990 г. окончила Горьковский государственный медицинский институт имени С.М. Кирова по специальности «санитария, гигиена и эпидемиология», получив квалификацию «врач-гигиенист, эпидемиолог, профпатолог».

Карьеру в медицине начинала с должности санитарного врача в СЭС, в 1991–2000 гг. – врач-статистик и руководитель кабинета медицинской статистики. В 2000–2005 г. работала в должности заведующей Владимирского областного государственного учреждения здравоохранения «Бюро медицинской статистики», с 2005 г., после его преобразования в ГУЗ особого типа Владимирской области «Медицинский

информационно-аналитический центр» – в нынешней своей должности.

Замужем.

Хобби – дача, прогулки в лес за грибами и путешествия.



**Михаил
НАТЕНЗОН,**

председатель
совета директоров,
научно-
производственное
объединение
«Национальное
телемедицинское
агентство»

Родился 30 октября 1949 г. в Москве. В 1972 г. окончил факультет прикладной математики Московского института электронного машиностроения. Канд. техн. наук, академик РАЕН, автор более 150 научных работ, изобретений и патентов.

В 1972–1997 гг. – старший научный сотрудник Института космических исследований РАН, в 1990–1991 гг. работал как приглашенный исследователь по международной программе в Институте теоретической физики Калифорнийского университета (США).

В 1993 г. создал группу компаний ТАНА, став генеральным директором компании «ТАНА – телемедицинские системы» (и остается им до настоящего времени). С 2002 г. – председатель совета директоров НПО «Национальное телемедицинское агентство», с 2005 г. – зам. руководителя

Региональной рабочей группы СНГ по телемедицине, с 2010 г. – координатор фокус-группы по мобильной телемедицине МСЭ, в 2012 г. стал содиректором от России в проекте «Разработка многонациональной телемедицинской системы для чрезвычайных ситуаций» комитета «Наука ради мира и безопасности» Совета Россия – НАТО.

Увлечения – работа и внуки.

Родился в 1972 г. в Калининграде. В 1994 г. окончил Военно-морской институт радиоэлектроники им. А.С. Попова (Санкт-Петербург) по специальности «математическое обеспечение АСУ».

С 1994-го по 1996 гг. служил в ВС РФ. В 1996–2008 г. – директор департамента ИТ ОАО «За рулем», в 2009–2010 гг. – начальник управления ИТ ФГУП «Радиочастотный центр Центрального федерального округа». С 2010 г. – директор службы ИТ в ОАО «Медицина».

Прошел обучение по системам менеджмента EFQM, ISO 9001, ISO 27001, член организации BICSI. Яркий поклонник практики ITIL. Любитель стандартов семейства TIA. Разработчик комплексного решения «Умная палата» (получено авторское свидетельство) и соавтор концепции «Smart-Клиника».

Женат, двое детей – девочка и мальчик.

Хобби – автомобили-вседорожки и автомобильные путешествия, фотография, виндсерфинг (участвует в любительских соревнованиях), велосипедные прогулки и игра на разных музыкальных инструментах.



**Федор
КИДАЛОВ,**

директор
службы ИТ,
ОАО «Медицина»

Родился 27 апреля 1958 г. в Темрюке (Краснодарский край). В 1977 г. окончил Краснодарский станкостроительный техникум, после чего был призван в армию. В 1979 г. поступил в МВТУ им. Н.Э. Баумана на факультет машиностроения, окончив его в 1985 г. по специальности «летательные аппараты».

В 1985–1989 гг. – председатель профкома студентов и заместитель секретаря парткома МВТУ им. Н.Э. Баумана. С 1989-го по 1996 г. – начальник отдела совместного предприятия «ИВК-Интернешнл», которое занималось разработкой и поставкой вычислительных машин для Министерства обороны, а затем выпуском портативных ПК. С 1996 г. – генеральный директор ИВК.

Женат, имеет дочь.

Хобби – боевые искусства, путешествия и рыбалка.



**Григорий
СИЗОНЕНКО,**

генеральный
директор,
ИВК



Джулиан КУДРИЦКИ

Странствующий жизнелюб из большого бизнеса

Азарт, любопытство, готовность к приключениям – эти качества необходимы не только путешественнику или исследователю. Джулиану КУДРИЦКИ, исполнительному директору Uptime Institute, они помогают управлять серьезным международным бизнесом и получать от этого удовольствие.

Прививка любознательности

Родился Джулиан Кудрицки летом 1975 г. в Сан-Франциско (шт. Калифорния, США). Сюда в восемнадцатилетнем возрасте перебрался из Германии его отец, здесь жила его мать, чьи предки поселились на американской земле еще во времена Льюиса и Кларка (руководители первой сухопутной экспедиции через территорию США, 1803–1806 гг. – *Прим. авт.*). Оба его родителя имели магистерскую степень в области литературы и искусства и были страстными поклонниками средневековой культуры. Пока детей в семье было двое, их всегда брали с собой в путешествия по Европе, куда ездили осматривать романские крепостные стены и готические соборы.

Дома, возложив обязанность приучения сына к порядку и дисциплине на католическую школу, отец, заядлый турист, прививал нашему герою и четверем его младшим сестрам вкус к походам по лесам и горам Калифорнии. «Мы жили отнюдь не в стерильных условиях, – вспоминает это счастливое время Джулиан, – зато привыкали к самостоятельной жизни, учились все делать своими руками и не теряться в неожиданных ситуациях». Так, однажды после долгого перехода усталые путешественники забрались в спальные мешки на вершине холма и тут же уснули, а поутру обнаружили, что расположились прямо на муравейнике.

Помнит Джулиан и семейные поездки на сбор винограда, гостеприимный дом и шесть особенных месяцев, проведенных им за чтением книг Генри Джеймса, сразу ставшего его любимым писателем.

Любовь к литературе и ныне помогает Джулиану Кудрицки в инженерном бизнесе – в нахождении общего языка с сотрудниками, партнерами и заказчиками со всего света, от Бразилии до Малайзии. А в юности она определила его выбор профессии, как тогда казалось, навсегда.

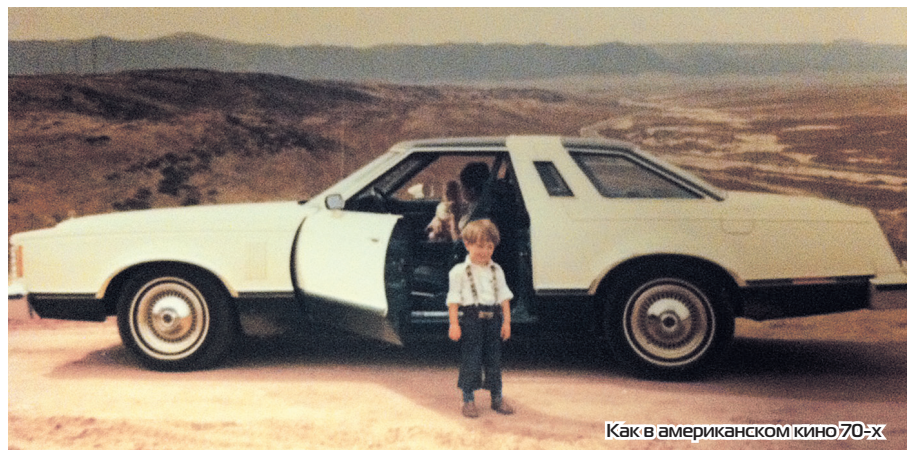
С запада на восток и обратно

Получив степень магистра в области истории английской литературы второй половины XIX века, Дж. Кудрицки переехал в Нью-Йорк, в культурную столицу США и сердце издательского бизнеса, чтобы посвятить себя работе над книгами. Короткое собеседование с руководителем одного известного издательства несколько охладило его пыл. «У меня только один вопрос: почему ты хочешь редактировать художественную литературу? – спросил собеседник и тут же добавил: – Только не отвечай: потому что ты любишь книги». Джулиан все-таки нашел место редактора. Он целый год готовил к изданию самую разную литературу – техническую, фотоальбомы, школь-

ные тетради, пока не понял, что в Нью-Йорке ему не хватает открытых пространств американского Запада и солнечных дней.

Вот почему он при первой возможности поменял мегаполис на одноэтажный Санта-Фе (шт. Нью-Мексико), где солнце светит 250 дней в году, и посчитал перемену позитивной. «Санта-Фе – маленький город, – рассказывает Джулиан Кудрицки об этом периоде своей жизни. – Основная статья его доходов – туризм. Я наслаждался жизнью в нем: занимался то тем, то сем, много гулял пешком, ловил рыбу».

Так прошел еще год, а весной 2004-го ему попалось объявление о вакансии в Uptime Institute: президенту этой компании срочно требовался ассистент, который к тому же мог бы готовить к публикации технические материалы и литературу. Первые недели и месяцы работы в новой должности Джулиану пришлось засесть за отчеты Uptime Institute, вникать в инженерную тематику и одновременно учиться бизнесу.



Как в американском кино 70-х

Три шага наверх

В то время Uptime Institute был не большой компанией, подразделения продаж в ней не было, бизнес вели консультанты. Они сами искали клиентов, обсуждали с ними условия контрактов, заключали их и получали комиссионные. Как-то раз Джулиану выпал счастливый случай – продать услуги Uptime Institute национальной нефтяной компании Саудовской Аравии Saudi Aramco. И когда после нескольких недель ночных телефонных переговоров с Дахраном, где находится штаб-квартира клиента, контракт был заключен, он оказался и самым крупным по объему, и самым дальним по расстоянию в том году. Таким был первый шаг Дж. Кудрицки от административно-обеспечивающей роли к непосредственному участию в развитии бизнеса.

Второй шаг Джулиан сделал в составе рабочей группы по разработ-

ке бизнес-программы Uptime Institute по сертификации, аккредитации, обучению и консалтингу. Его товарищами по команде были Хэнк Сидер и Винс Рено, а Питт Тернер, сооснователь компании, оказывал им поддержку со стороны руководства. Задача – сделать внутренние наработки Uptime Institute достоянием всей индустрии цодострое-ния – потребовала от команды года интенсивной работы. Результат ее деятельности, обнародованный в 2008 г., в большей степени заинтересовал компании из Саудовской Аравии, Китая и Великобритании, чем из США. У этих стран было гораздо меньше опыта в проектировании ЦОДов, поэтому и потребность в методической поддержке у них была острее.

Третий крупный шаг Джулиана по карьерной лестнице совпал по времени с приобретением Uptime

Institute компанией The 451 Group и переездом из Санта-Фе в Сиэтл. Новый владелец – Мартин Маккарти – сделал ставку на глобальное развитие компании и поручил Дж. Кудрицки создать сеть зарубежных офисов. Сегодня у Uptime Institute их шесть: в США, Бразилии, Великобритании, Малайзии, на Тайване и в России. Конечно, управлять людьми на расстоянии – это определенный вызов, поэтому так важен подбор управляющего директора каждого регионального офиса. «Согласно нашим критериям, – объясняет Джулиан Кудрицки, – управляющий директор должен быть человеком, с которым мы знакомы лично и который способен решать задачи самостоятельно при минимальной поддержке со стороны штаб-квартиры. Алексей Солодовников, занимающий эту позицию в России, – хороший тому пример».

→ БЛИЦ. В сезон ловли лосося

– Ваше время всецело принадлежит работе?

– Как и многие мои коллеги, я немало времени провожу в аэропортах, но это волнующее время: множество направлений, знакомства с новыми людьми, а потом радость возвращения домой, в Сиэтл. Там я встречаюсь с родными и друзьями, ловлю рыбу, и все вокруг – деревья, вода – помогает мне восполнить потраченную энергию. Сейчас у нас сезон ловли лосося – он начинается в океане и продолжается в реке. И мне кажется, я слышу его призыв...

– Какие черты вы считаете своими сильными сторонами?

– Назову одну из них, которой горжусь, – это любопытство. Меня не могут удовлетворить легковесный ответ и стандартное решение, я постоянно ищу необычные выходы из ситуаций, неожиданные сценарии. Мне близки люди, которые с пылом и страстью относятся к своему делу, я считаю, что это свойство лидера.

– От чего еще вы получаете удовольствие?

– Я люблю принимать у себя друзей и членов своей семьи, готовить блюда итальянской кухни. Французская кухня, может быть, более технична, зато в итальянской легче добиться успеха. Он зависит от правильного выбора ингредиентов. Я обожаю разыскивать и покупать все необходимое, потом колдовать над блюдом и сервировать стол в итальянском стиле. У меня получается по-настоящему вкусное ризотто, просто объеденье.



– Как часто вы встречаетесь с семьей, с сестрами?

– Одну из сестер я вижу ежедневно, она тоже работает в Uptime Institute. Мы очень близки с мамой, не так давно вместе побывали в Бразилии. С другими сестрами у меня тоже хорошие отношения. У каждой из них своя жизнь, но мы всегда радуемся встрече.

– А вы дрались в детстве?

– Как сумасшедшие. Нас было пятеро, все мы были независимыми и время от времени оставались без присмотра. Две пары дрались друг с другом, а пятый выбирал, к кому ему присоединиться.

– Что для вас счастье?

– Счастье в профессии – это удовлетворение, которое ощущаешь в конце рабочего дня от того, что энергия была потрачена тобой не напрасно,

это возможность получать удовольствие от того, что делаешь. А в личной жизни оно зависит от умения ценить время и радоваться простым вещам. Но я думаю, что главное для счастья – это не терять чувства юмора и быть готовым к приключениям.

– Каким вы видите себя через 20 лет?

– Женатым человеком с детьми, живущим в месте, которое люблю. К этому времени, надеюсь, я закончу ремонт одной очень старой машины, которым сейчас занимаюсь. Хочу сохранить близкие отношения с семьей. Наш дом всегда был полон друзей и друзей наших друзей, и мне хотелось бы, чтобы так было и впредь.

Записала Александра КРЫЛОВА

Новые вершины производительности
и облачных вычислений с серверами
ETegro Hyperion на базе
процессоров Intel® Xeon® E5-2600



Реклама

Представляем серверы ETegro Hyperion четвертого поколения



Корпоративный

ETegro Hyperion RS230 G4

до 2-х процессоров
Intel® Xeon® E5-2600,
до 768GB памяти DDR3 1600МГц,
до 2-х дочерних плат расширения,
до 12/24 дисков с передней панели,
дополнительно 2 диска 2.5",
2 порта 1GbE/10GbE,
5 слотов расширения PCIe 3.0,
питание 1100 Вт, 1+1



Производительный

ETegro Hyperion RS130 G4

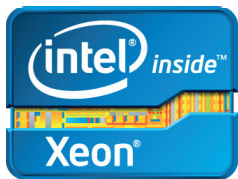
до 2-х процессоров Intel® Xeon® E5-2600,
до 768GB памяти DDR3 1600МГц,
до 2-х дочерних плат расширения,
до 4/10 дисков в корпусе 1U,
2 порта 1GbE/10GbE,
слот расширения PCIe 3.0,
питание 750Вт, 1+1



Экономичный

ETegro Hyperion RS125 G4

до 2-х процессоров Intel® Xeon® E5-2600, до 512GB памяти DDR3 1600МГц,
до 4 дисков в корпусе 1U, 2 порта 1GbE, дополнительно 2 порта 10GbE,
слот расширения PCIe 3.0, питание 650Вт



Конфигуратор и заказ

на сайте производителя www.etegro.ru



ETEGRO technologies

Тел./факс: 8 (495) 380-02-88, E-mail: sales@etegro.com, www.etegro.ru

ТЕХНИКА ETEGRO – ЗАЛОГ ВАШЕГО УСПЕХА!

© Intel, логотип Intel, Xeon и Xeon Inside являются товарными знаками корпорации Intel на территории США и других стран.

© Логотип ETegro Technologies является зарегистрированным товарным знаком ЗАО «ETegro Текнолоджис».

С 38-го на 40-е

место спустилась Россия в ежегодном рейтинге стран по индексу развития ИКТ (ICT Development Index, IDI), опубликованном Международным союзом электросвязи. Доклад МСЭ «Изменение информационного общества», в котором представлен рейтинг IDI по данным за 2012 г., охватывает 157 стран.

Как рассказал руководитель зонального отделения МСЭ для стран СНГ Орозбек Кайыков, индекс IDI рассчитывается на основе трех подындексов, отражающих уровень доступа к ИКТ (определяется по количеству линий фиксированной телефонной связи и мобильных телефонных контрактов на 100 жителей, пропускной способности международных интернет-каналов в расчете на одного пользователя, доли домохозяйств, имеющих компьютер и доступ в интернет), уровень использования ИКТ (учитывает долю пользователей интернета в населении страны и количество

пользователей фиксированного проводного и мобильного ШПД на 100 жителей) и навыки пользования ИКТ жителями той или иной страны (учитывает общий



О. Кайыков: «Первое место в рейтинге IDI третий год подряд занимает Южная Корея»

уровень образования населения). Самое высокое место Россия занимает по навыкам пользования ИКТ – 23-е (кстати, у Белоруссии – 5-е, а у Украины – 11-е). По уровню использования ИКТ мы занимаем 42-место, по уровню доступа к ИКТ – 37-е.

В общем рейтинге IDI в нынешнем году Россия заняла 40-е место, спустившись на две позиции по сравнению с прошлым годом, но при этом увеличив абсолютное значение индекса IDI с 5,94 до 6,19. Согласно программе «Информационное общество (2011–2020 гг.)», в настоящее время Россия должна занимать в рейтинге IDI место не ниже 45-го, так что оснований для «оргвыводов» пока нет.

www.itu.int

Говорим UC, подразумеваем – ..?

Siemens Enterprise Communications провела ребрендинг и теперь называется Unify. Новое имя компании напрямую ассоциируется с понятием «унифицированные коммуникации» (Unified Communications, UC).

Все крупные телеком-вендоры и разработчики ПО встали на рельсы UC, ведущие к заказчику. В этом заезде конкурентным преимуществом может стать не только технологическая оснащенность состава, но и его название. Так, ассоциативная связь нового имени Siemens Enterprise Communications с UC должна послужить четким ориентиром для заказчиков. Кроме того, как заметил Сергей Члек, технический директор Unify в России, в новом бренде компания видит отражение нарастающего тренда на корпоративном рынке телекоммуникационных услуг – смещения акцентов от телефонии в сторону программных решений. «Новый бренд в большей степени соот-

ветствует нашему видению рынка и тому, какой мы хотим видеть нашу компанию в будущем, – отметил Сергей Рассказов, гендиректор Unify в России и СНГ. – Мы не хотим дистанцироваться от Siemens, но это очень многоликий бренд, который играет на многих рынках, от производства стиральных машин до поездов. Мы считаем, что у нас есть все основания работать под самостоятельным именем».



С. Рассказов: «Бренд Unify не должен вызывать вопрос, какие именно продукты и решения предлагаются»

Под новым названием компания сфокусируется на разработке решений, позволяющих максимально упростить деловые коммуникации. При этом Unify полностью сохраняет организационную и управленческую структуры Siemens Enterprise Communications, портфель решений и номенклатуру продуктов, а также подтверждает все ранее заявленные планы по выпуску новых продуктов, развитию партнерской сети и т. п.

www.unify.com

Кадровые назначения

Минкомсвязь

Алексей КОЗЫРЕВ назначен заместителем министра по вопросам развития электронного правительства.

Олег ПАК назначен статс-секретарем – заместителем министра.

Роскосмос

Олег ОСТАПЕНКО назначен руководителем.

Игорь КОМАРОВ назначен заместителем руководителя.

«Ростелеком»

Антон КОЛПАКОВ назначен вице-президентом – директором макрорегионального филиала «Урал».

МТС

Андрей СМЕЛКОВ назначен вице-президентом по зарубежным компаниям.

Михаил ЧЕРНЫШОВ назначен директором макрорегиона «МТС Поволжье».

«ВымпелКом»

Павел БОРОДИН назначен исполнительным вице-президентом по поддержке бизнеса.

Николай ИВАНОВ назначен исполнительным вице-президентом, главным финансовым директором.

Сергей РУБЦОВ назначен вице-президентом, региональным директором Московского региона.

Михаил ТИТОВ

назначен директором по корпоративному бизнесу Белгородского филиала.

«Триколор ТВ»

Александр СТАРОБИНЕЦ назначен директором по маркетингу.

«Компания ТрансТелеКом»

Анна РЕВВА назначена руководителем департамента экономики и финансов.

Tele2

Алексей СИДОРОВ назначен коммерческим директором макрорегиона «Волга-Урал».

«ТехноСерв Тянь-Шань»

Айдарбек ЖОРОБЕКОВ назначен гендиректором.

«Связной»

Ксения МЕЗЕНЦЕВА назначена гендиректором программы лояльности «Связной-Клуб».

Huawei

Вань БЯО назначен главой компании в России.

«Беспомощность крупных операторов»

– так характеризует ситуацию с переносом сроков внедрения MNP директор департамента инфраструктурных проектов Минкомсвязи Дмитрий Алхазов. Регулятор откровенно недоволен тем, что операторы не хотят форсировать сроки, напрягать сети и разочаровывать абонентов, чтобы успеть к назначенной без их согласия дате 1 декабря 2013 г.

Большая тройка единодушна в определении причин переноса сроков: затянувшийся процесс подготовки регулятором нормативной правовой базы и до сих пор неполный ее комплект; необходимость длительного (от нескольких месяцев до года) периода внедрения; неуместность глобальных нововведений на сети в годоводные праздники – дни всеобщего роуминга.

«Могут быть неприятности и с точки зрения лояльности абонентов: 1 декабря придет к нам пользователь другой сети, мы его примем в «МегаФон» – а там ничего не работает», – говорит директор по PR «МегаФона» Петр Лидов.



Регулятор недоволен мобильным бизнес-сообществом

«База данных – самая простая часть этой системы. Но малые сотовые операторы и фиксированные сети не умеют автоматически взаимодействовать с ней – в итоге звонок не будет перенаправлен на номер абонента из одной сети в другую, входящей связи попросту не будет», – поддерживает коллегу директор по маркетингу МТС Вячеслав Николаев.

«Подготовка информационных систем оператора к новым процессам (у нас корректировки потребуют 56 ИС) и синхронизация операторами своих бизнес-процедур – это время. Около 30 операторских компаний сегодня не участвуют в операторском взаимодействии по MNP – они ждут нормативную базу», – добавляет директор департамента по аналитической поддержке GR «ВымпелКома» Алексей Рокотян.

Если регулятор и успеет с правовым полем к 1 декабря, то операторам, чтобы реализовать новые правила на своих сетях, потребуется минимум два-три месяца. По информации ЦНИИС (с 9 октября – оператора БД перенесенных номеров), межоператорское комплексное тестирование запланировано только на ноябрь.

ITK

РОССИЙСКИЙ ПРОИЗВОДИТЕЛЬ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ



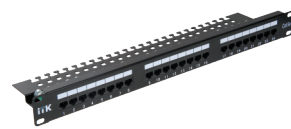
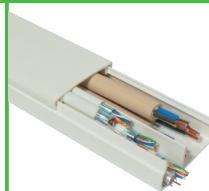
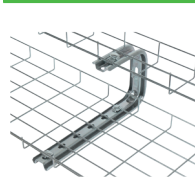
Кабель витая пара:

- Категории: 5E, 6, 6A, 7
- Оболочка: PVC, LSZH, LLDPE
- Экранирование: F/UTP, F/FTP, F/STP
- Solid или Patch



Металлические лотки:

- Проволочные
- Лестничные
- Листовые прокатные



- ✓ Стабильно высокое качество
- ✓ Точное соответствие российским и мировым стандартам
- ✓ Доступное ценовое предложение

Приглашаем к сотрудничеству дистрибьюторов и региональных партнеров

ИНТЕРТЕЛЕКОМПЛЕКТ
Тел.: (495) 54-222-24
e-mail: info@itk-group.ru
www.itk-group.ru



РЕКАМА

Сценарии развития Рунета на пятилетку

представлены в совместном исследовании РАЭК и НИУ ВШЭ «Экономика Рунета 2012-2013». Первый из них, инновационный, предполагает сохранение темпов роста российского сегмента интернета на уровне 2011 г. (33%), свободное развитие игроков, а вместо регуляторных барьеров – стимулирование безналичных платежей и реализацию госпрограмм, направленных на повышение конкурентоспособности и эффективности экономики Рунета. В результате ее совокупный объем увеличится на 35–40% к 2018 г.

Второй сценарий, стабилизационный, отражает ситуацию, складывающуюся в Рунете сегодня, когда не слишком жесткое воздействие регулятора не сдерживает рост проникновения интернета, на рынке идет консолидации игроков, а ежегодные темпы роста замедляются до 15–20%.

Третий сценарий, негативный, может быть вызван к жизни неэффективным

вмешательством регуляторов в развитие отрасли и проявиться в ее монополизации, вследствие чего интернет-рынок будет расти еще медленнее – всего на 6–10% в год.



С. Плуготаренко (РАЭК):
«Сейчас ведется разработка стратегии "Рунет 2020", закрепляющей отношения государства и интернет-бизнеса»

И наконец, развитие событий по четвертому, самому пессимистичному сценарию может спровоцировать глобальный кризис. В этом случае нужно ждать усиления контроля за национальными зонами интернета, закрепления приоритетного статуса телеком-инфраструктуры, отмены сетевой нейтральности и сокращения доступных в Рунете сервисов. Темпы роста его экономики снизятся до 3–6% в год.

Впрочем, результаты самого исследования не предвещают развития событий по последнему сценарию. Консолидированный объем интернет-экономики достиг 831 млрд руб., т.е. 1,3% ВВП. Это на 39% больше, чем в 2012 г.

www.raec.ru

Социальная сеть для бизнес-коммуникаций

Это сеть SAP Ariba, которая объединяет более 1 млн компаний в 186 странах мира, а теперь стала доступна и в России. Как сообщил гендиректор SAP СНГ Виталий Постолатий, полную локализацию решения в SAP планируют завершить к середине 2014 г. Под «полной локализацией» в данном случае понимается соответствие новому законодательству в вопросах поддержки электронных счетов-фактур и иных требований российского законодательства.

После окончания локализации SAP Ariba сможет предложить участникам полностью адаптированный под нужды российского бизнеса (от уровня enterprise до сегмента SMB) ресурс, который позволит компаниям быстро и прозрачно найти поставщика, партнера или заказчика и, что немаловажно, провести всю сделку, включая перечисление денежных средств и оформление документов, непосредственно из бизнес-сети.

В Ariba есть и российские участники – в первую очередь это представители западных компаний, в которых Ariba уже является корпоративным стандартом для процессов закупок, управления отношениями с поставщиками, развития партнерской сети. Ежедневно в Ariba проводится более 250 тыс. транзакций.

Автоматизация работы с поставщиками через бизнес-сеть Ariba помогает участникам в оптимизации цепочек поставок. Об этом свидетельствует опыт западных компаний: например, British Airways, подключившись к Ariba, сократила число своих поставщиков в 7 раз – с 14 тыс. до 2 тыс., а объем запасов – более чем на 200 млн ф. ст. А компания Staples, крупнейший дистрибьютор канцелярских товаров, перейдя на Ariba, на 40% уменьшила количество звонков клиентов в службу поддержки, на 10% сократила выпуск печатных каталогов, в 4 раза снизила затраты на каждую покупку.

<http://global.sap.com/cis>

М & А

«Ростелеком» завершил второй этап реорганизации, в результате чего **«Связьинвест»** и еще 20 акционерных обществ, полностью к нему присоединенные, прекратили деятельность.

ФАС одобрила ходатайство **ABR Investments B.V.** о покупке 10% оператора **Tele2 Россия** и ходатайство **Invintel B.V.** о покупке 40% **Tele2 Россия**. Обе компании аффилированы с банком «Россия».

Netbynet, дочерняя компания **«МегаФона»**, купила оператора **ЛНТ** в Лобне и **«Ратмир Телеком»** в Твери.

MAYKOR за период с августа по начало октября 2013 г. приобрела четыре сервисные компании: **«ОМНИ-ТО»** в Москве, **РЦТО ККТ** и **СибЦККТ** (входившие в **ЗАО «ВТИ»**) в Сибирском федеральном округе и **«Оргтехносервис»** в ЮФО.

Cisco приобрела 100% акций компании **Sourcefire**, специализирующейся в области информационной безопасности.

ФАС удовлетворила ходатайство **Schneider Electric SA** о приобретении прав, позволяющих определять условия осуществления предпринимательской деятельности компании **«Инвенсис Проуэсс Системс»**, путем приобретения 100% доли в уставном капитале **Invensys pls**.

Oracle купила **Compendium**, поставщика облачных решений для контент-маркетинга.

Genesys достигла окончательной договоренности о приобретении корпорации **Echopass** – лидера в сфере облачных контакт-центров для крупных предприятий.

Autodesk подписала соглашение о приобретении отдельных технологических активов компании **Graitec** по проектированию конструкций и автоматизации производства чертежей.

Кбайт
цитаток

«Дело это важное, занимается им государство. Поэтому мы заняли строгую позицию — мы не вмешиваемся.»

«Люди любят выбор, но не любят выбирать.»

«Государство вместо денег предлагает славу.»

«Сейчас народ бежит от государевых денег — замучают отчетностью.»

«Сотрудничество с западными корпорациями имеет давнюю историю. Еще в 16-м веке Борис Годунов отправил на Запад группу из 14 человек. Ни один не вернулся. Так дела обстоят и до сих пор.»

«Сегодня физический эксперимент подменяется компьютерным экспериментом.»

«Мобильный транспорт все еще дорог.»

«Катится поезд по колее. Зачем его на свободное ПО переводить, мешать движению?»

«Мы не комментируем свои планы, мы предоставляем готовый продукт.»

«Человек же полетел в космос, и свободное ПО когда-нибудь взлетит.»

«С увеличением рекламы на телеканале снижается готовность людей платить за этот канал.»

«Все, что могло писать, даже с ошибками, свои лицензии на СМИ уже получило.»

«Если раньше мы попадали на сервис, то теперь — на роботосервис.»

«Сегодня считается, что регулирование целесообразно, если оно устраивает больших операторов.»

«Это приложение позволит убрать из головы руководителя эту информацию и положить ее под руку.»

Школьники включаются в научный поиск

На III Всероссийском фестивале науки были подведены итоги очного этапа четвертого конкурса научно-технических работ школьников «Ученые будущего», организованного МГУ им. М.В. Ломоносова и корпорацией Intel. Цель конкурса — развитие интереса к изучению точных и естественных наук среди школьников.

В этом году на конкурс поступило около 600 заявок от учеников 9–11 классов из государственных и частных образовательных учреждений стран СНГ. Из них для участия в очном этапе было отобрано более 90 работ из Украины, Казахстана и разных регионов России. Школьники представили свои научные проекты в семи категориях: «Химия и нанотехнологии», «Физика», «Биология и науки о жизни», «Техника и инженерные науки», «Науки о Земле», «Математика» и «Программирование». Победителями и призерами конкурса были признаны 30 лучших проектов. На первом месте среди них работа Екатерины Мозгуновой и Дарьи Максимовой из Новосибирска, посвященная синтезу высокомолекулярного микробицидного и противоопухолевого препарата. Другие проекты из первой семерки каса-

ются исследования состояния почвы при загрязнении нефтепродуктами, влияния магнитного поля на посевные качества семян пшеницы, матричных обобщений функций Эйлера и пр.



Кто поедет в Лос-Анджелес?

Конкурс «Ученые будущего» — официальным этапом Intel International Science and Engineering Fair — международного конкурса научных работ школьников, ежегодно проходящего в США. В феврале 2014 г. Intel и МГУ назовут лучшие проекты из числа победителей и призеров «Ученых будущего», авторы которых представят свои исследования на Intel ISEF 2014 в Лос-Анджелесе.

www.intel.ru

Что мешает внедрению «Службы 112»?

Нехватка нормативной правовой базы. По предварительным оценкам Минкомсвязи, для того чтобы регламентировать использование телекоммуникационной инфраструктуры «Службы 112», в до- и переработке нуждаются около 45 действующих нормативных актов.

Принятая в марте текущего года Федеральная целевая программа «Создание системы обеспечения вызова экстренных оперативных служб по единому номеру «112» в Российской Федерации на 2013–2017 гг.» оставила открытым целый ряд технических и организационных вопросов, касающихся проектирования, ввода в эксплуатацию и функционирования телеком-инфраструктуры «Службы 112». Для их решения в Минкомсвязи готовятся изменения в действующую в отрасли нормативную правовую базу.

По словам Дмитрия Кострова, заместителя директора департамента регулирования радиочастот и сетей связи

Минкомсвязи, ведомству предстоит глубоко проработать принципы и порядок взаимодействия сетей общего пользования для прохождения вызовов, поступающих в службу по номеру «112». Также требуется решить, как будут строиться взаимодействие и взаиморасчеты операторов при обеспечении обратного вызова, определить границы зон ответственности операторов связи, МЧС, экстренных служб субъектов Российской Федерации в процессе обработки обращений. Кроме того, пересмотру придется подвергнуть действующие нормативные правовые акты, касающиеся обеспечения установленных действий при проведении системы оперативно-розыскных мероприятий. Еще один важный вопрос, который видит перед собой регулятор, касается технической реализации передачи данных о местоположении обратившегося за помощью абонента.

www.minsvyaz.ru



Начало новой тенденции

Оператор коммерческих ЦОДов компания DataSpace и «Восточный Экспресс банк» подписали договор об аренде последним целого зала под основной дата-центр банка в ЦОДе DataSpace 1, имеющем сертификаты Uptime Institute Tier III Design и Facility.

Сейчас банк имеет собственный дата-центр в Хабаровске, но бурный рост бизнеса и планы выхода на IPO заставили задуматься о масштабировании вычислительных мощностей. Поначалу банк планировал строить новый корпоративный ЦОД, однако анализ ситуации показал, что собственный ЦОД с тем уровнем качества, который обеспечивают современные коммерческие дата-центры, построить не удастся. В результате было решено провести тендер на аутсорсинг услуг ЦОДа. Как отметил председатель правления банка Сергей Власов, условия

о наличии сертификата Tier III в конкурсной документации не было, но оно учитывалось при выборе победителя.

Перевод основных массивов данных банка в ЦОД DataSpace запланирован на предстоящие новогодние каникулы, после чего дата-центр в Хабаровске станет резервным. Президент DataSpace Дэвид Хэмнер считает, что контракт с «Восточным Экспресс банком» может стать началом новой на российском рынке тенденции по размещению основных ЦОДов в коммерческих дата-центрах, которая уже не первый год наблюдается за рубежом. Там банки сначала размещают на коммерческих площадях свои резервные ЦОДы, потом постепенно переводят туда свои основные вычислительные мощности, а собственный корпоративный ЦОД превращают в резервный.

www.dataspace.ru



Д. Хэмнер: «Наша финансовая ответственность перед заказчиком застрахована в крупной международной страховой компании»

Рунет стал чище

за год работы проекта по кибербезопасности «Нетоскоп». По данным «Лаборатории Касперского», количество доменов, распространяющих вредоносные программы, за это время снизилось в 5 раз, количество доменов, участвующих в спам-рассылках, упало на 30%, а количество срабатываний веб-антивируса на территории РФ уменьшилось в 1,5 раза: с 154 млн до 100 млн срабатываний в месяц.

«Нетоскоп» – информационно-аналитический ресурс, посвященный инфобезопасности в доменном пространстве. На сайте публикуются информационные, справочные и аналитические материалы о распространении «зловредов» в интернете и ходе борьбы с вредоносными ресурсами. Посетителям ресурса доступен онлайн-сервис по проверке доменных имен на их использование в злой активной деятельности.

Участники интернет-проекта – Group-IB, Координационный центр национального домена сети Интернет, «Лаборатория Касперского», Mail.Ru,

«Ростелеком», RU-CERT, Технический центр Интернет и «Яндекс». «Нетоскоп» – проект некоммерческий, участники не имеют от него дохода, не размещают там рекламу и т.д. Весь профит – это получение информации о реальной ситуации на рынке, постоянная актуализация баз данных нарушителей и владение объективной информацией о существующих интернет-угрозах.

По словам гендиректора Group-IB Ильи Сачкова, на «Нетоскоп» сегодня ориентируются многие европейские страны, он стал, что называется, best practice для отрасли.

Участники проекта надеются, что взаимодействие в рамках «Нетоскопа» поможет бороться со спамом и наказывать недобросовестных владельцев доменных имен. И для того, и для другого требуется привлечение законодательных органов. И в этом случае «Нетоскоп» может стать общественным инструментом, с помощью которого будут продвигаться те или иные решения.

www.netoscope.ru

Кбайт фактов

ФСО опубликовала для общественного обсуждения проект указа президента, предписывающий создать государственный сегмент интернета и включить его в состав критической информационной инфраструктуры России. Подключение органов госвласти к этому сегменту будет осуществляться в соответствии со специальным порядком.

«ВымпелКом» начал региональную кампанию по запуску сетей четвертого поколения с запуска в коммерческую эксплуатацию сети в Калининграде. В настоящее время покрытие 4G обеспечено на 80% территории города.

МТС запустила тарифную линейку «Умный бизнес» для предпринимателей и корпоративных клиентов, которая предусматривает оплату мобильного интернета и бесплатное предоставление голосовых услуг связи.

«Ростелеком» закупает 656 тыс. телевизионных приставок для оказания услуги «Интерактивное телевидение» на общую сумму 1,183 млрд руб. Поставщиками оборудования станут компании «СмартЛабс», «Промзаказ» и «УЗ Промсвязь».

ГПКС приступила к выбору подрядчика на проектирование, разработку, изготовление, поставку, адаптацию, подготовку к запуску, проведение испытаний на орбите, сдачу в эксплуатацию и поддержку на орбите КА «Экспресс-АМУ2». Начальная максимальная стоимость работ по договору составляет 5,8 млрд руб.

Протяженность разворачиваемых МГТС сетей GPON в Москве превысила 24 тыс. км. В настоящее время сети GPON охватывают 14 тыс. жилых зданий в пределах МКАД, техническую возможность подключения к услугам GPON имеют 1,6 млн жителей столицы.

Кбайт фактов

Приоритетная регистрация доменов .moscow и .москва (для держателей товарных знаков) откроется в начале 2014 г., а к началу лета доменные зоны станут доступны всем москвичам. Как ожидается, новые домены могут в первую очередь заинтересовать учреждения культуры – музеи и библиотеки.

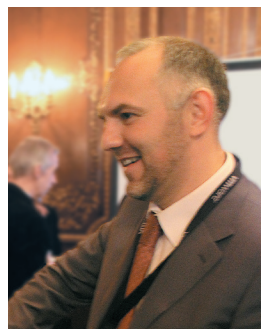
Tele2 перевела холдинговую компанию под российскую юрисдикцию. Теперь все региональные юридические лица оператора принадлежат **ООО «Т2 Рус Холдинг»** (в свою очередь, принадлежащему группе **ВТБ**). Ранее всеми операционными компаниями владела **Tele2 Russia Holding AB** (Швеция), перешедшая под контроль ВТБ после приобретения российского бизнеса у шведской группы **Tele2 AB** в марте 2013 г.



От виртуализации к... виртуализации

Распространяя концепцию виртуализации с серверов и рабочих мест на все новые и новые области, компания VMware, отмечая этот год 15-летия, представила решения для программно определяемых центров обработки данных. В их числе платформа для сетевой виртуализации VMware NSX, технология динамического хранения данных VMware Virtual SAN, новая версия программного комплекса для создания облачной инфраструктуры и управления VMware vCloud Suite 5.5 и VMware vSphere with Operations Management 5.5. В компании подчеркивают, что архитектура программно определяемого ЦОДа упрощает и ускоряет процессы предоставления ресурсов для вычислений, хранения данных и работы в сети, а также управления ими путем автоматизации на основе применения политик. Все решения станут доступны до конца 2013 г.

В текущем году VMware намерена не только расширить «матчасть» для программно определяемых ЦОДов, но и усилить партнерское сообщество в этой области. Во-первых, компания планирует добиться двукратного роста количества партнеров. Во-вторых, она продолжит тесное сотрудничество со стратегическими партнерами в области внедрения решений для управления облаком в существующие бизнесы и разработку новых методов для этих решений.



А. Василенко. В этом году пропорция «столица-регионы» в российском бизнесе VMware составляет примерно 70:30

Кроме того, VMware, чьи позиции традиционно были сильны в enterprise-сегменте, стала предлагать решения и для компаний с менее масштабным бизнесом. По словам Александра Василенко, главы представительства VMware в России и СНГ, теперь на российском рынке компания будет сфокусирована на сегменте рынка general (компания, не входящие в топ-400).

www.vmware.com

Системы видеоконференцсвязи SONY

PCS-XG100S
PCS-XG77S

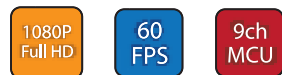


EVI-H100V*

PCS-XG100S

Удвоенная частота кадров расширяет границы общения

Видеоконференцсвязь в формате FullHD (1920x1080) и в сочетании с частотой 60 кадров в секунду позволяет добиться эффекта реального присутствия во время сеансов связи. Встроенный сервер многоточечной связи на 9 абонентов (опция) дает возможность существенно уменьшить затраты на внешний сервер для средних и малых систем. Широкий выбор совместимых камер делает систему универсальной для различных требований к установке.



* Модель показана, как пример совместимой камеры



www.sonybiz.ru

SONY
make.believe

ЗАО «Центр»
420061, Россия,
г. Казань,
ул. Зинина, д. 3а
www.cg.ru

ООО «БизнесМедиа»
115230, Россия,
г. Москва, Варшавское
шоссе, д. 36, стр. 1
www.bs-media.ru

ООО «Микротест»
115114, Россия, г. Москва,
1-й Дербеневский пер.,
д. 5, стр. 2
www.microtest.ru

ООО «АйПи-Ви»
129085, Россия,
г. Москва,
ул. Бочкова, д. 8, кор. 1
www.ip-v.ru

ООО «Красный Сектор»
125222, Россия,
г. Москва,
ул. Рословка, д. 4
www.redsector.ru

ТОО «Tandem TVS»
050050, Казахстан,
г. Алматы,
пр-т Райымбека, д. 169/1
www.ttvs.kz

Будущее инженерных коммуникаций – за интеллектуальными системами

уверены в компании – производителе СКС RiT Technologies. Эта уверенность зиждется на отчетности самой RiT и интересе со стороны заказчиков. Поэтому компания намерена сделать акцент именно на интеллектуальных системах, в частности, на своей платформе Center-Mind. Дарюш Заенц, директор RiT Technologies в России, прогнозирует увеличение доли интеллектуальных систем в структуре доходов компании в 2014 г. Эти системы в первую очередь эффективны для ЦОДов, и хотя сегодня доля дата-центров в общем объеме



Д. Заенц: «Наше отличие в том, что мы не работаем с мелкими заказчиками»

бизнеса компании сравнительно невелика, она ожидает больших заказов в области цодостроения. В работе уже находятся несколько проектов, информация о которых пока не разглашается.

По словам Д. Заенца, компанию интересуют только крупные проекты у крупных же заказчиков. Также в компании не планируют размывать границы в партнерской программе или географиче-

ской экспансии. Конечно, RiT Technologies открыта всем предложениям, но, по мнению Д. Заенца, неразумно иметь в партнерах десятки интеграторов, а в географии – Россию от Калининграда до Владивостока. Лучше иметь десяток проверенных партнеров, с которыми налажено взаимовыгодное сотрудничество, и основательно организовать работу в крупных городах, в первую очередь в Москве и Санкт-Петербурге. И в ближайшее время свою точку зрения по этим вопросам компания менять не собирается.

Такая политика приносит свои плоды: помимо значительного количества проектов по \$10–30 тыс., у RiT Technologies в 2013 г. были и контракты на сумму \$200–400 тыс. Среди реализованных или еще выполняющихся проектов – кабельная система для стадиона «Спартак», поставка системы PatchView для «Зарубежнефти» и ряд других.

www.rittech.com

Какая польза от «больших данных»?

Большинство (70%) российских компаний считают, что Big Data помогут повысить качество принимаемых бизнес-решений, положительно скажутся на их конкурентоспособности и упростят управление рисками. Таковы результаты проведенного корпорацией EMC опроса, в рамках которого 678 ИТ-руководителей российских предприятий поделились своими взглядами на то, какие задачи и возможности они связывают с «большими данными» и ИТ-трансформацией.

35% респондентов подтвердили, что высшее руководство их компаний полагается на результаты анализа «больших данных» при принятии принципиальных бизнес-решений, 31% опрошенных сообщил, что их компании получили конкурентное преимущество в результате внедрения технологий Big Data, а 51% считает, что отрасли, в которых используются такие инструменты, покажут наиболее высокий рост.

Более половины (51%) респондентов согласны, что технологии анализа «больших данных» сыграют решающую роль в выявлении и предотвращении кибератак. Последнее может оказаться важным фактором распространения этих технологий, так как только 67% респондентов в России уверены, что сумеют в случае необходимости полностью восстановить свои данные.

Казалось бы, итоги опроса внушают оптимизм. Однако компании скорее готовы теоретически рассуждать о возможностях и пользе Big Data. Так, 25% компаний, участвовавших в опросе, на данный момент не планируют внедрять технологии «больших данных». 49% компаний не находят, что «большие данные» сегодня помогают им в принятии бизнес-решений, а 16% не определились с точкой зрения по этому вопросу.

<http://russia.emc.com>

Кбайт фактов

Совокупная абонентская база **ТТК** достигла 1,4 млн пользователей. Оператор предоставляет услугу широкополосного доступа в интернет в 209 городах России, кабельное телевидение от ТТК доступно в 87 городах.

«**Дом.ру**» за последний год увеличил количество своих точек Wi-Fi на 80%. К концу сентября 2013 г. компания организовала в 56 городах России бесплатный Wi-Fi доступ в интернет в 4860 популярных местах пребывания, а год назад таких площадок насчитывалось 2700.

«**Авантаж**» и системный интегратор «**Техносерв**» начали строительство в Лыткарино (Московская область, 9 км от МКАД) коммерческого ЦОДа уровня Tier III емкостью свыше 2200 стоек. Суммарная энергомощность ЦОДа составит 20 мВт полезной нагрузки.

«**Открытые Технологии**» разработали и вывели на рынок автоматизированную информационную систему комплексного управления безопасностью, предназначенную для интеграции и анализа информационных потоков в рамках межведомственного взаимодействия в целях обеспечения региональной безопасности.

«**АрселорМиттал Темиртау**» с помощью системного интегратора **БЕЛТЕЛ** модернизировала свою корпоративную сеть, обеспечив на базе технологии VoIP единую платформу для оперативной и диспетчерской связи и единый нумерационный план для всего предприятия.

Число компаний, выразивших желание обмениваться электронными документами, направив в ФНС так называемые информационные сообщения участников электронного документооборота, за полгода выросло более чем в два раза – со 105 тыс. до 250 тыс.

Кбайт фактов

«Авиастар-СП» с помощью компании «Инфосистемы Джет» создала отказоустойчивую ИТ-инфраструктуру: запущены в работу серверные комплексы основного и резервного ЦОДа на платформе IBM Power, настроена синхронная репликация на уровне системы хранения данных, внедрена современная система резервного копирования.

Motorola совместно с проектом Phonebloks планирует создать модульную платформу для смартфонов, открытую для всех разработчиков и производителей аппаратных компонентов и состоящую из центрального «эндоскелета», на котором будут крепиться отдельные модули – компоненты смартфона – процессор, дисплей, клавиатура и т.д. По желанию эти модули можно будет заменять.



Ролевая модель на автомате

Компания «Аванпост» готова изменить ситуацию на рынке систем идентификации и управления доступом к информационным ресурсам предприятия (Identity Management, IDM).

В современной крупной компании для исполнения своих обязанностей сотрудникам необходимо взаимодействовать с десятками информационных систем, и во всех этих ИС человек должен обладать определенным набором прав. Если прав недостаточно, работа встанет, если же прав избыток – это «дыра» в системе информационной безопасности. При этом в любой организации распределение прав постоянно меняется – вследствие как развития ИТ-систем, так и потока кадровых событий (приема на работу, должностных перемещений, пересмотра должностных инструкций и т.п.). «Регулировщиком» этой постоянно меняющейся среды выступают системы IDM.



А. Конусов («Аванпост»):

«IDM-рынок долгое время сдерживали сложности создания ролевых моделей. Теперь они устранены»

Внедрение IDM-решений – процесс сложный и трудоемкий, предполагающий привлечение внешних консультантов и, как следствие, зачастую приводящий к неконтролируемым задержкам и неудачам в реализации проектов. Кардинальное ускорение этого процесса принесет анонсированный компанией «Аванпост» продукт Avanpost Role Manager для автоматизированного создания ролевых моделей и матриц доступа в крупных и средних организациях, использующих IDM-системы.

В настоящее время решение Role Manager протестировано в четырех организациях – и пилотные проекты были реализованы в сроки, которые при традиционной схеме создания ролевых моделей требуются только на разработку первичных документов.

www.avanpost.ru

ARinteg – защищаем Вашу информацию, дорожим своей репутацией!

ARinteg – эксперт в области информационной безопасности. Компания оказывает услуги по оценке и обеспечению соответствия требованиям регуляторов и стандартов по информационной безопасности:

Выполнение требований федерального закона №152-ФЗ «О персональных данных»
Выполнение требований федерального закона №161-ФЗ «О национальной платежной системе»
Выполнение требований Положения Банка России №382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств»
Приведение в соответствие требованиям PCI DSS
Приведение в соответствие требованиям СТО БР
Комплексная защита информации

8 495 221 21 41
www.ARinteg.ru

ARinteg®

ARinteg – член МОО «АЗИ» АЗИ ARinteg – участник НП «АБИСС» АБИСС

ARinteg обладает высшими партнерскими статусами ведущих мировых производителей программного обеспечения

Планы КПССные

«Приветствую членов КПСС – клуба профессионалов спутниковой связи», – так начал свое выступление один из участников конференции SatComRus, которая наконец вернулась в традиционную Дубну. Клуб сейчас сосредоточен на подготовке к запускам новых спутников и получении долгожданной емкости.

Спутниковый ШПД получит «прописку»

Для подключения глубинки России к ШПД Минкомсвязь разрабатывает национальную программу, в которой найдется место и спутниковой связи. Как сообщил Юрий Прохоров, гендиректор ФГУП «Космическая связь», по поручению министра предприятие подготовило предложения по использованию спутниковых технологий, в том числе Ка-диапазона, для обеспечения малонаселенных пунктов современными услугами связи. Пилотные зоны могут быть организованы уже в ближайшее время в регионах, где с 2013 г. партнеры ГПКС предоставляют услуги ШПД через лучи спутника KaSat (Москва и область, Санкт-Петербург и область, Калининград и область). Здесь оператор отрабатывает технологии и бизнес-модели предоставления услуг (за год подключилось более 3 тыс. абонентов), а с запуском в 2014 г. спутников с транспондерами Ка-диапазона – «Экспресс» AM5, AM6 и AM4R – планирует развитие собственной системы высокоскоростного доступа, которая охватит не только европейскую часть России, но и Сибирь и Дальний Восток. ГПКС, добавил Ю. Прохоров, уже подготовило к предстоящим запускам соответствующую наземную инфраструктуру.

Как известно, громко прозвучавший национальный проект спутникового ШПД Ка-диапазона был заморожен (см. «ИКС» №12'2012, с. 39). В письменном приветствии участникам конференции министр связи Николай Никифоров отметил, что в национальной программе ШПД спутниковая связь могла бы занять до 15% (9 млн домохозяйств), но для этого необходимо решить ряд задач – главным образом, пополнить орбитальную группировку современными спутниками. Михаил Кайгородов (Минкомсвязь) уточнил, что хотя в программе раздела спутниковой связи пока нет, но работа над ним ведется. По информации Россвязи, в последние годы запуски новых спутников проводились в основном в рамках реализации ФЦП цифровизации эфирного ТВ, и сегодня назрела острая необходимость создания мощной программы развития орбитальной группировки. Необходимый пакет документов Россвязь уже подготовила.

Следующий год может стать для всей спутниковой отрасли самым урожайным по количеству запусков (пожелаем ей удачи, она так необходима после череды потерь).

Спутники на подходе

Сейчас по заказу ГПКС в производстве находится восемь спутников. Первый из запланированных запусков, КА «Экспресс AM5» в точку 140 град. в.д., должен состояться в декабре этого года. Ранее на 2013 г. планировались также запуски AM6, AT1 и AT2, однако они перенесены на 2014-й, и в результате в следующем году на орбиту должно быть выведено шесть космических аппаратов: кроме уже упомянутых это AM4R, AM7, AM8. Если все пойдет по плану, с марта по ноябрь 2014 г. семь спутников будут введены в эксплуатацию.

По словам Ю. Прохорова, ГПКС завершает этап заключения контрактов на емкость аппаратов, запуск которых запланирован в первой половине 2014 г. Спутники AT1 и AT2 предназначены для СНТВ, и благодаря их эксплуатации оператор прогнозирует увеличение доли спутникового вещания в портфеле своих заказов до 35%. Учитывая, что спутники AM8 и AM7 обеспечат связь Европы с другими континентами, предприятие «Космическая связь», сообщил его гендиректор, совместно с партнерами начало формировать рынки услуг в Индии, Африке, Латинской Америке.

На 2015 г. запланирован запуск тяжелого спутника «Экспресс-AMU1», предназначенного для ТВ-трансляции в HD- и 3D-формате, для его производства в начале нынешнего года ГПКС выбрало EADS Astrium. А после 2015-го предполагается пополнить группировку «Экспрессами» AMU2, AMU3 и AMU4. Уже объявлен конкурс на изготовление спутника «Экспресс-AMU2», его итоги ГПКС подведет не позднее 31 января 2014 г., запуск в планах на 2016 г. Об участии в конкурсе на новый аппарат серии первым заявил Владимир Терехов, глава представительства EADS Astrium в России (с января 2014 г., проведя ребрендинг, будет именоваться Airbus) и гендиректор СП «Энергия SAT» – совместного предприятия EADS Astrium и РКК «Энергия». Можно не сомневаться, что компания не останется в стороне и от последующих тендеров на изготовление AMU3 и AMU4, коммерческие предложения к которым ГПКС уже разработало.

Следующей очередью, до 2020 г., группировку планируется пополнить аппаратами высокоэллиптической орбиты. Сейчас, по словам Игоря Чурсина (Россвязь), для снятия острейшего дефицита услуг связи и вещания в арктическом регионе прорабаты-

вается несколько проектов, в том числе создание системы спутниковой связи с использованием высокоэллиптических спутников «Экспресс РВ»; ГПКС будет предоставлять услуги связи и вещания объектам на трассах Северного морского пути и на архипелаге Шпицберген. Надо сказать, еще в 2007 г. предусматривалось изготовление и запуск в 2009–2010 гг. трех аппаратов – РВ1, РВ2 и РВ3. О намерении совместно разрабатывать спутники «Экспресс РВ» для высокоэллиптических орбит в 2008 г. объявили компания «Информационные спутниковые системы» им. академика М.Ф. Решетнева» (ИСС) и Thales Alenia Space (TAS). Были подписаны соответствующие меморандумы, разработан план сотрудничества, однако до заказа и контрактов дело тогда так и не дошло. Что, впрочем, не помешало укреплению сотрудничества двух компаний, реализовавших за 20 лет порядка двух десятков совместных проектов. Как сообщил Ашот Бакунц (Thales Alenia Space в России), в этом году зарегистрировано совместное предприятие TAS и ИСС – Universum Space Technologies, которое уже выполняет первые проекты. Вероятно, к теме «Экспресс РВ» спутникостроители вернуться на новом «высокоэллиптическом витке».

Кому нужнее дивиденд

Похоже, что с планом Минкомсвязи обеспечить широкополосным доступом глубинку России связана борьба между телеканалами и сотовыми операторами за частоты в диапазоне 694–790 МГц. Первым их законный «цифровой дивиденд» нужен для запуска новых тематических каналов и вещания в HD-качестве, вторым – для развития сетей LTE.

Широкую огласку противостояние получило в марте-апреле благодаря резонансному письму руководителя «Первого канала» вице-премьеру, где были высказаны опасения, что планы Минкомсвязи отдать телевизионные частоты под сети LTE застопорят развитие эфирного телевидения в стандарте HD. Кроме того, НАТ считает, что передача частот сотовым операторам приведет к вынужденным изъятиям тысяч частотных присвоений, ранее выданных телевещателям. В сентябре появились сообщения, что президент отклонил предложение министра связи полностью убрать с этих частот телевидение и отдать их под LTE, а предложение поручил доработать.

Как отмечает Валерий Бутенко, гендиректор ФГУП НИИР, частотная проблема для России традиционна, и если правительство не примет волевое решение в кратчайшие сроки, она так или иначе будет решена на Всемирной конференции радиосвязи в 2015 г. «Полоса определена для вещания, но думаю, что и среди вещателей есть люди со здравым смыслом, и они понимают, что нужно делиться, – считает В. Бутенко. – Вопрос в том, сколько можно отдать, чтобы не снижать темпы внедрения цифрового эфирного ТВ». Однако до консенсуса, видимо, еще далеко. По мнению Валентины Удаловой («Первый канал»), LTE – это дорогостоящий коммерческий проект, и

вряд ли коммерсанты будут продвигаться в малонаселенные пункты. «Если бы было заявлено, что все эти поселки и села будут охвачены ШПД, который приведет в каждый деревянный дом и телевидение, можно было бы говорить о перераспределении частот, – полагает В. Удалова. – Но этого нет. Эфирное ТВ должно сохраниться в нашей стране на долгое время, по крайней мере в малых населенных пунктах. Не дав им ни телевидения, ни ШПД, мы оставим этих людей без актуальной информации».



И. Чурсин и Ю. Прохоров. Россвязь и ГПКС собрали документы для «прописки» спутникового ШПД

Можно возразить, что ФЦП как раз и предусматривает гарантированную доставку в каждый дом как минимум 20 телеканалов, хоть и SD-качества. Тем не менее, если государственное цифровое ТВ-вещание действительно идет к HD, то частоты ему понадобятся, и еще до завершения программы цифровизации эфира. Как сообщил Виктор Пинчук (ФГУП РТРС), предприятие организует пять тестовых зон, в которых будет отрабатывать запуск канала в HD-качестве. «В Европе HD уже стандарт де-факто, и мы к этому тоже идем, – уверен В. Пинчук. – А дальше будет Ultra HD или 4K, это неизбежно».

Сегодня все производители выпускают телевизоры с диагональю больше 50 дюймов, а рост диагонали требует все более высокой четкости. Стоит эта красота недешево, около миллиона рублей, и в обычной квартире надо еще найти место (а лучше отдельную комнату) для кинотеатра. Но имеющие возможность получить такую вещь уже есть – как и операторы, способные доставить им контент 4K. Правда, оператор пока один – Eutelsat, с января этого года ведущий тестовое вещание специального демоканала для Европы. В РТРС считают, что имеет смысл думать уже не только о HD, но и об Ultra HD: к 2020 г. насыщение абонентской аппаратурой достигнет уровня, необходимого для массового внедрения технологии. И сейчас РТРС готовится к этому недалекому будущему – в конце года предприятие планирует продемонстрировать 4K на специализированной выставке в Москве.

Лилия ПАВЛОВА

3-я международная конференция

Cloud & Mobility

CONFERENCE

19 марта 2014

• Москва • Центр Digital October •



Темы конференции Cloud & Mobility 2014:

Облачные услуги для бизнеса

- Cloud Ready: инфраструктура и ПО
- Cloud Automation
- Безопасность
- Провайдер для облака
- Экономика облака
- Облако как платформа для Big Data

Корпоративная мобильность

- BYOD
- Управление мобильными устройствами (MDM)
- Бизнес-аналитика (BI)
- Мобильные устройства и приложения для бизнеса

Облачные провайдеры

- Успешные стратегии для сервис-провайдеров
- Приложения для облака
- SLA

Аудитория

Особенностью конференции является участие в ней большого количества представителей вертикальных рынков, как государственных ведомств, так и крупных российских предприятий, представляющих различные отрасли экономики: финансовый сектор, телеком, ритейл, нефтегаз, страхование, медицину, образование и др.

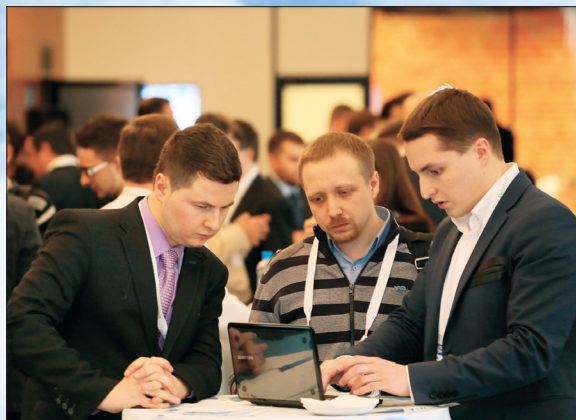


Планы участников Cloud & Mobility 2013 по внедрению облачных решений в ближайшие 1-2 года

Уже применяют	24%
Планируют внедрение частного облака в ЦОДе компании	34%
Планируют приобретать облачные приложения (SaaS)	8%
Планируют использовать PaaS	8%
Планируют использовать облачную инфраструктуру (IaaS)	14%

Приложения, которые участники конференции планируют вынести или уже вынесли на мобильные устройства

Только электронная почта	64%
Система документооборота	30%
Унифицированные коммуникации	32%
Системы CRM, ERP, ECM, BI	18%
Продукты MS Office и подобные	22%



По вопросам спонсорского и делегатского участия
обращайтесь в коммерческий отдел по телефонам:
(495) 229-4978, 785-1490, 502-5080 или по e-mail: dim@iksmedia.ru

www.cloudmobility.ru



Осеннее обострение-2013

Инфобезопасность входит в осень каскадом специализированных форумов, и трехнедельное обострение деловой активности порой напоминает «день сурка» – те же люди, сквозные темы и проблемы. Впрочем, безопасности много не бывает.

Регуляторная гиперактивность

С недавних пор и регуляторы приняли за аксиому, что нормативных актов в инфобезопасности не бывает много. Да и собственно регуляторов. Если несколько лет назад для их перечисления хватило бы пальцев одной руки, то сегодня, как подсчитал Алексей Лукацкий (Cisco), уже не менее 16 госструктур выпустили собственные, причем не согласованные ни с экспертами, ни между собой, нормативные акты в области защиты информации – документы, устанавливающие требования по защите данных, лицензированию деятельности, оценке соответствия, установлению квалификационных требований к специалистам. Только за последние два года издано 200 документов (столько же – за предыдущие 20 лет), и еще около 40 на подходе. Конвейер нормативных актов выдает в среднем четыре документа в месяц. «Раньше безопасники жаловались, что приходится работать со старыми документами, сейчас жалуются, что невозможно работать с огромным количеством новых требований», – резюмировал А. Лукацкий на DLP-Russia.

При обилии документов подзаконного уровня самая вершина нормативной пирамиды только-только формируется. Как отметил на INFOBEZ-EXPO Дмитрий Финогенов (ФСБ), в условиях отсутствия всеобъемлющего международного права и даже единого понятийного аппарата возрастает роль национального права и документов, которые в России принято называть документами стратегического планирования. К таковым он отнес сформулированные в 2012 г. «Основные направления государственной политики по безопасности

АСУ ТП», предусматривающие комплексную программу совершенствования госрегулирования, развития технологий и решения кадровых вопросов до 2020 г., а также вышедший 15 января 2013 г. указ Президента РФ № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ», где ФСБ предписывается создать подразделение, которое должно выполнить практически полный спектр работ по киберзащите российских ресурсов. В указе в первую очередь обращается внимание на защиту ресурсов госорганов, а также на взаимодействие с операторами и компаниями, имеющими лицензии на оказание ИБ-услуг.

Кроме того, по словам Д. Финогенова, в настоящее время дорабатывается законопроект «О безопасности критической информационной



ФСБ и СФ о терминах не договорились

инфраструктуры Российской Федерации», содержащий комплекс правовых, организационных и технических мер по созданию и эксплуатации системы безопасности объектов критической информационной инфраструктуры, а также их взаимодействию с государственной системой обнаружения, предупреждения и ликвидации последствий компью-



терных атак. Как сообщил Д. Финогенов, проект закона уже прошел общественные обсуждения, антикоррупционную экспертизу и первый круг согласований с федеральными органами исполнительной власти.

Очевидно, что в «верхах» всерьез взялись за стратегическое планирование национальной инфобезопасности. Вот и Совет Федерации не отстает, разрабатывает Стратегию кибербезопасности России. Как пояснил Александр Шепилов (СФ), кибербезопасностью государства профессионально занимаются специальные органы, а основным фокусом, ради которого СФ инициировал разработку стратегии, должна стать кибербезопасность бизнеса и гражданина. При этом упор будет сделан на технической стороне вопроса, которая «более понятна». Это заявление свидетельствует о некотором смещении акцентов в идеологии документа.

Напомним, в 2012 г. сенатор Руслан Гаттаров объявил о разработке Стратегии кибербезопасности России как в первую очередь политического документа («не слишком технического»), в котором должны быть обозначены стратегические подходы к обеспечению кибербезопасности государства, бизнеса, общества, отдельных граждан. Возможно, перефокусировка произошла в процессе обсуждений проекта документа. По словам А. Шепилова, еще одна поправка, вероятно, будет принята по рекомендации Минкомсвязи: в окончательной редакции предлагается назвать его не стратегией, а концепцией стратегии кибербезопасно-

сти России, что упростит согласование документа со всеми заинтересованными ведомствами. Это можно будет сделать до конца текущего года, после чего «в понятные сроки» можно доработать собственно стратегию.

По всей видимости, концептуальный документ согласовать легче, чем стратегию. В то же время в каком бы статусе этот документ ни принимался, его коренной смысл остается неопределенным. Как заметил Дмитрий Костров (Минкомсвязь), сегодня в российском законодательстве термин «кибербезопасность» как таковой отсутствует – и, возможно, следует для начала все же законодательно его ввести. А. Шепилов полагает, что «терминологический спор» затормозит продвижение документа. «Мы не считаем вопрос терминологии принципиальным. Гораздо принципиальнее вопрос конкретных действий и мер, которые будут прописаны и реализованы», – уверен представитель Совета Федерации. Кто прав? Думается, все понимают, что «кибербезопасность» – это безопасность в киберпространстве. Но стоит ли наступать на очередные грабли, полагаясь на интуитивный понятийный аппарат? Ведь сколько раз убеждались: как договоришься о терминах – так потом и пойдет работа...

Персданные утекают

Особое место в законотворческой деятельности занимает закон «О персональных данных», очередные изменения в который сейчас подготовлены. Как пояснил А. Шепилов, эти изменения нацелены на снижение технических требований к защите ИСПДн компаний, обрабатывающих персональные данные. В настоящее время большинство операторов персданных эти требования не выполняют, предпочитая выплачивать незначительные штрафы. А если бы выполняли, то, по словам А. Шепилова, общие затраты на их реализацию составили бы 5% ВВП. «Это огромные деньги, и у большинства компаний нет средств на исполнение высоких требований по защите ИСПДн, – признал представитель СФ. – Мы рассчитываем, что принятие законопроекта хотя бы частично снимет существующие противоречия. Думаем,

что, если дело не касается гостайны, государство должно оставить право выбора систем защиты персданных операторам, но гораздо более жестко спрашивать за выявленные факты их утечки». Одновременно со смягчением требований к хранению данных сенаторы предлагают увеличить штраф за утечки с нынешних десяти тысяч до миллиона рублей.

Пока же утечки становятся все масштабнее. В первом полугодии 2013 г. аналитическим центром InfoWatch зафиксировано в мире 496 случаев утечки конфиденциальной информации, что на 18% больше, чем за аналогичный период прошлого года, сообщила на конференции DLP-Russia Наталья Касперская (ГК InfoWatch). На самом деле утечек гораздо больше: по оценке InfoWatch, число зарегистрированных случаев, упомянутых в СМИ, публичных материалах компаний и госорганов, составляет лишь 1–5% числа всех подобных инцидентов. По данным центра, скомпрометировано более 258 млн записей, причем больше всего (93,8%) утечек информации связано с персональными данными и чаще всего – из госорганов и медицинских учреждений. Количество случайных и злонамеренных утечек примерно равно.

Интересно, что по количеству опубликованных утечек (42 случая) Россия вышла на второе место, обогнав Великобританию. Безусловным лидером являются США (312 случаев или 62,9% всех произошедших) – главным образом потому, что в этом государстве действует закон, обязывающий компании размещать в прессе информацию о каждом случае компрометации данных. Если такая норма будет принята у нас, это окажет позитивное влияние на рост рынка DLP-систем, считает Н. Касперская. Но нужно ли самим компаниям обязательство «посыпать голову пеплом»? С другой стороны, поскольку после опубликования понесенные убытки списываются, есть риск, что у нас быстро все «утечет и спишется»...

Цена безопасности

Подсчитать реальный размер убытков от утечки информации крайне

сложно, поскольку к ним относят и репутационные потери, и косвенный ущерб (прямой ущерб указывается крайне редко). Обнародованный в СМИ ущерб (затраты на ликвидацию последствий утечек, судебные разбирательства, компенсационные выплаты), понесенный компаниями вследствие утечек информации в первом полугодии 2013 г., составил \$3,67 млрд, сообщает аналитический центр InfoWatch. В действительности же, если учесть подводную часть айсберга незарегистрированных случаев, ущерб гораздо больше.

Сейчас в мире, по данным последнего отчета Ponemon Institute «2013 Cost of Cyber Crime Study», среднегодовой уровень расходов на противодействие кибератакам в расчете на одну организацию составляет \$11,56 млн (от \$1,3 до \$58 млн), что на 26% больше, чем в 2012 г. Ущерб, наносимый кибератаками российским компаниям, оценили эксперты «Лаборатории Касперского» совместно с аналитической компанией B2B International. Оказалось, что крупные предприятия несут убытки, связанные с ИБ-инцидентами, в размере \$650–700 тыс., мелкие – порядка \$14 тыс. По мнению аналитиков, существенно уменьшить угрозы и уровень расходов на борьбу с киберпреступностью помогают современные аналитические средства в сфере безопасности и сетевых технологий (например, системы Security Information and Event Management, SIEM). Однако, как показывает практика, убедить бизнес в необходимости внедрения таких систем весьма непросто.

Принято считать, что бюджет на информационную безопасность составляет 5–10% бюджета ИТ. Как заметил на DLP-Russia Рустэм Хайретдинов (ApperCut Security), по этой логике цена разминирования должна составлять 5–10% стоимости мины. «На самом деле расходы на безопасность должны рассчитываться исходя из рисков, а не из бюджета ИТ, – убежден эксперт. – Пока же работает остаточный принцип». Инфобезопасность не приносит денег, но окупается в комплексе, резюмировали и участники дискуссии об эффективности ИБ, развернутой в рамках Infosecurity



П. Головлев (справа): «Бюджет инфобезопасности – это доверие руководства плюс русский "авось"»

Russia. Как заметил Павел Головлев (СМП Банк), 75% организаций банковской отрасли могут вложить в информационную безопасность в год всего-навсего 5 млн руб., поскольку в маркетинговом триумвиате «быстро, качественно, дешево» бизнес всегда выбирает первую и третью позиции. «Безопасность – это категория качества, которая останется в провале, пока в умах законодателей не произойдет смена идеологии. – уверен П. Головлев. – До сих пор на информацию пытаются "натянуть" вещное право, а она сродни здоровью человека. Соответственно, защита информации сравнима со здравоохранением. Чтобы инфобезопасность была реальной, она должна стать социальным бизнесом».

Когда сдвинется парадигма?

В нынешнем году интересное исследование отечественного рынка информационной безопасности обнародовала группа независимых российских экспертов. По их оценке, объем рынка составляет \$1399 млн. Из 13 рассмотренных сегментов наибольшую долю занимают сетевая безопасность (\$570 млн) и системы антивирусной защиты (\$400 млн), за ними следуют аппаратные средства двухфакторной аутентификации (\$91 млн) и консалтинг инфобезопасности (\$83 млн). Единицы процентов в общем пироге занимают системы IDM, инструментальные средства анализа защищенности, системы DLP, системы защиты от НСД, образовательные услуги, системы контентной фильтрации,

системы сбора и корреляции событий, мероприятия по безопасности, аудит безопасности.

На этом подробном сегментированном рынке не представлены системы «высшего пилотажа» – анализа рисков на основе «больших данных». Их просто пока не существует. Как отметила в своем программном выступлении на DLP-Russia Н. Касперская,

большие данные уже анализируются в маркетинге, в рознице, в интернет-рекламе, в поисковых системах, в социальных сетях – но не в информационной безопасности предприятий. Сегодня системы защиты информации используются разрозненно: отдельно контентные (DLP, антиспам, веб-фильтрация), отдельно инфраструктурные (антивирус, межсетевой экран, SIEM, IDS/IPS, НСД и др.), отдельно шифровальные. При этом анализируются только технические явления. Между тем основные риски в инфобезопасности создают люди (халатность, переманивание, хищение информации, инсайд).

К слову, проведенный в августе-сентябре 2013 г. компанией LETA анонимный опрос 1100 офисных работников из нескольких сотен российских компаний различных сфер деятельности показал, что каждый пятый готов за вознаграждение передать третьим лицам конфиденциальную информацию, к которой он имеет доступ; 85% не осознают угрозы взлома корпоративной сети через электронную почту и открывают письма от незнакомых отправителей, 60% пересылают корпоративную информацию на личные почтовые ящики, чтобы поработать с ней из дома и т.д.

Системы комплексного анализа рисков и угроз на основе «больших данных» о персонале и инфраструктуре предприятия, способные минимизировать угрозы человеческого фактора, появятся, по мнению Н. Касперской, в ближайшие

три-пять лет. Они смогут анализировать поведение людей, проводить совместный анализ всех источников и потоков данных для раннего выявления и прогнозирования угроз, выполнять ретроспективный анализ, формулировать единые решающие правила для вычисления итоговых рисков персонала и ИБ-систем. «Это позволит перейти от парадигмы реагирования на угрозы к парадигме детектирования и оценки роста рисков в критических точках», – считает Н. Касперская.

Тенденция интеллектуализации систем защиты информации обозначилась вполне явно. Как заметил на Infosecurity Russia Игорь Ляпунов («Инфосистемы Джет»), все средства «айтишного» бизнес-анализа проецируются на инфобезопасность, и способы обработки собираемых массивов «больших данных» настолько сложны, а задачи настолько неординарны, что создание систем такого класса дает большой драйв самим разработчикам.

Впрочем, наверняка системы такого уровня должны стоить дорого – и совсем не очевидно, что бизнес, с трудом выделяющий бюджеты на «простую инфобезопасность», будет готов платить миллионы долларов даже за «самую умную безопасность».



При всем тематическом сходстве DLP-Russia, InfoSecurity Russia и INFOBEZ-EXPO «лица необщим выраженьем» обзавелось каждое мероприятие.

Отличительной чертой InfoSecurity остается ее выставка, собирающая наибольшее количество экспонентов. Экспозиция INFOBEZ в этом году сильно скукожилась, зато деловая программа креативила все три дня. На DLP атмосфера интеллигентная: аналитика, прогнозы, экспертиза. К слову, со следующего года это мероприятие «расфокусируется», тематика его расширится, а сама конференция будет переименована в Business Information Security Summit (BISS). То есть следующей осенью появится еще одно мероприятие «про всю инфобезопасность»...

Лилия ПАВЛОВА

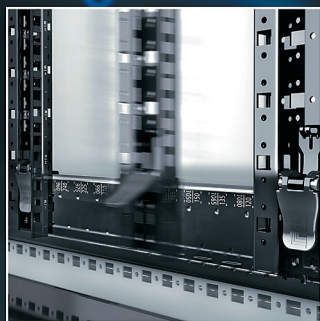
Rittal – The System.

Faster – better – worldwide.

Make IT easy.

**Новая стойка TS IT с технологией монтажа комплектующих без инструментов.
Простой и быстрый монтаж.**

Новый мировой стандарт для серверного и сетевого оборудования.



Make IT fast.

Быстрая сборка и удобная система монтажа комплектующих без инструментов.

Make IT simple.

Совершенная организация распределения кабеля.

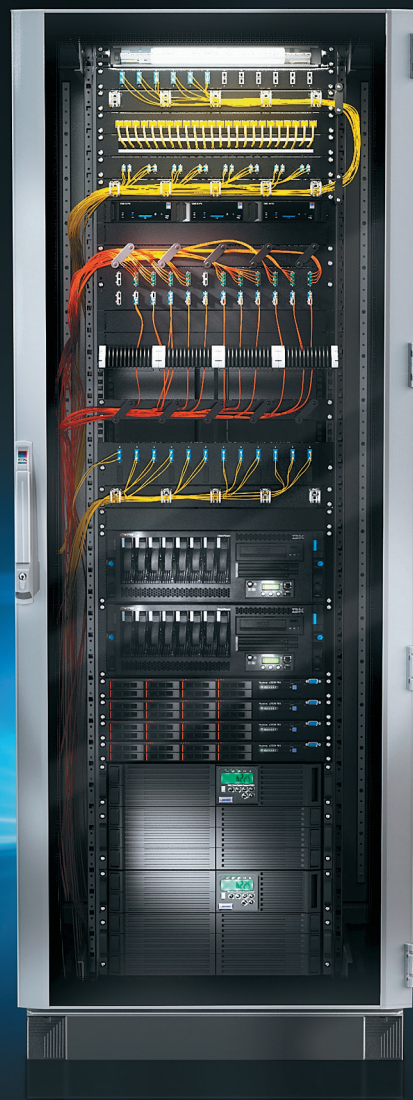


Make IT flexible.

Различные варианты дверей для серверного и сетевого оборудования.

Make IT perfect.

Дополнительные многочисленные функции и высокая энергоэффективность.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

www.rittal.ru



Кому полезны открытые данные?

Тема открытых данных значится в повестке дня «Группы восьми», G8. Она актуальна и экономически выгодна и государству и бизнесу.

Государству раскрытие данных о деятельности органов госвласти обещает повышение качества оказания гражданам электронных госуслуг и ускорение реакции на запросы бизнеса и общества. Бизнесу – даст возможность принимать решения, опираясь на достоверную информацию, создавать новые рабочие места, находить квалифицированных сотрудников. При этом наибольшую выгоду использование открытых данных сулит

чикам мобильных приложений, создав для них специальную инфраструктуру и открыв API к единой мобильной платформе. Вот некоторые цифры, приведенные на RIW2013 Дмитрием Бехтеревым (ДИТ Москвы): за полгода с момента открытия мобильной инфраструктуры города для разработчиков на специализированном портале зарегистрировались более 400 команд, ведущих разработку приложений с использованием открытых данных, 23 из которых уже доступны для скачивания из AppStore и Google Play. Основная тематика таких продуктов – транспортная, культурная и справочная.

Вдохновляют разработчиков мобильных приложений на использование в своих продуктах открытых данных городские конкурсы, организуемые ДИТ совместно с вендорами. Только за лето их было два: «Москва глазами разработчиков», проводившийся в партнерстве с Microsoft, и Moscow APP Contest 2013 – с Google и Apps4All. Надо сказать, что подобные конкурсы регулярно проходят за рубежом. Примером может служить NYC Big Apps с призовым фондом \$50 тыс. и задачей найти команды, чьи приложения на основе открытых данных позволяют сделать Нью-Йорк еще лучше и комфортней. По словам Виталия Власова (НКО «Открытый город»), разработчики приложений участвуют в нем не столько ради вознаграждения, сколько ради возможности показать потенциал своей команды инвесторам. Объем инвестиций, которые удастся привлечь, зачастую исчисляется миллионами долларов.

Московское правительство крупных денежных призов не обещает, зато берет за продвижение наиболее успешных приложений и поддержку их пользователей. Так, приложение «Мамнадзор», победившее в конкурсе Moscow App Contest 2013, получило статус официально рекомендованного правительством Москвы. Его автор, основатель Gaika Group Максим Каневский, признался, что на участие в конкурсе его команду вдохновил выделенный на портале data.mos.ru раздел Summer, объединивший 39 наборов открытых данных по теме летнего отдыха. А процесс разработки от определения целевой аудитории – молодых женщин, готовящихся стать или уже ставших мамами, – до его готовности к публикации в Google Play у команды программистов из пяти человек занял пять рабочих дней.

В планах ДИТ на три-четыре месяца, по словам Д. Бехтерева, предоставить разработчикам приложений возможность монетизировать свои продукты, а также сделать доступными для игроков краудсорсинга сервисы открытого правительства города. Так что органам, ведающим раскрытием данных на федеральном уровне, по-прежнему будет на кого равняться.

Александр КРЫЛОВА

А тем временем...



В октябре Минэкономразвития РФ объявило конкурс на создание и сопровождение портала открытых данных Российской Федерации, а в Москве был перезапущен городской ресурс – портал data.mos.ru.

ИТ-компаниям, перед которыми откроются новые возможности для бизнеса. Они смогут разрабатывать на их основе продукты и сервисы. И в этом смысле открытый конкурс, объявленный Минэкономразвития России, по теме «Создание и сопровождение портала открытых данных Российской Федерации» стоимостью 10 млн руб., тоже можно рассматривать как новую возможность.

В масштабах страны, президент которой в июне текущего года поставил свою подпись под Хартией открытых данных G8, сделано многое. С 1 июля 2013 г. вступил в силу Федеральный закон № 112-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и Федеральный закон "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления"», обязывающий ведомства всех уровней размещать открытые данные в сети интернет в чело- веко- и в машиночитаемом виде. И, что немаловажно, подготовлены все подзаконные акты, необходимые для регламентации этого процесса.

Однако многие вопросы еще не решены. В их числе обучение госслужащих работе с открытыми данными, формирование спроса у бизнеса и граждан на подобную информацию, выработка критериев оценки эффекта, как социального, так и экономического, от раскрытия данных. Они стоят на повестке дня Совета по открытым данным при Правительственной комиссии по координации деятельности открытого правительства, который ориентируется на достижения субъектов РФ – пионеров в этой области, таких как Москва, где портал data.mos.ru был открыт за полгода до вступления в силу закона № 112-ФЗ.

В московском Департаменте информационных технологий сделали ставку на сотрудничество с разработ-



А. Ермолаев (ДИТ Москвы):
«Мы заинтересованы в диалоге с разработчиками, чтобы понимать, какие открытые данные им нужны»

Организация эксплуатации и причины отказов в ЦОД

ВПЕРВЫЕ В РОССИЙСКОЙ ПРАКТИКЕ!

Международное консалтинговое агентство iKS-Consulting подготовило исследование двух важных и взаимосвязанных тем:

- 1) Причины отказов инженерных систем в дата-центрах
- 2) Методы снижения риска отказов оборудования

Первоочередная задача исследования – помочь руководителям и менеджерам ЦОДов, консультантам и всем заинтересованным участникам рынка выявить основные «болевые точки» современных дата-центров.

К участию в опросе были приглашены эксперты из коммерческих и корпоративных ЦОДов. В ходе исследования были выявлены **основные тенденции и закономерности** текущего состояния процессов эксплуатации инженерных систем дата-центров.



Представленные в отчете **выводы и рекомендации** могут быть использованы как оперативным руководством дата-центров, так и заказчиками их услуг – внутренними и внешними. Они помогут избежать фатальных ошибок при планировании работ, а также дадут возможность, основываясь на конкретном статистическом материале, аргументированно спланировать и защитить бюджет.

В ОТЧЕТЕ:

- роль и место отказов инженерного оборудования ЦОДов
- типы причин, по которым возникают отказы
- основные проблемы, связанные с сервисными подрядчиками и внешними услугами
- роль и место человеческого фактора в возникновении отказов
- основные недостатки взаимодействия внутри службы эксплуатации и проблемы совместных действий с сервисными подрядчиками
- значение систем управления эксплуатацией
- наиболее эффективные методы снижения числа отказов инженерного оборудования дата-центров
- применяемые модели всех видов технического обслуживания
- роль и место регламентного обеспечения в задачах эксплуатации инженерных систем ЦОДов
- способы организации службы эксплуатации, причины недостаточной численности и квалификации персонала
- жизненно важные для функционирования ЦОДа статьи операционного бюджета.

Параметры отчета:

- Количество страниц: **50**
- Цена: **60 тыс. руб.** без НДС
- Выход: **сентябрь 2013 года**

Подробная информация:

iKS-Consulting
+7 (495) 505-10-50
E-mail: ef@iks-consulting.ru

www.iks-consulting.ru

Как регулировать стагнацию

Замедление темпов роста экономики, в том числе телекоммуникаций, становится все заметнее. Назрела ли необходимость в кардинальном изменении правил игры или важнее обеспечить преемственность и в итоге защиту ранее сделанных участниками рынка инвестиций?

Обмен мнениями между представителями операторского сообщества и Минкомсвязи РФ состоялся на 14-й международной конференции АДЭ «Состояние и перспективы развития IP-коммуникаций и IP-сервисов в России».

Снова застой?

Телеком – чуткий индикатор изменений в экономике. И то, что на этом рынке постепенно перестают работать привычные парадигмы и успешные модели развития, по мнению Евгения Васильева (МТТ), говорит о вступлении России в полосу стагнации. Так, за минувший год уменьшилось количество слияний и поглощений. Такие крупные сделки, как покупка «Мегафоном» Yota, завершенная в 2013 г., начинались намного раньше. Операторы большой тройки приостановили покупку региональных интернет-сервис-провайдеров и, по информации из открытых источников, сами подумывают о продаже части своих ШПД-активов.

Иными словами, ставшее расхожим определение «бурно растущий» меньше подходит к сегодняшнему состоянию рынка телекоммуникаций, чем год назад. Вместе с тем любой системный кризис – это время возможностей, считает Е. Васильев, указывая, что недаром ряд успешных ныне компаний начинали свой бизнес в 2008–2009 гг. В таких условиях важно, насколько регулятор готов заботиться о профессиональных участниках рынка и прилагать усилия к сохранению динамики его развития.

Последний плацдарм

Широкополосный доступ – последний быстро растущий сегмент в традиционной связной модели. От сохранения темпов роста в этом сегменте зависит решение по-прежнему актуальной для нашей страны проблемы «цифрового неравенства», о необходимости покончить с которым много говорится на самом высоком уровне.

Понятно, что наиболее остро эта проблема стоит в субъектах РФ, коммерчески мало привлекательных для федеральных игроков рынка ШПД. В аутсайдерах по проникновению высокоскоростного доступа в интернет сегодня числятся Камчатский край, Сахалинская область, республики Саха (Якутия), Калмыкия, Дагестан. Уровень проникновения интернета в Чеченской республике аналитиками оценивается в 0,55%. В большинстве населенных пунктов в этих регионах монополистом является «Ростелеком», а сильных местных игроков, способных составить ему конкуренцию, нет. Вот и получается, что широкополосный доступ в интернет многим жителям не по карману. Они не пользуются услугой, а операторы не получают доходов, часть которых могли бы направить на строительство новых сетей.

Выйти из замкнутого круга игрокам рынка могла бы помочь поддержка в форме частичного или полного субсидирования со стороны государства, чей социальный заказ на обеспечение ШПД для его граждан они выполняют. Государство вроде бы не против. Но пока, признался Илья Мизикин («ВымпелКом»), каждый «заход» оператора в новый российский город – это бег с препятствиями. Наиболее тяжело дается операторам согласование размещения оборудования в домах. За пять лет стоимость аренды выросла на 70% и сегодня исчисляется тысячами рублей в месяц. К тому же жители не очень хотят, чтобы в их домах и подъездах стояло какое-либо оборудование. Приходится собирать подписи, проводить общие собрания и объяснять выгоды присутствия в доме интернет-провайдера.

С не меньшими сложностями, констатировал И. Мизикин, операторы сталкиваются при получении заключения на строительство сетей связи в субъектах Российской Федерации. Экспертиза всех проектов независимо от местонахождения населенного пункта, в котором они реализуются, проводится в Москве и занимает в среднем три месяца.

Словом, для того, чтобы строить широкополосные сети по всей России, развивать свой бизнес и сохранять темпы роста, операторам нужна поддержка регулятора в форме изменения нормативной правовой базы, причем не только отраслевой. Поправки требуются, например, в Жилищный кодекс и ряд других документов.

В режиме открытости

По заявлению представителей Минкомсвязи, ведомство уже выступило с несколькими подобными инициативами. В их числе внесение изменений в Земельный кодекс для облегчения операторам строительства сооружений связи и в Жилищный кодекс – с целью упрощения доступа в здания и сооружения для размещения средств и оборудования связи. Эти меры позволят сократить затраты на строительство сетей, будут способствовать развитию инфраструктуры и в конечном счете помогут снизить стоимость услуги широкополосного доступа для конечных пользователей в субъектах РФ.

«Мы достигли согласия о выделении бюджетных средств, чтобы совместно с операторами строить магистральные сети связи до населенных пунктов, еще не имеющих высокоскоростных каналов», – сообщил Олег Кузнецов (Минкомсвязь). В настоящее время в ведомстве активно прорабатываются варианты проектной части такого строительства.

Кроме того, в соответствии с принятой правительством в конце 2012 г. «дорожной картой» по развитию конкуренции и совершенствованию антимонопольной политики в Минкомсвязи разработаны Концеп-

ция межоператорского взаимодействия и Правила недискриминационного доступа.

И если недискриминационный доступ как аспект межоператорских взаимоотношений, по признанию Элдара Разроева (Минкомсвязь), остается достаточно сложным для понимания даже внутри операторского сообщества, то подходы к решению проблем недискриминационного доступа к инфраструктуре, которая может использоваться для размещения средств связи, специальной рабочей группой уже сформулированы. Например, предложено приравнять пассивную инфраструктуру к таким инженерным коммуникациям зданий, как электричество, свет, водоснабжение и т.д., и обязать прокладывать ее собственников жилых домов и бизнес-центров. Аналогичные требования планируется выдвинуть к реконструируемым зданиям, а затем установить переходный период для развертывания этой инфраструктуры во всех остальных еще не охваченных ею домах.

Другая группа объектов, которую операторы хотели бы задействовать: канализация, мосты, столбы – в случае ее принадлежности госоргану или муниципалитету должна стать доступной для размещения их оборудования по определению. Что же касается этих объектов, находящихся в частной собственности, то тут провозглашается создание равных для всех операторов условий доступа. Иными словами, если хотя бы одному из операторов удалось на таком объекте обосноваться, то условия его подключения становятся публичными и должны использоваться для всех остальных.

По словам Э. Разроева, основные принципы Правил недискриминационного доступа уже сформированы и в ноябре, возможно, будут представлены на Правительственной комиссии по связи.

С ГОТОВНОСТЬЮ К ПОДВИГУ

Однако не стоит ожидать, что все эти благие намерения регулятора осуществляются в короткие сроки. Постановлением Правительства РФ от 17.12.12 № 1318 для поправок в нормативные правовые акты предусмотрена непростая многоступенчатая процедура.

По опыту Виталия Крейнделина (Россвязь), выпуск нормативного правового акта средней сложности и не очень спорного занимает около девяти месяцев. Ровно столько времени в среднем проходит с момента размещения уведомления на сайте reg.gov.ru о намерении разработать такой правовой акт (1-й этап) до его официальной публикации (завершающий, 13-й этап). На любом из этих этапов согласующие органы – Минэкономразвития, ФСБ или Минюст – могут вернуть документ на доработку, что еще более затягивает процесс. «Выпуск нормативного правового акта, – заключил В. Крейнделин, – можно приравнять к подвигу».



Инициативы выдвинуты. Но может статься, что до той поры, как они пройдут все обсуждения, изменения, заключения, антикоррупционные проверки и проч., ситуация на телекоммуникационном рынке снова изменится.

Александра КРЫЛОВА



Энергия интеллекта

Ведущее аналитическое агентство России и СНГ в сфере телекоммуникаций, ИТ и медиа

- Аналитика
- Стратегии
- Бизнес-планирование
- Информационно-аналитическая поддержка
- Потребительские опросы в B2C и B2B сегментах



Лондон



Киев



Москва



Алматы

ИТ

Телеком

Медиа

Контент и сервисы

Системная интеграция

Голосовые услуги

Платное ТВ

Навигация и LBS

Дата-центры

ШПД

Мобильное видео

M2M

Облачные сервисы

Мобильный интернет

Игры

NFC

ИТ инфраструктура

VAS

Интернет-порталы

E-commerce

Офисная техника

Межоператорские услуги

Видео-контент

Теле-медицина

Сильнодействующее средство от адептов корпоративной мобильности

Проникновение личных мобильных устройств в ИТ-инфраструктуру компаний вызывает головную боль у служб ИТ- и инфобезопасности. Но, похоже, лекарство от нее уже найдено.

На глобальном рынке

Как выяснилось на октябрьском «Дне корпоративной мобильности», лабораторией, где такие «препараты» разрабатываются, служит экосистема, которая активно формируется сегодня в мире на основе мобильного корпоративного ПО, ИТ- и бизнес-услуг. Программное обеспечение для мобилизации бизнеса Елена Семеновская, директор по исследованиям IDC Russia, подразделяет на три вида: платформы разработки мобильных приложений (Mobile Enterprise Application Platform, MEAP), средства корпоративной мобильной безопасности (Mobile Enterprise Security, MES) и ПО управления мобильным предприятием (Mobile Enterprise Management, MEM).

Последний вид ПО, MEM, предназначается для решения проблем, возникающих в компаниях в результате перехода к концепции BYOD, и включает в себя системы Mobile Device Management – для управления личными устройствами, подключенными к корпоративной ИТ-инфраструктуре, и Mobile Application Management – для управления использованием и распространением в ней мобильных приложений.

Если же функциональности этих двух систем недостаточно, применяются программные средства обеспечения корпоративной мобильной безопасности, MES. С их помощью организуются управление безопасностью, защита от уязвимостей и угроз, контроль аутентификации и доступа, реализуются меры по защите информации при использовании в компании мобильных устройств, в том числе принадлежащих сотрудникам.

Пока на мировом рынке платформы разработки приложений для мобилизации бизнеса – самый объемный сегмент: по прогнозу IDC, к концу 2016 г. он достигнет \$3,7 млрд. Зато по темпам роста средства корпоративной мобильной безопасности и ПО для управления мобильным предприятием его обгоняют. К началу 2017 г. сегмент MES вырастет на 29,6% (до \$2,5 млрд), а MEM на 31,8% (до \$1,8 млрд) – против прироста в 24,1% у MEAP. В целом же объем глобального рынка мобильного корпоративного ПО на тот момент будет составлять \$7,8 млрд, при \$3 млрд в 2013 г.

В России

На нашем рынке, где, по словам Е. Семеновской, заказчики подобных решений демонстрируют «пилотный» подход к мобилизации своего бизнеса и где преобладают инфраструктурные проекты, основные затраты ассоциируются пока с закупкой мобильных устройств, а не

лицензий на ПО. Вместе с тем организация мобильных рабочих мест для сотрудников всех уровней в России в 2013 г. стала массовым явлением, констатировал Сергей Орлик, директор «Центра корпоративной мобильности» (ГК «АйТи»). А значит, вопросы централизованного приобретения программного обеспечения для них придется решать в самое ближайшее время.



С. Орлик: «В решениях контейнеризации можно подменять базовые функции устройств защищенными»

Пока же на повестке дня у руководителей ИТ-департаментов – адаптация находящейся в их ведении инфраструктуры, внедрение систем управления мобильными устройствами и систем управления мобильными приложениями, создание базовых прикладных решений общего назначения. Именно в этом году впервые на «Дне корпоративной мобильности» прозвучал тезис: «Для обеспечения безопасности очень важно запретить или ограничить доступ к корпоративным ресурсам мобильных устройств Apple с несанкционированной производителем разблокировкой доступа к файловой системе (jailbreak)». И вот почему: после такого «взлома» у владельца iPhone или iPad появляется недоступная ранее

возможность устанавливать на свое устройство любые приложения, в том числе из сомнительных источников, что чревато его заражением троянками и вирусами.

Выход есть!

Ответом на вызовы и угрозы мобильной безопасности, а следовательно, лекарством от головной боли для руководителей служб ИТ и ИБ может стать контейнеризация – отделение персональных данных и приложений сотрудника от его корпоративных данных и программ с помещением последних в специальный контейнер. Эта технология минимизирует риски, возникающие после принятия в компании подхода BYOD. Она обеспечивает авторизованный доступ к мобильным приложениям и контроль их соответствия политикам компании, безопасную мобильную передачу данных, их хранение в зашифрованном виде и столь же безопасный обмен данными между серверным ПО и приложениями, установленными на смартфонах. А кроме того, в контейнере для корпоративных приложений можно применять технологии Push для распространения обновлений политик.

Сегодня контейнеризацию поддерживают поставщики платформ, как мобильных (Apple в iOS7 и Samsung), так и облачных (Citrix). А значит, СТО компаний стоит попробовать сильнодействующее средство, обеспечивающее баланс нужд и интересов ИТ-специалистов и рядовых мобильных сотрудников.

Александра КРЫЛОВА

Вечная мерзлота сохраняет мамонтов и монополистов

Почти вся территория Якутии – зона сплошной многовековой мерзлоты. Здесь находятся 75% всех известных захоронений мамонтов в мире. А при взгляде на региональный телеком-рынок становится понятно, что в суровом климате отлично сохраняются не только доисторические гиганты.



Скажем, вполне современный оператор «Ростелеком» имеет завидную 80%-ную долю рынка даже в сегменте ШПД, недостижимую в большинстве других регионов.

По объему выручки от услуг связи Якутия занимает 28-е место среди субъектов РФ и третье среди регионов ДФО. В первом полугодии 2013 г. доходы якутских операторов росли быстрее, чем в среднем по России, увеличившись по сравнению с аналогичным показателем прошлого года на 7%, до 5,5 млрд руб.

Структура рынка связи Республики Саха



Более половины выручки регионального телеком-рынка принадлежит **сотовым операторам**. Тарифы на услуги мобильной связи в Якутии – одни из самых высоких в России. Это неудивительно, так как республика традиционно является регионом с высоким уровнем потребительских цен. Кроме того, на якутском сотовом рынке долгое время присутствовали только два оператора – МТС и «МегаФон», и здесь не ощущалось ценового давления конкуренции вплоть до 2008 г., когда в республике начал работу «ВымпелКом», развернув сеть третьего поколения. Лицензию на оказание услуг GSM в регионе оператор получил лишь в 2011 г., в коммерческую эксплуатацию сеть второго

поколения была запущена в апреле 2012 г.

Рынок **местной телефонии** Якутии также не может похвастаться большим количеством игроков. Всего в республике насчитывается порядка 153 тыс. квартирных абонентов, из них 97% обслуживает «Ростелеком».

Вечная мерзлота не позволяет расцвести конкуренции на региональном рынке **интернет-доступа** – немногие решаются осваивать суровый край. Рост количества альтернативных провайдеров долгое время сдерживался недостаточной инфраструктурой магистральных сетей и дороговизной оптового трафика «Ростелекома», фактического монополиста на рынке услуг по пропуску трафика. Соответственно, и розничные тарифы на интернет в республике высоки. Лишь в конце 2012 г. компания ТТК запустила в Якутии еще одну магистральную ВОЛС. В начале текущего года ТТК вышла на розничный рынок ШПД в регионе и сейчас активно набирает абонентов, рассчитывая в перспективе занять не менее 50% рынка. В Нерюнгри оператор приобрел местного игрока «Нерюнгри-телеком». Однако с появлением у «Ростелекома» конкурента ощутимого снижения цен для конечных пользователей не произошло, они все еще в разы отличаются от тарифов в центральной части России.

Другие заметные игроки местного рынка ШПД – «Экспресс сеть» и «ВымпелКом». Последний работает в Якутии на базе «Гелиос-ТВ», бывшей дочерней структуры приобретенной «ВымпелКомом» приморской «Новой телефонной компании». «Экспресс сеть» – провайдер,

предоставляющий услуги интернет-доступа в Якутске с 2003 г.

В общей сложности услугами высокоскоростного подключения к Сети в Республике Саха пользуются порядка 35% домохозяйств. В самом Якутске уровень проникновения ШПД достиг 46%.

Структура рынка ШПД Республики Саха по количеству абонентов



На республиканском рынке **платного телевидения** преобладают подключения к спутниковым операторам. Примечательно, что в Якутии IPTV популярнее кабельного телевидения. «Ростелеком» со своей абонентской базой IPTV – второй по величине абонентской базы игрок рынка платного ТВ, после спутникового оператора «Орион-Экспресс». «ВымпелКом», унаследовавший абонентов кабельной сети «Гелиос-ТВ», является третьим по количеству абонентов оператором платного ТВ в регионе.



Новые технологии, новые игроки и новые тренды постепенно проникают и в районы вечной мерзлоты, хотя и развиваются здесь несколько медленнее, чем в более благоприятных климатических условиях.

Дежурная по рубрике
Юлия ФЕДОРОВА,
аналитик iKS-Consulting

Блог, еще раз блог!

Реклама ■ Подписка ■ Все новости ■ Комментарии ■ Блоги ■ Глоссарий ■ RSS



Леонид РОГОЗИН Цель общественного контроля?

>>>> Появилась информация о том, что законопроект об основах общественного контроля в РФ будет подготовлен для внесения в Госдуму до 1 марта 2014 г.

Трудно предсказать судьбу этой инициативы. Много хороших проектов были засухены на корню. Однако уже сейчас очевидно, что в общественном контроле связи больше всего заинтересованы конечные потребители ее услуг – простые граждане. Именно они объективно заинтересованы в пресечении потоков административной ренты, ко-

торая оплачена из их кармана и открывает путь к реализации проектов коммерческой связи, проходящих через воздвигнутые усилиями нечистых на руку чиновников административные барьеры.

Поскольку важнейшими направлениями действия современного государства в области связи являются государственное регулирование и предоставление государственных услуг, постольку можно сформулировать главную цель общественного контроля на этом направлении:

Оказание содействия в пресечении коррупции и мошенничества в области связи в ходе осуществления государственного регулирования и предоставления государственных услуг.

[комментировать](#)



Михаил ЕМЕЛЬЯНИКОВ Слушаниями удовлетворен!

>>>> Прошли парламентские слушания «Законодательное обеспечение прав субъектов персональных данных при их автоматизированной обработке».

Редкий случай, когда участием в работе госоргана и, главное, результатом я удовлетворен полностью.

Совфед обещал не позднее 1 декабря этого года инициировать законопроект о внесении изменений в Федеральный закон 152-ФЗ «О персональных данных».

Положения нового законопроекта кратко излагаю с моими комментариями:

1. Ввести понятие субоператора и, главное, отказаться от требования обязательного согласия субъекта на поручение

обработки персональных данных субоператору, сохранив ответственность оператора перед субъектом. Здорово.

2. Наконец-то прямо написать, что конфиденциальность не требуется в отношении персональных данных, сделанных общедоступным субъектом, обезличенных, подлежащих опубликованию или обязательному раскрытию.

3. Прямо предусмотреть возможность получения согласия субъекта на обработку персональных данных дистанционно, путем использования электронных средств.

4. Наконец-то связать биометрию с возможностью автоматической идентификации.

5. Описать порядок обработки персональных данных иностранных граждан, собранных за пределами России, и регулировать эти вопросы законодательством государств, где такие данные собираются. Все правильно, но мало...

[комментировать](#)



Фил Циммерманн, наши криптографы и избыток безопасных мероприятий

>>>> В Москве пройдет еще одна конференция по информационной безопасности с простым названием «Информационная безопасность России 2013». Самое главное – приезд в Россию Филиппа Циммерманна, одного из гуру безопасности и фактически отца гражданской криптографии, основателя и разработчика легендарного Pretty Good Privacy (PGP).

...Тема утраты приватности меня волнует давно и глубоко, вот и разберемся, насколько такие опасения оправданы, растет ли опасность проникновения в частную жизнь со стороны государства, насколько серьезны кражи «электронной личности» и почему люди, довольно замкнутые в обычной жизни,

могут рассказать о себе в интернете все. Обсудим, к чему это ведет и можно ли гражданину, не готовому жить «с окнами без штор», самостоятельно противостоять атакам на приватность.

>>>> Несколько слов на тему, будоражающую моих друзей в Фейсбуке, об избытке мероприятий по информационной безопасности. Я лично в этом проблемы не вижу. Большой выбор – для специалиста всегда хорошо. Никто никого не заставляет посещать все. Возможность выбрать из многого интересное именно тебе – это гораздо лучше, чем информационный вакуум или ограниченный выбор. А законы конкуренции пока никто не отменял. В конечном счете должны остаться лучшие. Если верить старику Дарвину.

[комментировать](#)



Вы давно читали, чтобы наш блогер, да еще безопасник, был доволен слушаниями в Совете Федерации? Тогда загляните в блоги на IKS MEDIA.RU. И еще узнаете, почему другой блогер покинул Microsoft, а третий прогнозирует дефицит инженеров. Итак, блог, еще раз блог!



☐ Запомнить меня

■ Акции



Михаил ТАРАСОВ Почему я вас покинул...

>>>> Почему я вас покинул, Майкрософт? А потому, что вы меня, оказывается, не замечали, как и многих других своих клиентов, хотя и работали для меня и для других, сделав Windows Phone, а к нему – мультимедийную утилиту Zune. Пользуясь этим ПО, я неоднократно ловил себя на мысли, что неплохо бы сделать копию содержимого моего смартфона. Первый звонок прозвенел, когда телефон перестал заряжаться и соединяться с ПК.

Еще через три дня телефон (ему два года) выключился намертво. Из ремонта он вернулся абсолютно пустым: все эсэмэски и контакты, отсутствующие в hotmail, локальные записи были безвозвратно утеряны... Так вот оно значит что – могучая корпорация не дала мне шанса сохранить то, что было мне нужно.

P.S. А вам известны компании, которые с точки зрения своих клиентов действительно заботятся о них?

[комментировать](#)



Дмитрий МАРТЫНОВ Время сквозь пальцы

>>>> Многие жалуются на то, что спрос на учетно-управленческие ИТ очень спонтанный. Да, это так, точка возникновения спроса спонтанна, но общий поток стабилен.

ИТ дает бешеную эффективность. Эффективным оказывается даже проект, сделанный плохо. Те руководители компаний, кто почувствовал вкус управления с помощью ИТ-системы, начинают новый проект, как только старый развалился. Обычно это

меньше пяти лет. Продавцу же нужно оказаться в правильный момент в правильном месте. Как угадать? Для наглядности возьмем пример с аптекой.

Продавец может предложить вам две таблетки. Одна поможет, но вы об этом не знаете. Другая вам не поможет, но вы уверены, что это именно то, что вам нужно. При прочих равных вам продадут то, что вы хотите, а не то, что требуется. Если таблетки имеют разную маржу, то продавец постарается продать то, что ему выгоднее. Это характерно не только для ИТ. Маркетинг в ИТ такой же, как и везде. Продавцы продают клиентам их заблуждения, а не решения проблем. Например, ИТ-торговцы, продающие CRM, хорошо знают, что сколь-нибудь прилично сделанный CRM-проект потребует естественного роста до ERP. Но функциональность CRM этого не позволит. ИТ-торговец предупреждать об этом клиента не будет...

Вот когда руководители начинают считать деньги и выбирать технологии, исходя не из формального престижа, который на-гора продавец выдаст пачками, а из общения со специалистами, вникая в детали... Вот это самая правильная стадия. Руководителю лень вникать и хочется эту задачу повесить на кого-то, но уж больно все ушлые вокруг... опытные, жизнь их научила. Так что лезть в детали все равно приходится. Кстати, думая в эту сторону, я сейчас активно разрабатываю тему «честность в управлении»...

Вернусь к руководителям, которые начинают считать деньги, и обращаю внимание, что дело не в деньгах, совсем не в деньгах и очень не в деньгах. Время дороже. В попытке сэкономить 2–5 млн руб. можно выкинуть пять лет на неправильный проект. А ведь это пять лет плохого развития, пять лет мучений, ПЯТЬ ЛЕТ СОБСТВЕННОЙ ЖИЗНИ, в конце концов...

[комментировать](#)



Петр ДИДЕНКО Нет инженеров!

>>>> В следующие пять-семь лет будет плохо – новых молодых людей на рынке вообще не будет, и ИТ-компаниям, если высокий спрос на кадры продолжится ☺, будет несладко.

Сегодня мы с вами видим еще одну релевантную новость: оказывается, у нас в стране будет недостаток инженерных кадров, которые очень нужны в промышленности. То есть думать будет некому, лишь таджики с лопатами останутся. Будем теперь повышать ВВП только с их помощью. А все наши выпускаемые из вузов инженеры пойдут заниматься мелкой торговлей.

Будет интересно лет через десять (дай бог дожить!) почитать в учебниках истории, что же было дальше после этого момента! Никакой стабильности, понятно, не будет, а будет очередной кризис очень мутного толка. Хорошо бы, вероятно, придумать сейчас, как вести-то себя? ☺ Во что вложиться? ☺ Чем заниматься? В мутные времена, говорят, надо правильно сориентироваться. Думаете, пора?

[комментировать](#)



Евгений ЦАРЕВ Идем в облако и плачем

>>>> На конференции в Сочи рассказывал про будущее аутентификации. Общая идея в том, что сегодня есть возможность контролировать облачные сервисы в части аутентификации. Это было с интересом воспринято аудиторией, но это было еще не все. Через два-три года для поддержания контроля мы будем вынуждены вынести часть интерфейсов безопасности за пределы контролируемой зоны. То есть фактически сами создадим облачный сервис безопасности. Причем безопасников никто не спросит, нравится им это или нет, просто бизнес затребует расширенные возможности для доступа к ресурсам, и будут созданы так называемые страницы аутентификации.

[комментировать](#)



11–14 февраля 2014 г. в

Москве («Крокус-Экспо») пройдет XIX международный форум «**Технологии безопасности**» – крупнейший в России, СНГ и Восточной Европе конгресс по всему спектру вопросов обеспечения безопасности, ведущее техническое мероприятие в России для специалистов отрасли.

В рамках деловой программы форума запланированы конференции и семинары с участием конечных заказчиков. Экспозицию отличает четкое тематическое разделение для удобства навигации по выставке.

Контактный центр форума даст возможность общения с потенциальными клиентами в течение всего года, действует система заранее спланированных встреч.

Из участников мероприятия 38% составят государственные и корпоративные заказчики, 61% аудитории – руководители, принимающие решения о закупках.

Организатор – «Гротек».

Тел. +7 (495) 647-0442, доб. 2157
sadekova@groteck.ru
www.tbforum.ru

выставки, семинары, конференции

Дата и место проведения, организатор, сайт	Наименование мероприятия
19–21.11. Москва. Cisco: www.cisco-connect.ru	Ежегодная конференция по инфокоммуникационным технологиям Cisco Connect 2013
19.11. Москва. Connectica Lab: www.smartgrid-forum.com	2-й международный форум «Smart Grid & Metering. Перспективы и практика интеллектуальной энергетики»
20–21.11. Москва. «Гротек»: www.all-over-ip.ru	Международный форум All-over-IP
21–22.11. Санкт-Петербург. ADMIN: www.vasforum.ru	10th Mobile VAS & Apps Conference и Mobile Trends Forum
21–22.11. Москва. Exposystems: www.boss-forum.ru	Международный BOSS Forum-2013 Telecom & Enterprise
22.11. Москва. ИКС-МЕДИА: www.iksmedia.ru/conferences_medecina.html	Круглый стол «ИТ-ПОМОЩЬ МЕДИЦИНЕ: болевые точки и зоны роста информатизации здравоохранения»
27.11. Москва. Microsoft: http://events.techdays.ru/CloudOS/2013-11/	Cloud OS Summit
28.11. Москва. AHConferences: www.ahconferences.com	10-й форум «Информационные технологии в розничной торговле»

Присылайте анонсы ваших мероприятий на IKS MEDIA.RU

Еще больше на

4 декабря в Москве (отель Radisson Blu

Belorusskaya) пройдет четвертый международный форум «**Telecoms Loyalty & Customer Data**

Monetization: удержание клиентов и маркетинговая аналитика», в рамках которого планируется обсуждение комплекса вопросов, связанных с привлечением и удержанием абонентской базы телеком-операторами, с борьбой с оттоком клиентов, с практикой применения эффективных систем лояльности, актуальных инструментов маркетинговой аналитики, клиентского обслуживания.

Концепция потребительской лояльности является одним из важнейших инструментов в стратегическом планировании удержания абонентов, однако эффективность ее не всегда стабильна и экономически обоснована. Форум дает возможность поднять эти актуальные темы, согласовать интересы, обменяться опытом и обсудить варианты сотрудничества в рамках B2B-мероприятия.

Организатор – Connectica Lab.

Тел. +7 (495) 698-6385;
+7 (926) 427-5181
ob@connectica-lab.ru
www.telcoloyalty-forum.com

29 января 2014 г. в Москве («Крокус Сити

Холл») состоится торжественная церемония награждения лауреатов 5-й Национальной премии «**Большая Цифра**».

Премия в области многоканального цифрового телевидения «Большая Цифра» за четыре года существования стала знаковым событием для телевидения и телеком-отрасли в целом. Нововведение этого года – обновленный список номинаций в категориях «Компания-оператор», «Оборудование и технологии» и «Телеканалы». В категории «Компания-оператор» в 2014 г. выделена специальная номинация «Поддержка и обслуживание абонентов» для компаний-операторов с абонентской базой от 10 тыс. до 100 тыс. человек.

Победители премии будут определяться посредством голосования профессионального жюри, в состав которого входят ведущие эксперты в области кабельного и эфирного телевидения, журналисты, известные государственные и общественные деятели. Зрительское онлайн-голосование за лучший телеканал пройдет с 1 по 15 декабря на сайте премии «Большая Цифра».

Тел. +7 (495) 737-7479
anna@midexpo.ru
www.bigdigit.ru

ВЫСТАВКИ, СЕМИНАРЫ, КОНФЕРЕНЦИИ

Дата и место проведения, организатор, сайт Наименование мероприятия

28.11. Москва. Teradata: teradata-forum.ru	Teradata Форум 2013
28.11.2013. Москва. Академия информационных систем: antifraudrussia.ru	IV международная конференция «Борьба с мошенничеством в сфере высоких технологий. AntiFraud Russia – 2013»
29.11. Москва. Клуб топ-менеджеров 4CIO: www.4cio.ru	ИТ-Ассамблея 2013
04.12. Москва. Connectica Lab: telcoloyalty-forum.com/	4-й международный форум «Telecoms Loyalty & Customer Data Monetization: удержание клиентов и маркетинговая аналитика»
04–06.12. Казань. «Казанская ярмарка»: www.exposecurity.ru	Форум безопасности и связи
05.12. Санкт-Петербург. «ICF-Международные конференции»: www.intercomforum.ru	Форум Intercom Evolution 2013
12.12. Москва. AHConferences: www.ahconferences.com	IX форум Business Process Management
28–30.01.2014. Москва. «Мидэкспо», Ассоциация кабельного телевидения России (АКТР): www.cstb.ru	16-я международная выставка и форум CSTB'2014

www.iksmedia.ru

ИЩИТЕ все мероприятия на IKS MEDIA.RU
Планируйте свое время

5 декабря в Петербурге пройдет форум **Intercom Evolution** – ключевое мероприятие в отрасли телекоммуникаций на Северо-Западе России. В этом году форум получил новое название и новый формат, став существенно «ближе к народу».

Программа Intercom Evolution 2013 будет построена на необычных для форума блоках: от дискуссионного круглого стола о настоящем и будущем в области телекоммуникаций до новогодней вечеринки по случаю завершения – Intercom Award & NY Telecom Party.

В числе участников форума – топ-менеджеры и владельцы компаний – операторов связи, среди которых как крупнейшие федеральные, так и региональные телеком-операторы.

Одним из нововведений этого года станет проект независимого рейтинга отрасли Intercom Index. В рамках форума традиционно состоится вручение премии Intercom Award – первой профессиональной награды в области телекоммуникаций на Северо-Западе.

www.intercomforum.ru

29 ноября в Москве состоится **ИТ-Ассамблея**, на которой уже в шестой раз члены Клуба топ-менеджеров 4CIO подведут итоги года, проанализируют ситуацию в отрасли и дадут свои прогнозы на следующий год. Эксперты постараются дать прогноз развития рынка ИТ с целью собрать материалы и мнения, скомпоновать и отредактировать, а потом предоставить сбалансированный отчет всем членам сообщества.

В работе ассамблеи примут участие мэтры ИТ: руководители крупнейших вендоров, представленных на отечественном рынке; генеральные директора и владельцы известных российских ИТ-интеграторов; руководители ИТ-служб большого бизнеса – потребители ИТ-услуг.

Организатор – Клуб топ-менеджеров 4CIO.

www.4cio.ru

23 апреля 2014 г. в Москве (центр Digital October) состоится международная конференция **Data Center Design & Engineering**.

На конференции будут рассмотрены вопросы создания устойчивой инженерной инфраструктуры и ее эксплуатации, стоимости систем в зависимости от уровня доступности и надежности, потенциала применения новых технологических решений.

Основные темы конференции Data Center Design & Engineering:

- Системы электроснабжения
- Климатические системы
- Системы управления инженерной инфраструктурой (DCIM)
- СКС, фальшполы
- Системы физической безопасности

В работе конференции примут участие владельцы и руководители ЦОДов, ИТ-директора, директора по строительству, начальники служб эксплуатации, специалисты ИТ и инженерных служб.

Организатор – «ИКС-МЕДИА».

Тел. +7 (495) 229-4978
www.dcdeforum.ru



Ведущая темы
Евгения ВОЛЫНКИНА

ИТ-здоровье:

От представителей ИТ-отрасли часто можно слышать, что информационные технологии – это мотор развития новой экономики и катализатор роста любого бизнеса. Немалая часть медицины и системы здравоохранения давно стала бизнесом. Цель любого бизнеса – получение прибыли, и использование ИТ должно максимально этому способствовать. Однако в применении к медицине понятие «прибыль» не может выражаться в одних деньгах, речь ведь не только об оказанных «услугах», но и о здоровье человека. Поэтому драйвером информатизации медицины и здравоохранения в национальных масштабах во всех странах выступает государство.

Как и следовало ожидать, информатизация лечебных учреждений началась с тех элементов их деятельности, которые к самому процессу лечения отношения не имеют, – бухгалтерия, статистика, отчетность, – поскольку эти бизнес-процессы давно формализованы и автоматизированы в других отраслях экономики. Чтобы положительные результаты информатизации на своей работе и своем здоровье ощутили и врачи и пациенты, нужны сложные комплексные решения. Мы же пока находимся на этапе лоскутной информатизации – есть удачные системы, построенные местными энтузиастами, а общей архитектуры и идеологии нет.

Мировой опыт – дело хорошее, но даже в гораздо более развитых странах он не всегда положительный: например, программа модернизации здравоохранения Великобритании после 9(!) лет ее реализации была признана провалившейся. Далеко не все гладко и в США, раз тамошний минздрав решил наказывать долларом те медицинские учреждения, получающие финансирование из бюджета по национальной программе Medicare, которые к 2015 г. не внедрят системы электронных медицинских карт EHR и, что очень важно, не обеспечат их «осмысленное использование»!

Именно осмысленного использования информационных технологий и хотелось бы прописать нашей медицине.

Фокус

40

Все только начинается

Модель

45

Информатизация не должна нарушать порядок работы врача

Позиция

47

Главная проблема – нет правил игры



информатизация и высокие технологии в медицине

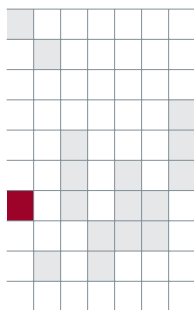
Сценарий
50
Россия –
классическая
страна для
телемедицины



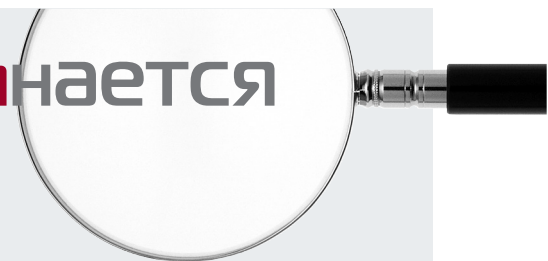
Дискуссионный
клуб «ИКС»
56
Разносторонний
треугольник:
пациент, врач
и государство

Ракурс
52
Врачебная тайна
эпохи интернета

Фокус



Все только начинается



В информатизацию здравоохранения в начале десятилетия влились большие по российским меркам государственные деньги. Но реальную отдачу от этих инвестиций мы увидим нескоро.

История с кибернетикой

Несмотря на то что медицина долго была одной из наименее компьютеризированных отраслей экономики России, информатизация здравоохранения имеет внушительную историю. Правда, в те времена термина «информатизация» еще не было, и в названиях лабораторий и отделов, создававшихся в 60-х годах прошлого века для решения проблем использования вычислительной техники в здравоохранении, часто фигурировали слова «кибернетика», «электроника» и «автоматизация». В 1967 г. у Министерства здравоохранения СССР появился Главный вычислительный центр, в 1975 г. в управлении статистики союзного министерства был создан отдел вычислительной техники, а при Ученом совете Минздрава РСФСР учрежден Совет по медицинской кибернетике и вычислительной технике, который занимался координацией разработок в области компьютеризации здравоохранения вплоть до 1994 г. В 1980 г. в нескольких продвинутых медицинских учреждениях уже были свои информационные системы: например, целых 11 штук автономных ИС работало в Институте сердечно-сосудистой хирургии им. А.Н. Бакулева. Среди них были не только традиционные ИС для отдела кадров и бухгалтерии, но и автоматизированный медицинский архив, несколько систем для диагностических отделений и исследовательских лабораторий. Кстати, медицинские айтишники со стажем говорят, что многие тогдашние разработки автоматизаторов этого института фигурируют в «Концепции создания единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)», утвержденной приказом Минздрава РФ №364 от 28 апреля 2011 г. Во всяком случае еще лет 30 на-

зад пришло понимание того, что в медицинских учреждениях нужно не только компьютеризировать бухгалтерию, но и создавать комплексные системы управления лечебно-диагностическим процессом – со сбором и анализом данных о пациентах и их лечении и с коллективным доступом к этим данным.

К нацпроекту и ЕГИСЗ

Работы по информатизации разных сторон работы учреждений здравоохранения в принципе никогда не прекращались, но самые продвинутые результаты достигнуты были, конечно же, в крупных клиниках силами энтузиастов. Медицина сама по себе чуть ли не самая регулируемая отрасль в любой стране мира, поэтому для массового внедрения современных ИТ во все области функционирования медицинских организаций необходимо было участие государства. В 2006 г. стартовал национальный проект «Здоровье», который предусматривал не только повышение зарплат медиков, но и поставки в лечебно-профилактические учреждения (ЛПУ) диагностического оборудования и компьютерной техники. Кроме того, в списке поручений Президента РФ по итогам Президиума Государственного совета РФ, состоявшегося 17 июля 2008 г., был пункт об утверждении комплекса мер по созданию государственной информационной системы персонализированного учета оказания медицинской помощи, подключению государственных и муниципальных медицинских учреждений к сети интернет и разработке необходимых нормативных правовых актов – со сроком исполнения 1 декабря 2008 г. Правда, почти три года спустя в уже упомянутой Концепции создания ЕГИСЗ констатировалось, что в целях автоматизации лечебно-диагностиче-

ского процесса в ЛПУ используется менее 20% имеющихся компьютеров, а в основном вычислительная техника служит для обеспечения административно-хозяйственной деятельности. Кроме того, там указывалось, что в российском государственном здравоохранении в среднем один компьютер приходится на 10,6 сотрудников, что электронные медицинские карты (ЭМК) или электронные истории болезни ведутся лишь в 7,7% ЛПУ и что средства телемедицины есть менее чем в 3% медучреждений.

В итоге на информатизацию здравоохранения и реализацию первого этапа создания ЕГИСЗ, предусматривающего обеспечение больниц и поликлиник доступом в интернет, внедрение медицинских информационных систем (МИС), оснащение ЛПУ компьютерным оборудованием и т.д., на период 2011–2012 г. было выделено почти 30 млрд руб. (точнее, 29,4 млрд, из них субсидии Федерального фонда обязательного медицинского страхования составили 20,2 млрд руб., а бюджеты регионов – 9,2 млрд руб.). Что же на этот почти миллиард долларов получили пациенты российских поликлиник и больниц? Вряд ли кто-то из них заметил грандиозные подвижки в лучшую сторону в работе давно знакомых медучреждений (прежде всего это касается сокращения очередей и повышения доступности врачей-специалистов). Руководство Минздрава объясняет, что эта сумма только кажется большой, ведь ее поделили на 83 российских региона, да и сделано было очень много: закуплено 279,7 тыс. единиц компьютерной техники, число комплектов оборудования для проведения медицинских видеоконсультаций превысило 4 тыс. штук (по сравнению с 887 единицами в 2009 г.), организованы защищенные каналы связи для ЛПУ, работы по созданию компонентов ЕГИСЗ проведены во всех регионах страны более чем в 9 тыс. государственных и муниципальных ЛПУ, к этой системе подключено около 600 тыс. автоматизированных рабочих мест медицинского персонала, запущены первые базовые сервисы ЕГИСЗ, в частности организована запись к врачу в электронном виде в 3920 учреждениях здравоохранения. В общем, по традиции деньги были потрачены главным образом на инфраструктуру, а что касается сервисов, то самый важный из них с точки зрения пользователей, а именно ЭМК, пока встречается далеко не в каждом ЛПУ. Причем Минздрав до сих пор так и не выпустил достаточного набора нормативных документов, регламентирующих требования к содержанию ЭМК, правила ее заполнения и использования. Юридически электронная и бумажная медицинские карты не уравнины в правах, поэтому даже при наличии системы ЭМК врачам приходится вести и бумажную карту.

В аналогичную коллизию попали и телемедицинские сервисы, крайне актуальные для страны с очень неравномерным распределением населения, треть жителей которой обитает в сельской местности и удаленных районах. Модельный закон «О телемедицинских услугах», определяющий порядок организации телемедицинских услуг и участников этого процесса, у нас есть. Есть и закон «Об обязательном медицинском

страховании», где прописана возможность финансирования телемедицинских систем из средств ОМС, но нет приказов Минздрава, регламентирующих функционирование этих систем и оплату работы специалистов по проведению видеоконсультаций.

Медицинская вертикаль

Разные версии сервисов, называемых ЭМК, есть сейчас почти во всех регионах, но содержащаяся в них информация варьируется от минималистичного набора «ФИО, дата рождения, пол, адрес» до бесконечности, размеры которой определяются фантазией разработчиков и емкостью СХД. Особой необходимости во введении единой для всей страны ЭМК нет – каждый регион в соответствии со своими особенностями может определить требуемую ему функциональность, но нужны единая структура, общие правила заполнения карты, общие форматы данных и стандарты обмена ими, а также поддержка интеграции с федеральной ЕГИСЗ. Такой практики сочетания разнообразия реализаций и единых общих правил придерживаются во всех странах, где внедряются ЭМК: например, в США медучреждения могут выбрать любую из более чем 600(!) сертифицированных систем.

Ну а у нас с созданием федеральных информационных медицинских сервисов пока связаны два довольно забавных конкурса Минздрава, состоявшихся в 2012 г. Их победителем стал «Ростелеком», который взялся за один рубль (1 руб.) разработать базовый функционал «Интегрированной электронной медицинской карты» (ИЭМК), а за другой рубль – первую очередь «Федеральной электронной регистратуры» (ФЭР) при стартовых ценах соответственно 83 млн руб. и 46 млн руб. Но от базового функционала до полноценного решения, готового к внедрению в масштабах всей России, дистанция огромного размера, хотя, по утверждению Минздрава, в начале нынешнего года ИЭМК была внедрена в сотнях российских поликлиник. В 2013 г. эпопею с глобальными заказами Минздрава продолжил аукцион по выбору подрядчика, готового сдать в аренду федеральный ЦОД и каналы связи для обеспечения работы ЕГИСЗ (в том числе сервисов ИЭМК и ФЭР) сроком на полгода, т. е. до 1 января 2014 г. Аукцион состоялся, несмотря на возражения Минкомсвязи, сенатора Р. Гаттарова и жалобы в ФАС, ФСБ и ФСТЭК, выиграла его компания МТС, снизив цену контракта с 1,74 млрд руб. до 564,94 млн руб. Срок аренды скоро заканчивается, и возникает большой вопрос – что будет дальше? Речь ведь о государственных информационных ресурсах и системах, обрабатывающих в том числе и персональные данные граждан. Перенос в «государственное облако», продолжение сотрудничества с МТС или выбор другого арендодателя? Ответ мы скоро узнаем.

Онлайн и офлайн

Особенно у нас гордятся запуском услуги записи к врачу через интернет: по данным Минздрава, по состоянию на середину 2013 г. этим сервисом в медучреждениях страны, работающих с ЕГИСЗ, воспользовались

более 10 млн пациентов, т. е. в среднем получается 7% населения. Но, например, в Пензенской области 8,9% граждан записываются к врачу через интернет, а в Пермском крае на местном портале записи к врачам зарегистрировались уже 20% жителей. А вот в Москве доля записи к врачу через интернет составляет всего 6%. Правда, во многих подмосковных городах, даже довольно крупных, такой записи вовсе нет. Можно, конечно, спорить о полезности этой опции в нынешней ее реализации, поскольку очереди к кабинетам врачей меньше не стали, но факт остается фактом. Кстати, несмотря на победные реляции о популярности интернет-записи, Минздрав пока так и не выпустил официальный регламент работы этого сервиса.

Раздельный старт

Система ЕГИСЗ хоть и называется «единой», но небольшую ее часть составляют региональные сегменты, а стартовые позиции российских регионов в деле информатизации здравоохранения к моменту утверждения концепции ЕГИСЗ были очень и очень разными. Где-то инфраструктура для широкополосного подключения лечебных учреждений к интернету уже была построена, где-то количество внедрений многофункциональных МИС позволяло говорить даже о массовости, а где-то не было почти ничего. К чести Минздрава, полного единообразия решено было не вводить, поэтому в каждом регионе программы информатизации имеют свои особенности и свои проблемы. Например, на недавней XIV ежегодной конференции «Информационные технологии в медицине – 2013» представители Краснодарского края и С.-Петербурга рассказывали

о довольно высоком начальном уровне оснащенности каналами связи, компьютерным оборудованием и ПО, но у этого есть и обратная сторона – необходимость поддерживать унаследованные ИС. В частности, в Петербурге многие ЛПУ начали информатизировать свою деятельность еще 10–12 лет назад, а созданная в последние годы единая городская мультисервисная сеть обеспечила широкополосный защищенный доступ всем госучреждениям, в том числе и медицинским. В итоге сейчас в городе работают 6 решений для автоматизации амбулаторных учреждений, 5 решений для информатизации стационаров, 3 вида ИС для лабораторий, 3 вида PACS-систем, 4 решения для колл-центров и т.п., из-за чего возникли проблемы не только с поддержкой этих систем, но и с интеграцией их с региональными и федеральными сервисами. А вот в Саратовской области «лоскуты» информатизации были в очень редких ЛПУ, регион строил свой фрагмент ЕГИСЗ почти с нуля и, похоже, нисколько об этом не жалеет – удалось без особых трудностей создать единое информационное пространство для всех 112 медучреждений области.

Есть контакт?

Практически все региональные участники процесса информатизации здравоохранения говорят о трудностях интеграции с федеральными сервисами, что обусловлено их частыми изменениями и отсутствием своевременной информации от Минздрава об этих изменениях. Тем не менее следует всячески приветствовать попытки министерства наладить взаимодействие по вопросам информатизации с медицинским сообществом и ИТ-специалистами, работающими в здравоохранении.

Наладить сотрудничество всех заинтересованных сторон



Роман САФРОНОВ,
заместитель директора
департамента
информационных технологий
и связи, Министерство
здравоохранения РФ

Даже при том, что информатизация медицинских учреждений считается второстепенной задачей, выполняемой в рамках общей программы модернизации здравоохранения, а многие руководители региональных органов здравоохранения по своему образованию являются специалистами-медиками, далекими от проблем ИТ, результаты, достигнутые в деле информатизации здравоохранения в большинстве регионов, достойны как минимум уважения, а иногда и восхищения. Конечно, в некоторых регионах нам пытались показывать потемкинские ИТ-деревни, но все-таки в большинстве случаев мы видели у местных специалистов огромный энтузиазм и инициативу, которые принесли очень достойные результаты.

Но эта работа шла бы еще более эффективно, если бы свои усилия объединили все участники проектов информатизации и пользователи медицинских ИТ-решений, а именно региональные министерства здравоохранения, медицинские информационно-аналитические центры, главные врачи ЛПУ и, конечно, системные интеграторы. Кое-где участники, на мой взгляд, увлеклись разделом сфер влияния, тогда как места для творчества и самореализации в проектах информатизации здравоохранения

вполне достаточно для всех. Мы все в одной лодке, и в наших общих интересах направить энергию на достижение максимального результата.

В последнее время Минздрав инициировал публичные обсуждения в интернете и в прессе различных документов и проектов, которые планируется реализовать в рамках программы информатизации. Эти обсуждения показали, что мы недооценивали широту аудитории, заинтересованной в информатизации здравоохранения. Это не только разработчики МИС, ИТ-специалисты медицинских организаций, органы управления здравоохранением, но и всё медицинское сообщество, а также организации пациентов. Все они имеют разные позиции и разное видение вопросов информатизации – и все хотят и должны быть выгодоприобретателями этой программы. Это означает, что для успешного развития информатизации мы должны наладить сотрудничество всех заинтересованных сторон.

ранении. В октябре 2012 г. Минздрав ввел должность главного внештатного специалиста по внедрению современных ИС в здравоохранении, на которую была назначена заведующая кафедрой медицинской кибернетики и информатики Российского государственного медицинского университета имени Н.И. Пирогова Татьяна Зарубина. Затем для организации неформальной обратной связи от регионов при главном внештатном специалисте была создана профильная комиссия, в которую вошли представители всех 83 субъектов РФ. В начале 2013 г. Минздравом «в целях реализации единой методической и технической политики при создании и развитии ЕГИСЗ» был сформирован Экспертный совет по вопросам использования ИКТ в системе здравоохранения, в рамках которого создано шесть рабочих групп по разным проблемам информатизации.

В положении об экспертном совете указывается, что он должен готовить рекомендации по использованию и развитию ИКТ в сфере здравоохранения и обеспечивать регулярное взаимодействие Минздрава с представителями экспертного ИТ-сообщества. Однако отзывы членов совета о результативности его работы, мягко говоря, не очень оптимистичные. Взгляды руководства Минздрава и членов экспертного совета на то, чем должен заниматься совет, как оказалось, не совпадают. Поэтому Т. Зарубина в своем выступлении на уже упомянутой конференции «Информационные технологии в медицине – 2013», признав само наличие экспертного совета совместным достижением министерства и медицинского ИТ-сообщества, заявила о необходимости сделать работу совета более регламентированной. Она также подчеркнула, что ситуация вполне исправима при наличии доброй воли сторон к взаимному движению навстречу. Значит, есть надежда, что экспертный совет все-таки сможет внести достойный вклад в дело информатизации здравоохранения.

Вообще открытость Минздрава, даже чисто внешняя, за последнее время заметно выросла. Недавно профессиональному сообществу было предложено обсудить внесение изменений и доработку концепции создания ЕГИСЗ, текст которой был выложен в интернет. Кроме того, для широкой публики в интернете было запущено голосование по поводу функционального наполнения нового электронного сервиса «Личный кабинет пациента», который, как предполагается, предоставит пациентам доступ к их ЭМК, позволит записаться к врачу через интернет, контролировать прием лекарств, записывать какие-то свои медицинские данные. Правда, по мнению некоторых экспертов, «личный кабинет» – не такой уж необходимый для пациентов сервис, пока не решены гораздо более важные для работы ЕГИСЗ проблемы со стандартами обмена данными, с организацией доступа к данным региональных и федеральных МИС, с едиными классификаторами и справочниками.

Больше сервисов, хороших и разных

Но, конечно, нашему здравоохранению, и в первую очередь пациентам, нужны самые разные медицинские сервисы, которые может предложить ИКТ-отрасль,

даже если сейчас они представляются дорогими излишествами. Какие из них станут действительно массовыми, пока сказать сложно – их выберут пациенты и рынок. Примечательная особенность этих сервисов – для их внедрения и дальнейшего функционирования, как правило, необходимы согласованные действия многих участников: разработчиков, пациентов, медицинских сотрудников, телеком-операторов, провайдеров облачных сервисов. В качестве примера приведем проект «Монитор здоровья», разработанный НИУ ВШЭ и ГК «АйТи». Это облачный сервис, предоставляющий услуги удаленного (с помощью мобильных устройств) мониторинга жизненных показателей человека, с прогнозом риска их ухудшения и оперативным реагированием в экстренных ситуациях. «Монитор здоровья» обеспечивает съем и анализ информации с медицинских устройств, защищенную ее передачу в единое хранилище данных, а также взаимодействие с врачами и существующими МИС. Если необходима консультация, на портале сервиса врачи разных специальностей могут совместно использовать собранные данные. При этом портал предусматривает возможность связи с пациентами и между врачами, в том числе по видео посредством Microsoft Lync и Skype. Разработчики считают, что «Монитор здоровья» способен повысить доступность медицинской помощи и снизить затраты на нее.

Несколько медицинских сервисов есть у сотового оператора МТС. В сентябре компания объявила о новом проекте – до конца 2013 г. планируется обеспечить более 2000 пенсионеров и инвалидов Москвы смартфонами с предустановленными sim-картами МТС, чтобы они могли получать круглосуточную социально-медицинскую помощь в центре «Системы Забота» (проект реализуется по заказу Департамента социальной защиты города Москвы в сотрудничестве с создателем этой системы компанией «Леге»). МТС обеспечивает доступ к диспетчерскому центру системы, с помощью которого можно вызвать скорую помощь и специалистов экстренных служб, оповестить родственников, проконсультироваться о приеме назначенных лекарств, получить информацию о работе лечебных учреждений, решить проблемы с коммунальными и социальными службами, организовать уход и помощь по дому, получить психологическую поддержку. Кроме того, в Воронежской и Свердловской областях, Краснодарском крае, Республике Коми, Удмуртии и Башкирии МТС помогает оборудовать мобильные кардиографы телематическими sim-картами, чтобы передавать диагностические данные из машин скорой помощи в стационар по каналам мобильной связи. По сведениям министерства здравоохранения республики Коми, в результате внедрения этого решения смертность от болезней системы кровообращения снизилась на 25%. В нескольких регионах России, в частности в Омске, Горно-Алтайске, Архангельске, Воронеже, Новосибирске, Сочи и Тамбове, решения МТС используются для мониторинга и координации работы машин скорой помощи, сокращая время прибытия врачей. В Тюмени ряд поликлиник использует услугу

МТС «Мобильные сотрудники» для того, чтобы отслеживать передвижение участковых врачей и наиболее эффективно направлять их по адресам.

С 2012 г. по всей территории России работает служба медицинской сигнализации «Кнопка жизни», которая позволяет экстренно реагировать на обращение абонента, нуждающегося в помощи. Прежде всего это касается пожилых людей и инвалидов. В решении используются мобильный телефон с кнопкой SOS, GPS-трекер или браслет с датчиком падения, оснащенные sim-картой МТС. Сигналы с этих устройств поступают в круглосуточный центр помощи, оператор которого в зависимости от ситуации может вызвать скорую помощь, МЧС или другие службы, связаться с родственниками пострадавшего и т.п. Причем в центре помощи хранится вся необходимая медицинская информация

пациента, которую оператор сообщит врачам при вызове. Поддерживается и возможность определения местоположения телефона по вышкам сотовой связи.



В общем, силами ИТ-отрасли, телеком-операторов и самих медиков в информатизацию российского здравоохранения заложен довольно основательный фундамент. Не везде еще он заметен снаружи рядовым пациентам, но на нем уже строятся не только массовые, но и нишевые медицинские сервисы, оценить удобство которых нам предстоит в ближайшие годы. И все же хотелось бы пожелать всем не иметь дел ни с какой, даже трижды информатизированной, системой здравоохранения. ИКС

Тектонические сдвиги будут заметны не сразу



Олег СИМАКОВ,
директор по ИТ,
Медицинский
информационно-
аналитический
центр РАМН

В деле внедрения ИТ в российское здравоохранение в последние годы произошли серьезные изменения. Но пока завершен только почти невидимый широкой публике «нулевой цикл» строительства будущего здания.

С 1991 г. и до 2008-го внедрение ИТ-средств и систем в медицинских организациях происходило лишь по инициативе отдельных их руководителей, понимавших, что для эффективного управления учреждением необходим электронный документо-

оборот в лечебно-диагностическом процессе. При этом основы персонифицированного учета оказанной медицинской помощи внедрялись системно с середины 90-х годов прошлого века силами федерального и территориальных фондов обязательного медицинского страхования (ОМС), так как эти сугубо финансовые учреждения просто не могли работать без автоматизированного учета предоставленных пациентам услуг. Поэтому территориальные фонды устанавливали в медицинских организациях рабочие места и собирали реестры счетов по оказанным услугам. Однако все это имело мало отношения к лечебно-диагностическому процессу, никак не влияло на повышение его эффективности со стороны медицинского персонала и не было заметно пациентам.

В 2008 г. начался процесс перехода к информатизации отрасли на основе поручений Президента РФ, данных по итогам заседания Президиума Государственного совета РФ 17 июля 2008 г. В результате было выпущено большое количество соответствующих документов и реализовано несколько первоочередных прикладных информационных систем непосредственно в интересах тогдашнего Минздравсоцразвития России, а в 2010–2011 гг. – раз-

работана Концепция создания единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ), утвержденная приказом министерства от 28 апреля 2011 г. №364 (первая редакция документа появилась на его сайте в январе 2010 г.). Принятие Концепции дало регионам возможность приступить к детальному планированию шагов по внедрению технических средств и информационных систем. Защита региональных программ информатизации в Минздравсоцразвития России и их согласование с Минкомсвязью и Федеральным фондом ОМС начались в октябре 2011 г. и продолжались почти год, до осени 2012 г. К середине 2013 г. в основном (по оценке экспертов, на 85–90%) были выполнены планы первого этапа оснащения медицинских организаций техническими средствами и частично проведено внедрение информационных систем, запланированных в рамках региональных программ.

Необходимо учитывать, что выделенные в рамках программы развития здравоохранения средства на информатизацию, даже с учетом регионального софинансирования, составляют не более 30–33% от суммы, необходимой на создание первой очереди ЕГИСЗ. В целом «лед тронулся», но если учитывать качество реализации первых проектов и реальные итоги их запуска, то можно говорить о том, что пройдено только 20–25% длинного пути полномасштабного создания этой социально значимой глобальной системы.

Главная проблема восприятия результатов заключается в следующем: эксперты и пользователи (к ним можно отнести пациентов, медицинский персонал и управленцев) пришли к пониманию, что система только на конечном этапе построения сможет удов-

летворить всех участников процесса. Ведь функции, нацеленные на повышение эффективности лечебно-диагностического процесса и управления медицинскими организациями, реализуются разными элементами информационной системы с использованием разных подходов, хотя в основе всего функционала и лежит электронная медицинская карта.

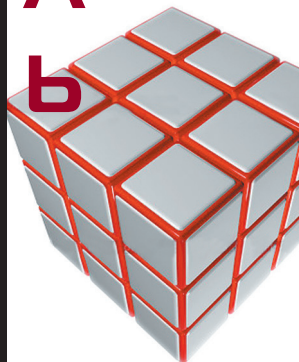
Автоматизированное формирование медицинской документации (и ее хранение в электронном виде), с однократным вводом информации, должно снизить непроизводительную нагрузку на медицинский персонал, связанную с оформлением медицинской документации и отчетности, и одновременно существенно повысить качество отчетности, поскольку она будет создаваться на основе первичных документов при минимальных ошибках и искажениях. Но сегодня электронный медицинский документооборот не имеет равных с бумажным юридическим правам, а формализация единой нормативно-справочной информации на федеральном уровне не реализована в полном объеме. Это два основных фактора, которые создают существенные препятствия промышленной эксплуатации информационных систем; к тому же, в соответствии с региональными программами, на текущем первом этапе такие системы внедрены только в небольшой части учреждений, поэтому эффекта от них не ощущают ни медицинский персонал, ни пациенты.

Однако ряд сервисов внедрен на федеральном уровне и соответственно получил широкое распростране-

ние в первичном звене. Уже сегодня виден эффект от довольно часто критикуемой «записи к врачу» через интернет. К сожалению, в проекте мало внимания уделяется разъяснению его деталей широкой общественности, в том числе медицинской. Например, эта самая «запись к врачу» – всего лишь первый шаг к решению глобальной задачи управления ресурсами сети медицинских организаций, что в конечном счете должно привести к прозрачности планирования и использования этих ресурсов – и соответственно к тому, чтобы на практике довести объем государственных гарантий до пациентов, исключить создание искусственных очередей и неэффективное использование оборудования и коечного фонда, а также различные формы вымогательства по отношению к пациентам. Поэтому могу констатировать: сделано много, но поскольку это только первый шаг, а хочется «всего и сразу», то много и критики. Но разве можно «оценить слона по его хоботу»?!

Сейчас главное – не останавливаться, а продолжить работу по внедрению системы в полном объеме. Это значит запланировать следующие шаги на ближайшие три года и понимать, что в лучшем случае мы пройдем только полпути, а всю систему при сохранении нынешнего уровня финансирования и эффективности работ удастся создать не ранее чем к 2022 г. Если мы хотим ускорить этот процесс, то нужно увеличивать финансирование и улучшать управление проектом, прежде всего на региональном уровне. ИКС

М
О
Д
Е
Л
Ь



Информатизация не должна нарушать порядок работы врача



На оснащение медучреждений компьютерным оборудованием и ПО потрачено немало средств. Что нужно для того, чтобы «железо» превратилось в востребованные сервисы для врача и пациента? Об этом – Георгий ЛЕБЕДЕВ, заместитель директора по ИТ ЦНИИ организации и информатизации здравоохранения.



↑
Георгий ЛЕБЕДЕВ

– Можно ли уже говорить о существенных изменениях в уровне информатизации российского здравоохранения?

– О существенных изменениях говорить можно будет немного позднее, а пока хорошо уже то, что на федеральном уровне было принято решение о необхо-

димости информатизации здравоохранения, и более того – выделены финансовые средства, которые позволяют как минимум сделать первый шаг в построении единой информационной системы в сфере здравоохранения. В рамках программы модернизации реализовано инфраструктурное решение – все меди-

цинские учреждения страны подключены к интернету, закуплены средства вычислительной техники и ПО. Активно идет внедрение компонентов единой информационной системы, которое продвигается довольно сложно, что в принципе и ожидалось, поскольку ни одна внедряемая ИТ-система не начинает нормально работать сразу после установки. Для системы такого масштаба этого придется подождать год или даже два.

– Ну а пока широкая публика может опробовать только пресловутую запись к врачу через интернет?

– По большому счету, чтобы нормально реализовать запись на прием к врачу через интернет, нужно сначала наладить учет рабочего времени врачей в медицинских учреждениях, т.е. в каждом из них нужно выделить специального человека для ведения расписания приема, разработать административный регламент, что может себе позволить далеко не всякое медучреждение. Кроме того, получилось так, что этот сервис уже внедрен, а официально утвержденного регламента его работы нет и, соответственно, нет организации, которая за него отвечает, нет ни федеральной службы его сопровождения, ни ответственных за этот сервис в каждом из субъектов РФ.

– Каково сейчас состояние нормативно-правовой базы для медицинских информационных систем?

– Проблем с ней немало. Единственное направление, в котором дела обстоят хорошо, это программа стандартизации: в сфере информатизации здравоохранения уже действует около 40 национальных стандартов, и в этом году планируется принятие первых стандартов группы HL7, определяющих правила обмена, управления и интеграции электронных медицинских данных. С остальными документами ситуация не простая. Ожидается целый ряд нормативных документов, в частности нормативный документ о введении в действие паспорта медицинского учреждения, регламент работы единой федеральной электронной регистратуры, порядок применения единых классификаторов и справочников в информационной системе здравоохранения. В этом может серьезно помочь создание федеральной целевой программы «Электронное здравоохранение», которая будет включать в себя и законодательное, и нормативное обе-

спечение. Очень полезной будет методика расчета эффективности применения информационных систем в сфере здравоохранения. Пока же вместо многих необходимых документов есть только временные инструкции и регламенты, которые носят необязательный характер.

– Вы не упомянули среди необходимых нормативных документов единый стандарт для ЭМК. Насколько он необходим?

– В международной практике достаточно стандартов, определяющих требования к ЭМК и ИЭМК, мы внедряем их в виде ГОСТов. А вот Положения об электронной медицинской карте и интегрированной ЭМК, ссылающегося и на эти стандарты и на правила учета медицинской помощи в РФ, пока нет, в организациях здравоохранения можно увидеть разные версии электронных карт. Думаю, что в этом нет ничего страшного. В принципе все эти ЭМК очень похожи, потому что вышли они из тех информационных систем, которые уже давно внедрялись и эксплуатировались в крупных лечебных учреждениях. Объем вводимых в них данных в принципе одинаков, а отличия есть только в системах ввода информации. Полагаю, что подвести все эти системы под единые требования, когда они будут сформулированы, проблемы не составит. Просто по большому счету создавать ЭМК должны не айтишники, а врачи вместе с ИТ-специалистами, потому что внедрение электронных средств не должно нарушать порядок оказания медицинской помощи.

– Ваши прогнозы: чего вы ждете от информатизации здравоохранения в ближайшие годы?

– Очень надеюсь, что в скором времени появятся и начнут в полном объеме работать те информационные ресурсы, которые составляют основу единой государственной информационной системы, что информатизация начнет реально повышать качество оказания медицинской помощи, что наконец-то будет построена система управления здравоохранением, в которой для поддержки решений, принимаемых должностными лицами здравоохранения, будет использоваться ЕГИСЗ. Нужно не забывать, что все информационные системы – это вспомогательные инструменты для здравоохранения, и задача информатизации состоит в том, чтобы обеспечить всем необходимым работу людей, оказывающих медицинскую помощь. **ИКС**

От манифеста – к результату



Борис ПОДДУБНЫЙ,
директор по развитию
бизнеса, IBM в России
и странах СНГ

Многие изданные Минздравом и правительством РФ документы, касающиеся планов модернизации и информатизации здравоохранения, по уровню содержания носят характер манифеста.

В них можно прочитать, что нужно снизить смертность, повысить продолжительность жизни и улучшить различные другие статистические показатели, принятые в нашей системе здравоохранения. Но нигде не определено, каким образом все это должно быть сделано, какие практические шаги нужно пред-

принять, чтобы получить заявленный результат, т.е. в документах нет конкретной программы в этих терминах.

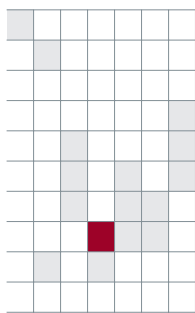
Например, можно поставить задачу в течение двух последующих лет повысить качество медицинской помощи за счет усиления ответственности врачей за результаты лечения. Реализовать это

можно следующим образом: все врачи, работающие с МИС, должны получить в удостоверяющих центрах электронные цифровые подписи, после чего они должны заверять ими все свои записи и назначения в ЭМК. Кроме того, пациенту нужно предоставить максимум информации о его собственном лечении: на специальном портале, подключенном к той же МИС, он сможет посмотреть, что именно прописал ему врач, какой рейтинг у этого врача и какой опыт, в каких медицинских учреждениях он раньше работал, какие врачебные ошибки совершал, как о нем отзываются другие пациенты, к какому еще врачу можно обратиться за консультацией по той же проблеме и т.п. Нужно предоставить пациенту возможность управления собственным здоровьем, не полагаясь на мнение единственного врача. На Западе порталы пациента – обычная практика, а во внедряемых сейчас в России медицинских информационных системах, даже в столь продвинутых, как московская ЕМИАС, таких возможностей нет, хотя реализовать их совсем несложно – аналогичные системы уже работают у нас в других отраслях. Такой практический шаг, взятый как пример, может существенно улучшить ситуацию в здравоохранении.

Россия – далеко не первая страна, которая занялась информатизацией медицины, и ей стоило бы использовать опыт предшественников. Но не надо это делать путем механического перевода и трансляции зарубежных стандартов в области информатизации медицины и здравоохранения. Эти стандарты создавались исходя из абсолютно других предпосылок и условий сложившейся системы здравоохранения за рубежом. Нужно понимать, что стандарты накопления и обработки ин-

формации должны быть тесно связаны с существующей системой показателей эффективности здравоохранения, которые нуждаются в реформировании вместе с принятием стандартов. Кроме того, в здравоохранении очень важны многолетнее накопление и систематизация информации, изменение подхода на уровне первичной информации нарушит преемственность сбора данных, и адекватный ее анализ будет невозможен.

Необходимо выделить те технологические аспекты информатизации, которые оказали бы системное влияние на принципы оказания медицинских услуг. Например, нам был бы полезен опыт эффективного использования высококвалифицированного труда узких специалистов-медиков. Скажем, опытный радиолог может заниматься только расшифровкой и описанием снимков, которые он получает по сети из нескольких больниц, более того, он может делать это, находясь у себя дома. Он не тратит время на укладывание пациента в томографе, на проведение самого исследования и даже на ввод текста в ЭМК, он наговаривает описание голосом и отправляет его, например, в мединститут, где студенты, обучающиеся по этой специальности, переводят звуковой файл в текст, сверяясь с полученным снимком. Так они учатся диагностике у настоящего профессионала, получают практический опыт и заодно выполняют определенный этап работ по обследованию пациента. Стоимость такой медицинской услуги будет, конечно, ниже, чем в случае, когда высококвалифицированный специалист сам выполняет все операции по получению снимка и занесению диагноза в ИС. Организация четкой работы этого комплексного сервиса требует немалых усилий, но именно такие медицинские системы надо создавать. ИКС



Главная проблема – нет правил игры

На информатизацию здравоохранения в 2011–2012 гг. государство выделило в общей сложности почти 30 млрд руб. О том, насколько эффективно используются эти немалые средства, – Михаил ЭЛЬЯНОВ, президент Ассоциации развития медицинских информационных технологий (АРМИТ).



Михаил ЭЛЬЯНОВ



– Какие изменения, по вашим впечатлениям, произошли в деле информатизации российского здравоохранения за последние год-два?

– В рамках программы модернизации в российское здравоохранение пришли огромные деньги, но, к сожалению, потрачены они в основном на оснащение ЛПУ компьютерами. Это, конечно, хо-

рошо, но таким способом была решена лишь самая примитивная часть задачи информатизации, и эффективность этих затрат оказалась очень мала. Продвинутое медицинские организации, доля которых составляет всего 5–7%, хорошо понимают, что делать с этим компьютерным оборудованием, и соответственно, используют его с макси-

Темпы есть, а системности нет



Федеральный центр всего за два года «взял на грудь» очень большой вес проблем, связанный с внедрением ИТ, таких темпов не было ни в одной западной стране. Есть примеры Голландии, Швеции, Великобритании, США, Канады, Испании, Израиля, Бразилии – и все они начинались со стратегии и принятия национальных проектов, рассчитанных не менее чем на 7–10 лет. Важно, что глубина проработки этих проектов на государственном уровне даже не касалась таких тривиальных тем, как покупка вычислительной техники. Российская же программа модернизации здравоохранения была нацелена на приобретение техники, подключение к интернету, организацию электронных услуг (запись на прием), создание ЭМК (заметьте, не исключая бумажной амбулаторной карты!) и ряда других электронных сервисов, которые сейчас вызывают прямое отторжение у врачей и граждан.

Предвидя такой поворот событий, компания ИБК, подписывая в феврале 2011 г. соглашение о намерениях по развитию ИТ в здравоохранении с Астраханской областью, предложила создать защищенную информационную инфраструктуру – и на ней в дальнейшем, масштабируя действующую систему, развить ИТ-функционал, реализующий учетную функцию, которая в обязательном порядке заменит бумажный медицинский документооборот. Такая инфраструктура создана, пилотные учетные сервисы запущены, а вот дальше – как всегда в России. Надо внедрять, развивать, сопровождать, а механизмы финансирования не созданы. Бюджеты области не позволяют запустить эти работы. Государственно-частное партнерство – это слабо осязаемый проект в медицине. Включение ИТ в тарифную политику отчислений от средств ФОМС и ДМС не регулируется федеральными нормативными документами, хотя и не запрещается.

Мы видим, что ни федеральные, ни региональные чиновники не собираются участвовать в процессах развития ИТ в здравоохранении. ИТ-компаниям, которые заинтересованы именно в продолжении, а не в начале новых работ в медицине, предлагается самим отправиться на поиски финансирования в ЛПУ.

Для обсуждения новых сервисов нужна активная позиция регионов. Сегодня мы в инициативном порядке разрабатываем технологии и сервисы, которые принципиально нацелены на граждан-пациентов, врачебное сообщество, создание одновременно частных и публичных сервисов, апробацию техник «удаленной медицины». И мы готовы внедрять их в «своем» регионе. Но все же хотелось бы, чтобы во всей программе информатизации здравоохранения была осмысленность и системность.

Григорий СИЗОНЕНКО, генеральный директор, ИБК

мальной отдачей. У подавляющего большинства это оборудование, грубо говоря, только пыль собирает. Пока я вижу главным образом попытки информатизации в интересах чиновников, которые стремятся отчитаться о достигнутых успехах.

– Как, на ваш взгляд, обстоят дела с решениями для автоматизации документооборота медицинских учреждений и информатизации работы врача?

– Проблем нет, пожалуй, только с бухгалтерскими программами, т.е. с самыми простыми, давно внедряемыми решениями, выполняющими хорошо формализованные задачи. Что же касается электронного документооборота, который касался бы всех сторон деятельности медицинской организации, то проблем с ним немало. Да, в Москве сейчас активно внедряются эти решения, в частности система ЕМИАС, но ситуация в регионах не дает большого повода для оптимизма. Массовых тиражируемых программ для электронного документооборота ЛПУ на рынке пока нет.

Ну а с автоматизацией работы врача просто полный провал. В поручениях президента РФ еще в 2010 г. говорилось о переходе к электронной медицинской карте, но до сих пор никакой типовой электронной карты не разработано и понимания того, что в нее должно входить, нет. Да, в ряде медицинских учреждений работают системы ЭМК, но установлены они были по инициативе главных врачей этих учреждений и фактически представляют собой продукты внутреннего пользования. На рынке есть несколько крупных игро-

ков с большим количеством внедрений, предлагающих системы ЭМК, но сравнивать эти решения за неимением стандарта очень сложно. Некоторые даже называют электронной картой программу, с помощью которой вводят ФИО, пол, адрес и код диагноза пациента по МКБ-10, но такие вещи делали еще 30 лет назад, причем на гораздо более высоком интеллектуальном уровне и за гораздо меньшие деньги.

– В чем причина такого «бухгалтерского» уклона?

– В уровне постановки задач государством. Последствия падения этого уровня я вижу хотя бы в каталоге «Медицинские информационные технологии», который ведет ассоциация АРМИТ. В последние годы четко прослеживается тенденция сокращения количества разработчиков медицинских ИТ-систем, причем опережающими темпами уходят с рынка разработчики наиболее наукоемких из них – систем поддержки принятия решений врачами, обработки данных, изображений и сигналов. Некоторые могут сказать, что это следствие конкуренции – уходят слабые. Но это не так. Когда государство своими целевыми программами и заказами создает многомиллиардный рынок, то на нем должны появляться новые игроки, а этого не происходит, потому что перед разработчиками ставятся по сути задачи для АСУ – посчитать кадры, услуги, финансовый оборот, – и все они были по большому счету решены 30–40 лет назад. А сейчас к этим системам по сути лишь добавляют графический интерфейс, чтобы они стали более доступными для рядового пользова-

теля. Такие вещи, безусловно, нужно делать, но к повышению качества медицинского обслуживания все это имеет очень косвенное отношение.

– В чем вы видите основные проблемы российской версии информатизации здравоохранения?

– Пожалуй, главная проблема неэффективности программы информатизации даже не в неграмотной постановке задач, а в отсутствии правил и стандартов. Мы как-то хотели вместе с разработчиками сформулировать список приоритетных направлений информати-

зации, чтобы попытаться убедить Минздрав выделить на них целевое финансирование, но многие разработчики прямо заявили, что им нужны только четкие правила игры, в том числе строго соблюдаемые всеми правила проведения конкурсов, с прозрачными критериями оценки участников и их продуктов. Конечно, информатизация здравоохранения идет и будет развиваться, никуда мы не денемся, это столбовой путь развития человечества. Просто мы проходим этот путь с очень большим опозданием и далеко не самым оптимальным образом. ИКС

Главная задача информатизации пока не решена

До сих пор абсолютно все успешные региональные проекты информатизации здравоохранения – это, безусловно, результат выполнения федеральных программ силами местных энтузиастов. В принципе все регионы могут решить любую задачу, которая будет поставлена Минздравом, но вопрос в другом: насколько всё это нужно, каковы цели и кто будет анализировать результат?

Пока же не решена главная задача информатизации – снижение объема бумажного документооборота при сборе отчетов и сокращение времени, которое врач должен тратить на заполнение новых первичных учетных документов (особенно при диспансеризации граждан). Уже создано множество сайтов и регистров федерального уровня, однако одновременно с этим в лечебные учреждения продолжают поступать запросы по отчетам, которые по идее должны автоматически формироваться из данных федеральных систем. Хорошо, если в регионе есть механизмы подготовки отчетов из систем федерального уровня, но чаще всего такого функционала нет.

Сейчас определенно можно сказать, что любая региональная программа информатизации должна начинаться со строительства каналов связи и сетей в медицинских организациях. Это главная составляющая дальнейшего развития информатизации. Автоматизированная система без обеспечения единого информационного пространства бесполезна. При выборе программных продуктов необходимо отталкиваться от модели реальных бизнес-процессов в здравоохранении, которые должны быть максимально адаптированы к автоматизированной обработке и полностью обеспечены нормативной базой. Однако эта адаптация ни в коем случае не должна ограничивать в правах участников процесса – ни пациента, ни медицинского работника.

Конечно, для внедрения современных ИС в здравоохранении нужны квалифицированные ИТ-специалисты, и эту проблему на региональном уровне решить практически невозможно. К сожалению,

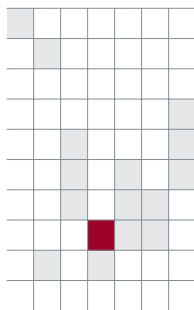
договорная система обслуживания МИС в большинстве случаев не решает все задачи, которые стоят перед конкретными медицинскими организациями. Немало у нас претензий и к системным интеграторам, предлагающим ИТ-решения для здравоохранения. Нередко бывает так, что описание ИТ-сервисов своевременно не актуализируется (т.е. не соответствует самому сервису), форматы обмена данными часто меняются, сервис дает не те данные, которые нужны, а те, которые он может дать. В результате в ответ на запрос «чем болел пациент?» мы получаем ответ «чем-то с номером таким-то». Ответ-то мы получили, но взять с него региональной системе по факту нечего. Есть утвержденные формы первичного учета с четкими правилами заполнения, есть стандарты обмена данными между медицинскими организациями и ФОМС, почему же нельзя по аналогии предусмотреть ответ интеграционного сервиса? Это существенно снизит нагрузку и на федеральные ресурсы: ведь сейчас, чтобы получить нужную информацию, региональная система посылает несколько запросов вместо одного.

Хотелось бы также, чтобы каждый новый информационный ресурс, внедряемый Минздравом, предусматривал и сервис обмена данными, и возможность загрузки-выгрузки данных, и конечно же, аналитическую среду для региона как поставщика этих данных. ИКС



Мария ДЕГТЕРЕВА,
директор,
Государственное
учреждение
здравоохранения
особого типа
Владимирской
области «Медицинский
информационно-
аналитический центр»

Сценарий



Россия – классическая страна для телемедицины



Страна, расположенная в девяти часовых поясах, 50 млн населения которой живет в сельской местности и удаленных районах, с очень неравномерным распределением больниц, поликлиник и других ЛПУ, без телемедицинских технологий не сможет обеспечить доступность и единые стандарты качества медицинской помощи всем своим гражданам.

Россия является классической страной для внедрения телемедицины. Ее востребованность очевидна, и необходимо детально обсуждать пути внедрения разномасштабных комплексных телемедицинских систем.

В государственной программе «Развитие здравоохранения Российской Федерации», разработанной Минздравом и принятой правительством в конце 2012 г., присутствует раздел «Телемедицина». По инициативе России на Межпарламентской ассамблее государств – участников СНГ принят модельный закон «О телемедицинских услугах» от 28.10.2010, а 19 ноября 2010 г. подписано «Соглашение о сотрудничестве государств – участников СНГ в создании совместимых национальных телемедицинских систем и дальнейшем их развитии и использовании». В этих документах определены термины в области телемедицины, участники процесса оказания телемедицинских услуг и порядок их организации. Есть поручения правительства, где говорится о необходимости внедрения телемедицинских технологий в масштабах не только отдельных регионов, но и всей страны. Однако на практике этого не происходит, и тому есть объективные причины.

Один из основных тормозов – проблема межведомственного взаимодействия. Ни одно отдельно взятое ведомство не в состоянии создать телемедицинскую систему в масштабах всей страны. Минздрав, который является постановщиком задач и главным пользователем системы, не обладает ни техническими, ни инфокоммуникационными возможностями для ее реализации. Для этого необходимо участие Минэкономразвития, Минфина, Минкомсвязи, Минпромторга, а значит, нужен орган на уровне правительства, который координировал бы работу этих ведомств по созданию Национальной телемедицинской системы России. Проблема усугубляется еще и тем, что на разных этапах обоснования проекта, проектирова-

ния, разработки, создания и эксплуатации телемедицинских систем различные ведомства должны играть ведущую роль.

До сих пор не решен вопрос организации финансирования телемедицинских услуг: пока не будет принято решение об оплате дистанционных консультаций из фонда ОМС, дело не сдвинется с мертвой точки. Разговоры идут уже лет двадцать, все всё понимают, но воз и ныне там, а без решения этой проблемы даже установленные телемедицинские комплексы используются крайне неэффективно, больше простаивают, чем работают.

Системы телемедицины, рассчитанные на самые разные применения и условия эксплуатации, давно разработаны. Есть компании, которые производят, поставляют и обеспечивают функционирование телемедицинских консультационно-диагностических центров для стационарных медучреждений всех уровней, в том числе для федеральных медицинских центров, областных, городских и районных больниц и фельдшерско-акушерских пунктов, а также мобильные комплексы для медицинского обслуживания населения там, где нет стационаров.

В 2010 г. президент США подписал программу создания телемедицинских систем для сельского населения, на которую было выделено \$450 млн, – американцы подсчитали, что реализация этой программы в течение 15 лет принесет экономике страны \$500 млрд. Рискну заявить, что программа, разработанная в России, эффективнее, системнее и комплекснее американской. Российские телемедицинские системы по своим характеристикам находятся на очень хорошем уровне. НАТО просит сейчас нас поделиться опытом в создании телемедицинских систем и начинает финансировать совместный с Россией проект, который теперь получил статус многолетнего и мультинационального. Российские мобильные телемедицинские комплексы уже успешно работают в Африке. Остались «совсем пустяки»: добиться, чтобы они лечили не только африканских детей, но и российских. ИКС



Михаил НАТЕНЗОН,
председатель совета директоров,
НПО «Национальное телемедицинское агентство»

Разрыв между возможностями и реальностью

У России обширная территория, поэтому для нашей страны очень актуальны проблемы консультирования и диагностирования сельского населения, особенно проживающего в удаленных и труднодоступных регионах. Для этого разработан целый ряд решений, но они по тем или иным причинам не получают широкого распространения. По стране ездит больше десятка мобильных телемедицинских диагностических комплексов, закупленных некоторыми регионами, но в масштабах России это капля в море. Таких комплексов в стране должно быть как минимум тысяча штук, причем они должны быть соединены в сеть хотя бы в масштабах региона, чтобы в проблемных случаях быстро запросить консультацию специалиста. «Автономные» же мобильные комплексы, без современных средств формирования и передачи баз данных, отбрасывают нас в прошлый век, когда по деревням ездили «пазики» с флюорографическими аппаратами.

Даже в райцентрах, не говоря уже о сельских поселениях, ситуация с медицинской помощью просто требует внедрения мобильных телемедицинских комплексов. Многие районные поликлиники «оптимизировали», и их пациентам приходится ездить в областные ЛПУ. Запись через интернет – дело, конечно, хорошее, но надо учитывать, что в регионах у пожилых людей домашнего доступа в интернет нет, компьютерами они не пользуются, так что единственный выход – отправляться с утра пораньше за десятки километров в областной центр, чтобы взять талончик в регистратуре, и на другой день повторять это путешествие, чтобы, просидев в очереди, наконец-то оказаться у врача. А если понадобится сделать какие-то анализы или исследования? А если врач отправит к другому специалисту, у которого тоже очередь и запись на несколько недель вперед?

В принципе хорошие решения для мобильной телемедицины в стране есть. Есть разработки, которыми интересуются даже за границей. Проблема – с их внедрением. И этот разрыв между возможностями и реальностью, к сожалению, пока не уменьшается.

Александр СМЕРНОВ, генеральный директор, Ассоциация организаций оборонно-промышленного комплекса – производителей медицинских изделий и оборудования



Здравоохранение – перспективный рынок для телекома

Мошны каналы передачи данных, дата-центры с облачными платформами, массовое распространение современных мобильных устройств – у телеком-операторов есть все условия для предоставления медицинских сервисов.

Американский оператор связи Verizon недавно получил разрешение от FDA (Управление по контролю качества пищевых продуктов и лекарственных препаратов США) на использование облачного телеком-решения Converged Health Management для предоставления медицинских сервисов, которые соединяют врачей с находящимися дома пациентами, позволяют удаленно считывать данные с приборов: тонометров, глюкометров, оксиметров. Потенциальный рынок очень широк: более 90 млн жителей США страдают хроническими заболеваниями, требующими постоянного наблюдения. Думаю, что в России таких пациентов тоже немало.

Активно занимаются медицинскими телеком-сервисами европейские операторы. Например, компания Swisscom предоставляет медицинские видеоконсультации прямо из аптек. В проекте участвует более 500 аптек в Цюрихе: если человека замучили насморк и кашель, а высокой температуры нет, то он может зайти в аптеку, получить по видеосвязи консультацию врача и сразу купить необходимые лекарства. Причем страховые компании оплачивают предоставление подобных ус-

луг, они заинтересованы в том, чтобы пациенты меньше обращались в клиники.

Привлекательный сервис для операторов связи, имеющих облачные платформы, – так называемая медицинская биржа, которая обеспечивает обмен информацией по разным медицинским случаям между врачами, специализированными клиниками, страховыми компаниями и пациентами с соблюдением всех мер защиты персональных данных. В развитых странах с большой территорией широкое распространение получает удаленная медицина. К примеру, австралийский оператор связи Telstra предоставляет медицинские сервисы с использованием передвижных мобильных комплексов автомобильного базирования разной специализации (есть, к примеру, комплексы для маммографических исследований, для диспансеризации жителей сельской местности). Французский оператор связи Orange активно работает с го-



Евгения РЯБИКОВА, директор по работе с операторами связи, Cisco Consulting Services

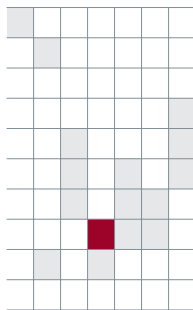
спиталиями и домами престарелых, обеспечивая им удаленные видеоконсультации врачей. Есть и специальные облачные медицинские сервисы, ориентированные на конечных пользователей. Например, клиенты оператора Telefonica получают из облака сервис отслеживания передвижения больного или его местоположения в доме; существуют специальные программы, напоминающие о необходимости принять лекарство, или реабилитационные комплексы упражнений, которые можно делать дома самостоятельно.

Многие из перечисленных услуг, несомненно, будут востребованы и в России. Уже есть сервисы, использующие современные телекоммуникационные технологии: можно, например, сделать МРТ в Москве, а расшифров-

ку снимка получить от врача, работающего в Воронеже. Однако операторы связи в цепочку предоставления этого сервиса пока не включены. Сейчас для хранения данных и их защиты компании используют собственные дата-центры, но операторы могли бы предоставлять эти услуги лабораториям как управляемый сервис.

Предоставление медицинских сервисов операторами связи – это новое интересное направление бизнеса. Конечно, оператору необходимо иметь соответствующую компетенцию и твердое желание перейти от традиционных услуг передачи голоса и данных к более сложным, но менее маргинальным индустриальным сервисам. Решение непростое, но рынок диктует этот переход, и операторам лучше заранее к нему подготовиться. ИКС

Р а к у р с



Врачебная тайна эпохи интернета



Проблемы с информационной безопасностью считаются одним из факторов, сдерживающих информатизацию здравоохранения. Это вполне понятно: никому не хочется, чтобы информация о состоянии его здоровья попала к посторонним. В конце концов, слова о врачебной тайне фигурируют в клятве Гиппократов, известной еще с III века до н.э. И эту тайну надо защищать, в том числе и с помощью современных технологий.

Мечты об инфобезопасности в здравоохранении

Михаил ЕМЕЛЬЯННИКОВ, управляющий партнер, консалтинговое агентство «Емельяников, Попова и партнеры»

Нормативной базы, регламентирующей порядок защиты и обеспечения безопасности сведений,

составляющих врачебную и медицинскую тайну, в России вообще не существует. Сам факт наличия в законодательстве этих двух видов тайн говорит о непроработанности проблемы. Это одно и то же или нет? Если нет, то чем эти сведения отличаются друг от друга? Стремление отнести абсолютно все сведения о состоянии здоровья к персональным данным и защищать их именно по требованиям, установленным для персональных данных, мне представляется не совсем правомерным. А отдельных документов, аналогичных, например, американскому HIPAA (Health Insurance Portability and Accountability Act), принятому еще в 1996 г., в России нет.

Минздрав в 2009 г. разработал «Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здра-

воохранения, социальной сферы, труда и занятости», однако они устарели и не соответствуют текущему состоянию нормативного регулирования. Сейчас ведется работа по их актуализации, но почему-то исключительно силами общественных-добровольцев. Для этого в Экспертном совете Минздрава создана рабочая группа по информационной безопасности. Но опять-таки, при этом предполагается, что вся информация о состоянии здоровья относится к персональным данным, хотя законодательство выделяет эти сведения в отдельную группу – персональные данные специальных категорий, обработка которых обставляется дополнительными условиями и требует принятия повышенных мер безопасности.

К примеру, на обработку таких сведений лицами, которые не являются медицинскими работниками и не обязаны хранить врачебную тайну, требуется согласие пациента в письменной форме. Но ни одна МИС не сможет



функционировать без администрирования, а администраторы (системные, баз данных, приложений и т.д.) медицинскими работниками не являются, хотя доступ к информации фактически имеют. Вот и ломают голову главврачи, что в этих условиях делать. Где-то от пациента перед приемом у врача требуют подписать согласие на обработку персональных данных, которое он резонно подписывать не хочет, а отказать ему в медицинском обслуживании нельзя. Где-то пишут о запрете доступа администраторов к информации в МИС и обеспечении этого запрета «организационными методами».

Для МИС надо обеспечить минимум третий уровень защищенности персональных данных, а это, в соответствии с приказом ФСТЭК, требует выполнения порядка 40 базовых мер безопасности на основании актуализированной частной модели угроз. О том, кто конкретно и на какие средства должен это делать в районной или городской больнице, частной стоматологической клинике или диспансере, наши законодатели и регуляторы скромно умалчивают. Учреждениям здравоохранения средства на информатизацию при общем немалом бюджете этой программы выделяются крайне скудно, и последние проблемы, которые в этих условиях будут решаться, – это проблемы безопасности.

В идеале МИС должны сразу разрабатываться с учетом требований российского законодательства и регулято-

ров к обеспечению информационной безопасности. Например, архитектура МИС, позволяющая обезличивать сведения о состоянии здоровья, могла бы существенно снизить затраты на защиту. Заменить в системе ФИО пациента каким-либо идентификатором, например, номером полиса обязательного медицинского страхования, технически совсем не сложно. Пришел пациент на прием, предъявил номер полиса – и вся информация о нем доступна врачу, однако использовать ее во вред пациенту нельзя, так как связь между номером полиса и конкретным субъектом устанавливается совсем в другой системе. В такие системы могли бы сразу встраиваться подсистемы, обеспечивающие реализацию базовых мер безопасности: антивирусной защиты, управления идентификацией и доступом, контроля целостности и т.д. При нормальном взаимодействии разработчиков МИС с российскими вендорами средств ИБ такие решения не сильно бы увеличили стоимость систем.

Упростить задачу могла бы локализация МИС и отсутствие у нее подключений к интернету, но взятый Минздравом курс на облачные технологии эту возможность закрывает. Облегчила бы жизнь медикам и разработка МИС с помощью методов защищенного программирования, что повысило бы защищенность таких систем от взлома с использованием недеklarированных возможностей. Но пока все это только мечты. ИКС

Защита от дилетантов

Алексей САБАНОВ, заместитель генерального директора, «Аладдин Р.Д.»

Положение дел с нормативно-правовой базой, касающейся сбора, обработки и передачи медицинских данных пациентов, обстоит у нас в стране крайне плохо. Только вдумайтесь: последние отраслевые положения нормативно-правовой базы, опубликованные на сайте Минздрава, датированы 2009 г.

С защитой медицинской информации пациентов все обстоит достаточно просто. Требования 152-ФЗ перекрывают требования статьи 23 Конституции РФ о защите личной тайны. Следовательно, для защиты медицинской информации необходимо всего-навсего выполнить требования 152-ФЗ, которые разъясняются во множестве подзаконных актов. Однако некоторые законы в сфере ИБ у нас принимаются в таком виде, что требуют многочисленных разъяснений, и не всегда толкования положений закона от уполномоченных лиц и организаций совпадают. С защитой личной тайны и персональных данных врачей все гораздо запутаннее. С одной стороны, информацию, отнесенную к этим видам тайн, надо защищать, с другой стороны, некоторые данные обязательны к раскрытию (публи-

кации). До сих пор многие коллизии здесь не разрешены.

Обеспечение конфиденциальности любых данных, в том числе персональных и медицинских, неизбежно влечет за собой их шифрование. Если говорить о российских условиях, то все программные реализации (алгоритмы) шифрования должны соответствовать ГОСТ 28147-89. Не секрет, что требования к разработчикам медицинских систем в плане встраивания шифросредств завышены. В этом одна из причин того, что разработчики МИС избегают такой дополнительной работы и перекладывают задачу защиты данных на встроенные в операционные системы или СУБД средства, которые, конечно же, не удовлетворяют российским требованиям. В итоге в подавляющем числе ЛПУ наши с вами данные в МИС и на бумаге на сегодняшний день, как правило, не защищены или защищены только от дилетантов. Что делать? – думаю, это предмет отдельного обсуждения. ИКС



Требований инфобезопасности слишком много

Андрей ПРОЗОРОВ, ведущий эксперт по информационной безопасности, InfoWatch

С точки зрения информационной безопасности есть несколько проблем, которые сдерживают развитие информатизации здравоохранения в РФ. Прежде всего это большое число требований, связанных с защитой пер-

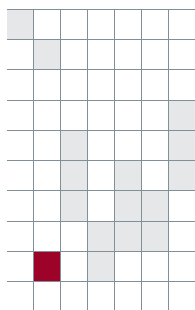
сональных данных (152-ФЗ, ПП1119, приказ ФСТЭК №21 и другие), которые необходимо учитывать и выполнять. С учетом того, что в ИС здравоохранения обрабатываются персональные данные о здоровье (спе-



циальная категория ПДн), количество и сложность требований, а значит, и стоимость их выполнения, возрастают. Ситуацию усугубляют многочисленные требования, связанные с использованием государственных и муниципальных ИС (приказ ФСТЭК №17), которые необходимо будет выполнять при подключении к ЕГИСЗ, что тоже не просто и довольно затратно.

Но основная сложность в том, что все эти требования периодически меняются. Так, в 2011 г. был существенно изменен 152-ФЗ, в конце 2012 г. вышло постановление Правительства №1119, в начале 2013 г. – приказ ФСТЭК России №21, а сейчас регуляторы готовят рекомендации по выполнению его требований. Подход к защите персональных данных за последние полгода серьезно изменился, и тем операторам, которые привели свои информационные системы в соответствие ранним требованиям, сейчас придется проделать дополнительную работу.

Большинство данных пациентов, обрабатываемых в МИС, подпадают под «специальную категорию ПДн» (сведения о состоянии здоровья, лабораторных исследованиях и пр.), а также в ряде случаев и под категорию «биометрические персональные данные», что повышает требования к системе защиты. Медицинские учреждения должны также обеспечивать безопасную трансграничную передачу персональных данных пациентов (например, при телемедицине). Помимо стандартных средств обработки данных (рабочие станции и серверы) в МИС может присутствовать специализированное медицинское оборудование, для которого не подходят стандартные программные и аппаратные средства защиты информации, и тогда должны применяться встроенные средства защиты и/или организационные меры. Кроме того, довольно часто в медицинских учреждениях встречается «самописное» и/или разработанное по договору ПО, при создании которого практически не учитывались требования ИБ. Проверить и внести необходимые изменения в исходный код и настройки таких систем обычно бывает не просто. ИКС



Требуются реалистичные комплексные решения

Уровень предлагаемых поставщиками решений для информатизации лечебных учреждений растет, расширяется и спектр предложений, заказчику есть из чего выбрать. Но у этой медали есть и другая сторона...

И с этой стороны мы видим устаревшие платформы, сложную интеграцию, завышенную стоимость поддержки и отрыв от реальности («страшно далеки они от народа...»). Разработчикам определенно не хватает общения с заказчиками. Иногда они явно забывают, что решение нужно не только создать, но и внедрить, а как раз на этапе внедрения и начинаются самые большие сложности любого проекта.

Очень остра проблема поддержки ИТ-решений: далеко не все поставщики готовы предложить SLA, который в полной мере отвечал бы медицинским процессам, ведь в медицине часто нужна очень быстрая реакция, а по отдельным сервисам – круглосуточная поддержка.

Справедливости ради нужно сказать, что интересные решения для информатизации медицины у отечественных разработчиков есть. Одно из внедренных у нас в клинике решений – комп-

лекс автоматизации операционных зон, который обеспечивает тотальный сбор и хранение информации со всего медицинского оборудования из операционных залов (а это более 40 параметров), предоставляет доступ к медицинским данным и автоматизирует рутинные процедуры.

ЭМК в нашей клинике используется уже более 15 лет и стала привычным инструментом врача. Она предоставляет быстрый доступ ко всем диагностическим данным, в том числе удаленный (у врача на выезде есть возможность посмотреть электронную карту пациента). В нашей ЭМК есть и личный кабинет пациента, где он может не только получить доступ ко всем своим медицинским данным, но и записаться на прием, оценить



Федор КИДАЛОВ,
директор службы ИТ,
клиника ОАО
«Медицина»

Требуется стандарт

До недавнего момента российские ЛПУ автоматизировались собственными силами и на свой страх и риск. Нередко каждое отделение ЛПУ занималось автоматизацией без привлечения специалистов других отделений и даже руководства. Итог – «лоскуты» автоматизации, разбросанные по предприятию, передача информации о пациенте из отделения в отделение «на бумажке», потеря времени.

Сейчас здравоохранение попало в поле зрения государственных чиновников, и вопросы автоматизации медицинских организаций вышли на передний план. Формируется понимание того, что необходима единая государственная информационная система (ЕГИС), которая взяла бы на себя роль связующего звена между ИС отдельных ЛПУ, региональными и областными центрами здравоохранения, страховыми компаниями, органами социального развития и помощи, правоохранительными органами и т.п.

Камнем преткновения для создания подобной ЕГИС по сей день остается отсутствие единого стандарта ЭМК. Попытки его создания на всероссийском уровне группы энтузиастов предпринимали неоднократно, но пока все закончилось лишь проектами документов ЭМК для медицинской организации и интегрированной ЭМК, разработанными с участием авторов ГОСТ Р 52636-2006 (Национальный стандарт РФ «Электронная история болезни») Б.В. Зингермана и Н.Е. Шкловского. Таким образом, сейчас организации здравоохранения поставлены в условия, когда существовать без автоматизации уже невозможно, а единых стандартов и принципов еще нет. Это неизбежно привело к росту рынка решений для автоматизации деятельности ЛПУ, в частности самого популярного их элемента – МИС.

Востребованность МИС настолько высока, что в России разработкой и внедрением таких систем занимается более 200 компаний. Каждая из них старалась вложить в свою систему все накопленные знания и опыт, а также учесть пожелания заказчиков. В итоге на рынке появилось огромное число систем, сформированных с учетом видения сотрудников того или иного ЛПУ. С одной стороны, такое разнообразие позволяет выбрать готовое решение, максимально подходящее к требованиям конкретного учреждения, с другой – все больше отдаляет нас от появления единого стандарта в формировании ЭМК. Различия в МИС, принципах их построения приводят к затруднениям даже при банальной смене места работы: врачу приходится тратить много времени на то, чтобы привыкнуть работать в другой системе.

Андрей ЛИТВИНОВИЧ, директор по ИТ, «АКАДО Телеком»



работу врача, оплатить услуги, получить телемедицинские консультации.

В нашем новом корпусе есть и ЦОД, и современная сеть передачи данных, и «умные палаты», и «умные операционные», где инженерным оборудованием управляет iPad, и отделение лучевой терапии с полностью интегрированными ИС. Это результат трех лет работы большой международной команды единомышленников. Понятно, что персонал клиники должен уметь работать со всеми этими системами. К обучению врачей мы подходим комплексно: есть вводный курс с ис-

пользованием системы электронного обучения и с тестированием полученных знаний и навыков, предусмотрены консультации ИТ-специалиста и взаимодействие с врачом-наставником на этапе самостоятельной работы, в общем, всегда есть кто-то, кто подскажет. С ИТ-специалистами вопрос более сложный. Увы, за неделю-другую такого специалиста не научить и не воспитать, поэтому мы начали работу с институтами, предлагаем студентам проходить практику в нашей клинике. В этом году у нас уже появились первые практиканты. **ИКС**

Требуется единая платформа

В медучреждениях должна быть единая МИС – в которую войдут и ЭМК, и система управления потоком пациентов, сервисы записи к врачам, система поддержки принятия решений для врачей, средства передачи медицинской информации пациента другим врачам клиники и в другие лечебные учреждения.

ИТ-решения для медицинских учреждений, предлагаемые сейчас на рынке, в большинстве своем находятся на довольно низком качественном уровне. Их разработчики – это часто небольшие коллективы, не способные построить решение на надежной про-

граммной платформе, не умеющие быстро реагировать на изменение потребностей бизнеса и не обладающие достаточной квалификацией (в том числе в управлении проектами). Как правило, это продукты с



Игорь СКОБЕЛЕВ,
ИТ-директор,
ГК «Медси»

закрытым исходным кодом, что, в свою очередь, обуславливает проблемы при внедрении и эксплуатации: срыв сроков, невозможность для заказчика сменить поставщика ПО и/или команду внедренцев. Похожим образом лет десять-двенадцать назад складывалась ситуация в других отраслях экономики, в частности в финансовом и нефтегазовом секторах, в ритейле.

Да, в медицине есть острый дефицит квалифицированных ИТ-специалистов, которые сейчас предпочитают идти в банки, где уровень зарплат выше. Да, пока мы видим в здравоохранении лишь локальные кусты информатизации (там, где все же есть достаточно сильные специалисты) при очень низком ее среднем уровне. И тем не менее качественные ИТ-решения на этом рынке уже есть. Среди них особо хотелось бы отметить московскую единую медицинскую информационно-аналитическую систему (ЕМИАС). Подход к ее созданию выбран абсолютно правильный и наиболее экономически эффективный: это модульная система, в которой использованы и уже готовые решения, и собственные разработки. Довольно сильный проект был реализован компанией «Медлайнсофт» в Ярославской области, где создана единая интеграционная платформа для предоставления различных сервисов пациенту,

сбора и анализа медицинской информации. Интересные решения для разных учреждений здравоохранения, построенные на базе единой платформы, есть в арсенале и других производителей. Все они предназначены для автоматизации основных процессов медицинской организации, связанных с обслуживанием пациентов: запись на прием, ведение единой ЭМК, хранение всей информации о пациенте, в том числе электронных изображений, анализ этой информации, интеграция со всем имеющимся медицинским и диагностическим оборудованием и т.д.

Тот факт, что российским законодательством стандарт ЭМК пока не принят, не является препятствием для внедрения подобных решений. Например, для ЕМИАС выбран международный открытый стандарт openEHR, который поддерживается Всемирной организацией здравоохранения, и вполне возможно, что именно на его основе будет построен российский стандарт для ЭМК. Не стоит опасаться и использования ИС иностранных вендоров – там информатизацией здравоохранения занялись намного раньше нас, соответственно, качество решений достаточно высокое, а для выхода на большой российский рынок любой вендор выполнит локализацию. **ИКС**

Разносторонний треугольник: пациент, врач и государство

Рынок решений для информатизации здравоохранения во многом зависит от государства – и не только от госфинансирования, но и от нормативной базы, которая не должна сдерживать внедрение новых, удобных для врача и пациента технологий.



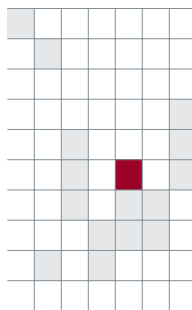
«ИКС»: Какие драйверы у информатизации здравоохранения в России и что тормозит внедрение ИТ в медицину?

Юрий БЕЛЬСКИЙ, директор представительства, Allied Telesis в России и странах СНГ: Главным драйвером является давно сформировавшийся в обществе запрос на основательную и комплексную модернизацию медучреждений в целом. Информатизация — то, без чего этот процесс невозможно представить. Люди недовольны медицинским обслуживанием и состоянием клиник, тем, сколько времени приходится в них терять. В попытке ответить на этот запрос на здравоохранение выделяются значительные бюджетные средства, однако зачастую, с одной стороны, их оказывается недостаточно

для проведения комплексной информатизации, а с другой – не всегда предлагаются оптимальные решения.

Михаил ПЕРЕВЕРЗЕВ, руководитель департамента сетевых решений, медицинские системы, «Фуджифильм-РО»: Важно, что информатизация здравоохранения неразрывно связана с изменением структуры финансирования медицины и переходом на платные услуги. В результате на первый план нередко выходят административно-аналитические задачи информатизации, а повышение эффективности работы врача оказывается на втором плане.

ДИСКУССИОННЫЙ КЛУБ «ИКС»



«ИКС»

Усложняет решение задачи высокая разнородность медицинских данных – медицинские документы, статистические отчеты, результаты диагностических и лабораторных исследований. Многие используемые в России МИС не имеют интерфейса HL7 для обмена медицинскими данными, либо нет опыта его корректного использования.

Владимир ДМИТРИЕВ, директор по продажам подразделения системной интеграции, T-Systems CIS: Пока основным драйвером и инвестором развития здравоохранения в России является государство. Программы развития телемедицины, внедрения единой ЭМК, технологии персонального мониторинга здоровья прописаны в качестве ключевых целей в Федераль-



В. ДМИТРИЕВ

ной программе здравоохранения на 2013–2018 гг. Например, уже к декабрю этого года процент медицинских карт, представленных в электронном виде, должен вырасти до 26%, а 95% всех федеральных государственных бюджетных учреждений должны поддерживать использование дистанционных форм диагностики и лечения (телемедицина).

Александр ВАСИЛЕНКО, глава представительства, VMware в России и СНГ: Основные барьеры для реализации проектов в здравоохранении – дефицит квалифицированных ИТ-кадров непосредственно

в медицинских организациях и сложности в организации качественных каналов связи. В связи с этим одно из главных требований к решениям, внедряемым в инфраструктуру медицинских организаций, – достаточно простое администрирование, с которым могли бы справиться специалисты лечебных учреждений.

Дмитрий ФИШЕЛЕВ, руководитель коммерческого блока, «ПингВин Софтвэр»: Безусловно, главным драйвером процесса является давление государства, обусловленное планом реализации госуслуг населению. В здравоохранении этот план требует для начала создания ИТ-ландшафта, покрывающего всю территорию России – со всеми вытекающими из этого последствиями. А главным тормозом процесса являются, собственно, сами врачи. Как недавно педагоги старались избежать применения в своей профессиональной деятельности компьютерной техники, так же сейчас это делают медики. Но педагогов освоить эту область заставили дети, а у врачей такого мощного драйвера нет. Средний возраст медицинского персонала, сложившиеся методы приема и лечения пациентов просто не оставляли места для информатизации. Всей стране известны случаи, когда закупленная сверхдорогая медицинская техника стоит без дела, потому что в этом ЛПУ никто не умеет ею пользоваться.



Д. ФИШЕЛЕВ



«ИКС»: Какие ИТ-решения наиболее востребованы сейчас в российском здравоохранении, изменились ли приоритеты в их выборе за последние год-два? И какие перспективные технологии и сервисы остались пока за бортом федеральной программы?

Артем РЯБИНКОВ, руководитель отдела по развитию бизнеса, «1С-Битрикс»: Повысился интерес к комплексным решениям, которые обеспечивают автоматизацию различных областей – учет услуг, регистратура, запись на прием к врачу онлайн, хранение и обработка изображений. Со своей стороны мы можем констатировать большой интерес к готовым интернет-решениям, интегрированным с внутренними МИС. У многих остро стоят задачи масштабного присутствия в интернете и предоставления актуальных данных пациентам онлайн.



Ю. БЕЛЬСКИЙ

Ю. БЕЛЬСКИЙ: Нынешний приоритет российского здравоохранения – построение базовой инфраструктуры во всех учреждениях.

Во многих регионах уже есть больницы и госпитали, использующие самые новые разработки.

Андрей СВИРИДЕНКО, председатель правления, SPIRIT: Аппаратные системы

ВКС зачастую по-прежнему чересчур дороги для медучреждений, поэтому наиболее удобными для предоставления консультаций и работы с пациентами оказываются программные продукты для видеоконференций. Особенно те, которые позволяют организовать видеоконференцию непосредственно через браузер. По нашим данным, организации здравоохранения сегодня составляют не менее 7% общего числа покупателей программных ВКС в России.



А. СВИРИДЕНКО



Д. КАТЮШИН

Денис КАТЮШИН, директор управления по консалтингу, Optima Consulting (группа Optima): Поскольку медицина все больше переходит на коммерческие рельсы, для многих ЛПУ теперь важно не только достойное качество диагностики и лечения пациентов, но и достижение целевых экономических показателей. Поэтому наряду со специализированными ИТ-решениями, ориентированными на диагностику, лечение, профилактику, в клиниках востребо-

ваны решения для автоматизации управленческого и бухгалтерского учета, а также системы бизнес-аналитики, которые позволяют проводить разносторонний анализ деятельности клиники вплоть до конкретной услуги, врача, кабинета.



И. НИКУЛИН

Игорь НИКУЛИН, директор департамента ИТ, КРОК: Самые перспективные технологии в здравоохранении по большей части те же, что и в других областях. В первую очередь нужно создать ИТ-инфраструктуру, автоматизировать рабочие места медицинских сотрудников, внедрить специализированные системы аналитики и СЭД, решить вопрос защиты

данных. Дальше уже можно будет думать о системах телемедицины, мобильных решениях и т.д. При реализации федеральной программы информатизации здравоохранения, на мой взгляд, можно было больше внимания уделить методологии внедрения информационных сервисов, таких как запись на прием к врачу, ускоренная госпитализация, аналитика работы лечебных учреждений.

Дамир ЕНГАЛЫЧЕВ, директор по работе с ключевыми заказчиками департамента по работе со здравоохранением, IBS: В текущем фокусе информатизации – по-прежнему административные процессы: учет затрат, управление ресурсами, минимизация бумажного документооборота, снижение затрат и повышение качества подготовки медицинской отчетности и статистики. Тем не менее уже в рамках федеральной и региональных программ



Г. ШЕВЧЕНКО

здравоохранения предусмотрено внедрение технологий, направленных на автоматизацию самого лечебного процесса. Появляются отдельные элементы поддержки принятия врачебных решений (поддержка стандартов лечения, предупреждение о лекарственном взаимодействии при выписке электронного рецепта, предоставление врачам доступа к медицинской информации). В качестве наиболее интересных направлений можно отметить технологии речевого ввода информации, поддержки принятия решений на основе сведений, содержащихся в ЭМК пациента, технологии медицинских исследований, позволяющие выявлять закономерности на основе анализа больших объемов псевдонимизированных медицинских данных.

Григорий ШЕВЧЕНКО, коммерческий директор, «Открытые Технологии»: К сожалению, сегодняшний процесс информатизации медицины развернут в сторону ИТ-компаний, а они пытаются адаптировать уже имеющиеся решения для других отраслей под задачи медицинской информатизации. Надо вернуться к истокам, посмотреть на задачи в комплексе, увидеть и проанализировать то, что уже сделано и сделано хорошо. И в первую очередь заняться разработкой и внедрением технологий, повышающих качество лечения и управления лечебно-диагностическим процессом. Ведь медицина прежде всего должна лечить и вылечивать, а потом уже эффективно управлять финансами.



Д. ЕНГАЛЫЧЕВ



«ИКС»: Какова ситуация со стандартами, которые должны обеспечить совместимость разных МИС? Приживутся ли в России западные стандарты? И нужна ли разработка национальных?

А. РЯБИНКОВ: На сегодня в России нет общепринятого стандарта для взаимодействия медицинских систем. Например, стандарт HL7, широко распространенный в мире, далеко не всегда применим в конкретных российских проектах – прежде всего в силу высокой сложности, избыточности, проблем с русификацией. По этой причине для интеграции веб-систем с МИС многие производители медицинского ПО используют свои закрытые форматы. Необходим российский отраслевой стандарт для этих задач, и тогда решать их будут гораздо быстрее и эффективнее.



А. РЯБИНКОВ

Андрей ЕГОРОВ, ведущий архитектор практики медицинских проектов, AT Consulting: После принятия концепции создания ЕГИСЗ и начала ее разработки множественность стандартов перестала быть

актуальной. Тем не менее требуется большая работа в области стандартизации электронных документов. Прямой перевод существующей системы «бумажной» медицинской документации в электронный вид не принесет ожидаемых результатов, а, возможно, только повысит трудоемкость их создания.

Д. ЕНГАЛЫЧЕВ: Собственных стандартов обеспечения interoperability медицинских данных в России нет. Всё, что есть, так или иначе заимствовано или локализовано. Создание собственных стандартов – это очень длинный и затратный путь. Сейчас нет школ, которые могут взять на себя эту задачу. А те организации, которые готовы подключиться к международному процессу стандартизации, не получают достаточного и системного финансирования.



А.ЕГОРОВ



«ИКС»: Насколько полезен зарубежный опыт внедрения медицинских ИС? Как показали себя в российских условиях западные решения для информатизации медицины?



С. ШЕРБИНА

Сергей ШЕРБИНА, заместитель гендиректора, Esri CIS: Платформенные технологии западных поставщиков вполне могут использоваться в России, наша система хотя и имеет свою специфику, но задачи, стоящие перед ней, совершенно не уникальны. Например, проведение геостатистического анализа распространения того или иного заболевания и выявление опреде-

ляющих его факторов требует одних и тех же инструментов независимо от страны. В этом смысле оправдано использование продуктов, «обкатанных» в сотнях и тысячах реальных внедрений по всему миру.

Г. ШЕВЧЕНКО: Западный опыт на российском рынке фактически не востребован, очень немногие иностранные фирмы предлагают здесь свои МИС. Не существует стандартного механизма передачи или обмена опытом применения ИТ между Западом и Россией ни в медицине, ни в любой другой индустрии. Что касается доработки и тиражирования западных МИС, это также непросто. У нас сегодня нет двух похожих клиник, поэтому о ти-

повых внедрениях говорить не приходится, под каждое конкретное учреждение нужна существенная доработка.

Сергей МАРТЫНОВ, директор по развитию бизнеса с госсектором, «Техносерв Консалтинг»: Западные МИС отражают специфику модели зарубежного здравоохранения, поэтому без доработок они не могут массово использоваться в России. Есть отличия в функциональных обязанностях работников (например, за рубежом медицинская сестра выполняет значительный объем тех работ, который у нас выполняет врач), в нормативах времени на прием одного пациента и т.д. Но отдельные направления развития зарубежных систем нашли применение при создании отечественных МИС – например, разработка формализованной клинической документации (стандарт openEHR). Открытый стандарт управления, хранения и обмена электронными историями болезни – это как раз тот опыт, который может быть успешно перенесен из западной практики в отечественную.



С. МАРТЫНОВ



«ИКС»: Ваши ожидания от информатизации здравоохранения в ближайшие годы?

С. ШЕРБИНА: Мы ожидаем развития региональных систем и их интеграции в единую федеральную систему управления здравоохранением, роста востребованности порталных решений, внедрения систем для решения задач управления и оптимизации ресурсов и объектов инфраструктуры здравоохранения, более эффективных систем диспетчеризации, повышения оперативности и качества собираемых медицинских и других данных.



М. ПЕРЕВЕРЗЕВ

М. ПЕРЕВЕРЗЕВ: Участие в проектах информатизации здравоохранения уже привело к росту профессиональной грамотности всех заинтересованных сторон – врачей, пациентов, ИТ-специалистов, руководителей здравоохранения и т.д. Это ведет к формированию новых, более четких требований к информационным сервисам в медицине. Кроме того, постепенное

развитие сетевой инфраструктуры будет способствовать более широкому использованию облачных решений в здравоохранении.

С. МАРТЫНОВ: Наиболее мощные прорывы произойдут в частной медицине. А поскольку для негосударственных медицинских учреждений очень важен аспект экономической эффективности, то они будут активно внедрять специфические для отрасли «ERP». Помимо базового функционала в таких системах най-

дут отражение ряд бизнес-процессов и задач, специфичных для медицинского учреждения.

В. ДМИТРИЕВ: Мы надеемся, что в стандартах по здравоохранению появятся такие направления, как телемедицина, и будет пересмотрена правовая база для появления этой услуги в России. Следует также ожидать появления единой карты пациента, и с технологической точки зрения работы эти ведутся. Но правовая база пока определяет работу с бумажными картами как единственно возможный вариант.

А. ВАСИЛЕНКО: В 2012 г. в России была создана база для развития ИТ-инфраструктуры в медицине, к концу 2013 г. формирование единого информационного пространства в основном будет завершено, но отдельные блоки будут постепенно внедряться еще в течение нескольких лет. В ближайшие годы мы ожидаем дальнейшего развития и становления высокотехнологичного медицинского сектора. Основная идея – наладить обмен медицинской информацией, увеличить скорость обработки запросов на местах и структурировать все данные в электронном виде.



А. ВАСИЛЕНКО

ПОЛНЫЙ ТЕКСТ

Дискуссионного клуба читайте на



Трансформаторные ИБП в медучреждениях: надежность прежде всего



↑ Константин ЕРМАКОВ



↑ Алексей МОРОЗОВ

Мощные ИБП двойного преобразования, построенные по трансформаторной схеме, незаменимы там, где требуется надежная защита оборудования. Об особенностях их применения в больницах и медицинских центрах мы беседуем с Константином ЕРМАКОВЫМ, главой представительства компании Powercom в России, Казахстане и Белоруссии, и с Алексеем МОРОЗОВЫМ, директором по дистрибуции.

В защите нуждаются

– Какому медицинскому оборудованию необходима защита электропитания?

Алексей МОРОЗОВ: Прежде всего оборудованию, установленному в операционных и отделениях интенсивной терапии. Это аппараты искусственной вентиляции легких, наркозно-дыхательные аппараты, мониторы пациента – их бесперебойная работа жизненно необходима в прямом смысле слова. Кроме того, по требованиям ГОСТа ИБП должны применяться для защиты электропитания лифтов, поднимающих больных в операционные.

В надежной защите электропитания нуждается все дорогостоящее диагностическое оборудование, например магнитно-резонансные и компьютерные томографы. Ну и конечно, никто не отменял требований по использованию ИБП для защиты установленного в медучреждении ИТ-оборудования, систем освещения и вентиляции.

– От каких проблем с электропитанием требуется защищать высокотехнологичное медицинское оборудование?

А. М.: В первую очередь от полного пропадания напряжения в электросети и от существенных отклонений в его качественных характеристиках, которые могут привести к отключению защищаемого оборудования. И онлайн-ИБП Powercom серии ONL-33-II высокой мощности защищают дорогостоящее диагностическое оборудование от всего спектра проблем: от пропадания напряжения, различных помех, искажения формы синусоиды. В этих системах

проверенная временем схемотехника сочетается с расширенными функциями управления.

Заказчику требуется...

– Какие требования к оборудованию для защиты электропитания выдвигают медучреждения в конкурсной документации?

А. М.: По нашему опыту, больше всего заказчиков этой категории интересует надежность и отказоустойчивость оборудования. Эти требования выдвигаются еще на этапе выбора поставщика, поскольку для медицинских учреждений они критичны. Второе место по частоте запросов занимают сроки поставки ИБП, на третьем – время, которое потребуется для его установки, и, естественно, качество установочных работ.

– То есть вы хотите сказать, что цена такого оборудования у заказчиков из сферы здравоохранения не на первом и даже не на третьем месте?

А. М.: Многие из них сегодня понимают, что цену ИБП не стоит ставить во главу угла, поскольку она составляет считанные проценты стоимости высокотехнологичного оборудования.

Константин ЕРМАКОВ: Если клиническая больница или медицинский

центр получили из бюджета миллион долларов на томограф, то экономить на ИБП – значит, не защищать уже сделанные инвестиции. Вместе с тем компания Powercom всегда стремилась к тому, чтобы предлагать оптимальное соотношение цена/качество. Если бюджет заказчика ограничен, мы стараемся «вписаться», а если ничего не сможем подобрать, то так и скажем. И уж точно не будем предлагать ему дешевое и заведомо неработоспособное решение: мы очень дорожим своей репутацией.

– Обращают ли внимание заказчики из сферы здравоохранения на энергопотребление источников бесперебойного питания, как это делают операторы ЦОДов?

А. М.: Для них все-таки важнее бесперебойность и отказоустойчивость оборудования. Именно этими качествами отличаются мощные трансформаторные ИБП Powercom. Их высокая надежность и помехозащищенность обеспечиваются за счет гальванической развязки, т.е. полной изоляции выходной цепи от входной.

К. Е.: Задача ЦОДов – зарабатывать деньги, поэтому и все затраты считаются там скрупулезно. К тому же надо

Справка

Поставки систем защиты электропитания Powercom для нужд отечественного здравоохранения начались в 2005–2006 гг. Тогда ИБП были установлены на всех подстанциях столичной скорой помощи. В 2008 г. источниками бесперебойного питания Powercom ONL-II-60K33 был оборудован КГБУЗ «Перинатальный центр» в Хабаровске. В начале 2012 г. в рамках городской программы по модернизации здравоохранения в клинические больницы Москвы были поставлены 70 систем ONL-33-II мощностью по 120 кВА для защиты электропитания магнитно-резонансных томографов, а до конца 2012 г. все ИБП были запущены в эксплуатацию. Сегодня в портфеле компании несколько новых «медицинских» проектов.

понимать, что чудес не бывает и что эффективность у всех ИБП примерно одинаковая. И хотя коэффициент полезного действия трансформаторных систем на 1–2% ниже, чем у транзисторных, зато они обладают высокой перегрузочной способностью. А это существенно снижает риск отключения в случае незапланированной перегрузки.

– Как бы вы оценили востребованность заказчиками из сферы здравоохранения функций мониторинга ИБП?

А. М.: У нас было несколько проектов в регионах, в рамках которых мы поставляли онлайнные ИБП небольшой мощности в больницы для защиты ИТ-оборудования – рабочих мест и серверов. Поскольку на одно лечебное учреждение приходилось одно устройство, его размещали в серверной стойке и устанавливали в него трехпортовую SNMP-карту, к одному разъему которой

ценные и сертифицированные нами инженеры наших сервисных партнеров. Перед инсталляцией ИБП они проверяют проводку, наличие защитных автоматов, а для мощных устройств – и систем охлаждения. Затем, если все условия выполнены, производят подключение источника бесперебойного питания и обучают сотрудников заказчика основным операциям с ним. Замечу, что в старших моделях ИБП Powercom есть возможность заблокировать сервисные функции, чтобы нельзя было внести изменения, которые могут привести к выходу ИБП из строя или его отключению. После подписания акта сдачи заказчик регистрирует установленное оборудование на нашем сайте, чтобы мы могли обеспечить ему должный уровень сервиса и постгарантийной поддержки.

– Какую роль исполняет при реализации проектов по установке ИБП представительство Powercom?

К. Е.: С момента обращения к нам заказчика или партнера мы принимаем в проекте живое участие: консультируем партнеров, помогаем и с расчетами мощности, и с определением параметров места инсталляции, и с оценкой готовности помещения к установке оборудования. Повторюсь, мы дорожим своей репутацией



ИБП ONL-33-II общей мощностью 45 кВА для обеспечения бесперебойной работы операционной

подключалась сеть, ко второму – датчики температуры и влажности, а к третьему – беспроводные датчики открытия окон и дверей, а также задымления. В результате системный администратор, в ведении которого находится сразу несколько больниц, может получать сообщения обо всех изменениях параметров окружающей среды в серверных и при необходимости реагировать на них.

Сервис «на уровне»

– Как подходит компания Powercom к сервису, гарантийному и постгарантийному обслуживанию ИБП в медицинских учреждениях?

А. М.: Инсталляцию всех наших систем высокой мощности выполняют только авторизованные специалисты – сотрудники представительства или обу-

ей и предпочитаем все несколько раз перепроверить. Как показывает наш опыт, в 60% случаев причиной выхода из строя ИБП является неправильно подобранная мощность. С новым партнером первые несколько инсталляций обязательно выполняем вместе. Иными словами, практически каждый мало-мальски крупный проект мы держим под контролем.

– Сколько у представительства Powercom в России сервисных партнеров?

К. Е.: У нас 180 партнеров в более чем 100 городах. Но сервисных сетей у нас две. Первая – это «Сеть компьютерных клиник», она отвечает за ремонт всего спектра нашего «легкого» оборудования, а вторая – «ЦРТ-Сервис» (входит в ГК MAYKOR). Именно ее инженеры занимались подключением ИБП для за-

щиты томографов во всех клинических больницах Москвы.

Фундамент для будущего роста

– Можно ли сказать, что лечебные и диагностические учреждения – фокусное направление поставок ИБП для глобальной компании Powercom?

К. Е.: Я бы так не сказал, поскольку это в России государство сейчас активно вкладывает средства в модернизацию здравоохранения. Нашим коллегам за рубежом приходится фокусироваться на других вертикальных рынках. Так что в области поставок ИБП для медицины российское представительство лидирует в глобальной компании точно так же, как и по объему продаж этого оборудования в целом (доля российского представительства в глобальных продажах Powercom приближается к 20%).

– Есть ли у вас «медицинские» проекты в Казахстане и Белоруссии?

К. Е.: Сопоставимых проектов пока нет, но это связано с тем, что мы присутствуем в этих странах сравнительно недавно. В Астане у нас есть дистрибьютор. Кроме того, наши российские дистрибьюторы тоже имеют офисы в Казахстане. Так что мы надеемся реализовать там несколько интересных проектов.

А. М.: В Белоруссии мы разворачиваем инфраструктуру, сертифицируем специалистов для инсталляции «тяжелых» систем, недавно открыли сервисный центр в Минске. Белорусские коллеги констатируют, что тенденции, наблюдающиеся в России, отмечаются у них с опозданием на два года. Исходя из этого, можно предположить, что уже в следующем году в Белоруссии будут выделены деньги на модернизацию здравоохранения. И мы к этому готовы.



Представительство Powercom
в России, Казахстане
и Республике Беларусь:
+7(495) 651-6281;
www.pcm.ru

Снова в «ЗЕЛеной» зоне

В конце сентября – начале октября на российском фондовом рынке сохранялся довольно устойчивый восходящий тренд, но большинство отраслей, кроме нефтегаза, росли медленно. Зато бумаги телеком-компаний торговались заметно лучше рынка.



**Анна
ЗАЙЦЕВА,**
аналитик,
УК «Финам
Менеджмент»

Из мировых факторов драйверами роста рынка выступали надежды на разрешение проблемы американского госдолга, а также окончание shutdown – вынужденного отпуска государственных учреждений в США. Политики долго не могли договориться, но в последний момент был найден компромисс, который помог Штатам избежать технического дефолта.

На российских площадках основным локомотивом движения был нефтегазовый сектор, в других отраслях рост шел существенно медленнее. Отметим, что совсем недавно

был опубликован большой блок статистических данных, касающихся экономики РФ, который не вызывает особого оптимизма. Так, инвестиции в основной капитал по итогам трех кварталов упали на 1,4% (г/г). Данные по розничному обороту оказались не лучше: в сентябре рост показателя замедлился до 3% (г/г) – минимального значения с мая этого года. Таким образом, ключевые драйверы роста российской экономики, на которые возлагались большие надежды, по-прежнему не работают.

Показатели сектора телекоммуникаций были в целом заметно лучше рынка. Поддержку котировкам игроков ТМТ-индустрии оказывали в первую очередь многообещающие корпоративные новости и рост интереса к технологичным секторам на фоне больших объемов свободной ликвидности. А бумаги отдельных эмитентов продемонстрировали и существенно более сильную динамику.

Сотовики вырвались в лидеры

Наиболее сильные результаты в отчетном периоде зафиксированы в бумагах «Вымпелкома» – расписки оператора подорожали на 17% (до 13,17). Формально основным катализатором роста стала новость о включении бумаг компании в индекс NASDAQ-100 с 29 октября, в день сообщения объемы торгов выросли почти в 4 раза к стандартным средним уровням. Дополнительный позитивный фон создали заявления

о планируемом листинге на европейских площадках. Вхождение в индекс и выход на биржи Европы, где концентрируется значительная часть глобального бизнеса Vimpelcom, несомненно, положительно отразится на ликвидности бумаг и станет одним из наиболее эффективных шагов к повышению рыночной капитализации. Необходимо учесть и фундаментальный фактор – с середины октября группа Telenor, контролирующая крупнейший мажоритарный пакет оператора, в результате прекращения действия моратория 2011 г. сможет конвертировать 305 млн своих префов «Вымпелкома» в обыкновенные акции. У компании есть на это 2,5 года, и пока она, по официальным заявлениям, не торопится исполнить опцион. Тем не менее эти обстоятельства определенно мотивируют инвесторов к покупкам, так как в результате конвертации капитализация может заметно вырасти, а free-float – сократиться.

На втором месте по темпам роста – бумаги МТС. За отчетный период они выросли в цене на 7,8%, до 341 руб. за акцию, и уверенно демонстрируют хорошую восходящую динамику. При этом новостной фон был скорее нейтральным: наиболее сильным корпоративным катализатором роста можно считать утвержденное ВОС решение о выплате дивидендов за первое полугодие 2013 г. в размере 10,786 млрд руб. (завершение выплат – 29 ноября), а также сообщение о выкупе материнской АФК «Система» 0,3% МТС за \$60 млн.

Несколько слабее выглядели результаты «Ростелекома». Тем не менее предыдущая коррекция уступила место заметному восходящему движению. Акции оператора подорожали на 5,5% – до 108 рублей за штуку. Компания порадовала целым рядом корпоративных новостей и многообещающих инициатив. Основным драйвером роста для ее бумаг, конечно, остается развитие событий вокруг Tele2. Напомним, что 17 октября новым владельцем 50% Tele2 стала группа стратегических инвесторов – банк «Россия» Юрия Ковальчука и структуры «Северстали» Алексея

Справка ИКС



В период с 25 сентября по 20 октября индекс ММВБ вырос на 3,87% – до отметки 1535,17 пункта, а индекс РТС прибавил 4,4%, до 1516,96 пункта. Отраслевой индекс «ММВБ телекоммуникации» показал прирост на 6,3% – до 2472,12 пункта.

Мордашова. С высокой вероятностью сделка прошла в интересах «Ростелекома» и в ближайшее время будет проведена интеграция бизнеса Tele2 с мобильными активами национального оператора. Этот сценарий, учитывая, что издержки консолидации «Ростелеком» в такой конфигурации практически не несет, формирует значительный апсайд для роста его капитализации.

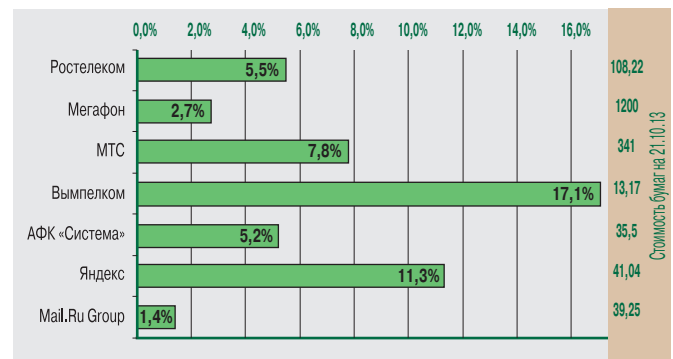
Другая интересная новость – сообщение о возможном приобретении «Ростелекомом» крупного розничного банка (предметом сделки в СМИ называют «Собинбанк»). В целом можно вполне позитивно интерпретировать такую стратегию. Тенденция приобретения или создания собственного банка сейчас широко распространена в телеком-секторе: МТС уже давно развивает «МТС-Банк», а гендиректор «МегаФона» совсем недавно обмолвился, что компания находится в поиске небольшого банка для последующей покупки. Собственно, эта сделка продиктована рыночными реалиями: «Ростелекому» нельзя отставать от конкурентов, тем более в свете возможного создания СП с Tele2. Приобретение собственной банковской структуры позволит компании двинуться в финансовый сектор и начать работать над развитием мобильного банкинга, POS-кредитования и системы онлайн-платежей.

И наконец, наименее выраженные темпы роста среди операторов связи показали бумаги «МегаФона». На российской площадке они торговались довольно волатильно, но в целом уверенно удержались в «зеленой» зоне. Котировки выросли за период на 2,7% – до 1200 рублей за бумагу. Новостной фон был довольно спокойным, основным корпоративным событием стало официальное завершение сделки по приобретению 100%-ной доли в Maxiten Co Limited (владеющей 100% долей в ООО «Скартел» и ООО «Йота») у Garsdale Services Investment Limited. Общая стоимость сделки составила \$1,18 млрд (учитывались обязательства по обеспечению долговых гарантий по задолженности аффилированных структур). В целом поглощение бизнеса Yota, конечно, давно учтено в котировках; тем не менее окончательное завершение сделки означает консолидацию результатов спутника в отчетности «МегаФона», что, учитывая отрицательную маржинальность «Скартел», может оказать давление на показатели рентабельности оператора. Нивелировать негативный эффект могла бы заметная синергия на операционном уровне, но полная интеграция активов и достижение качественных положительных результатов, вероятно, произойдут как минимум в среднесрочном периоде.

«Яндекс» идет в кино

Бумаги АФК «Система» по итогам периода продемонстрировали рост на 5,2%; в целом акции компании торговались в рамках рыночных трендов. Одной из наиболее заметных новостей стало сообщение о покупке председателем правления АФК Михаилом Шамолиным и членом правления Антоном Абуговым 0,2% компании на сумму около \$24 млн. Такой новост-

Изменение котировок телеком- и ИТ-компаний
с 25.09.13 по 21.10.13



ной фон краткосрочно позитивно повлиял на котировки – как правило, рынок положительно интерпретирует личные инвестиции топ-менеджеров в акции возглавляемых ими компаний, особенно если речь идет о значительных суммах, что обычно свидетельствует о высокой оценке менеджментом перспектив развития и потенциала увеличения капитализации.

Довольно интересно в рассматриваемый период выглядели бумаги крупнейшего российского поисковика: капитализация «Яндекса» выросла на 11,3%, стоимость расписок группы на NYSE достигла \$41. Компания анонсировала ряд событий, в перспективе значимых для котировок. Главное из них – объявление о покупке сервиса «КиноПоиск», одного из самых популярных ресурсов Рунета в сфере видео- и киноиндустрии (стоимость M&A оценивается в горизонте \$40–50 млн). Сделка позволит «Яндексу» не только контролировать высоко-рентабельный и быстрорастущий бизнес, но и сформировать на базе профильных компетенций и контента ресурса сильные дополнительные сервисы в сфере видеопродукции и киноиндустрии, что будет работать на укрепление лидерских позиций корпорации на рынке поиска. На фоне динамичного роста спроса на видео-контент сделка M&A, которая обеспечит поисковику быстрый синергический эффект, безусловно, весьма актуальна.

«Яндекс» также объявил о запуске нескольких новых сервисов, в частности бесплатного инструмента для анализа аудитории мобильных приложений «Яндекс.Метрика», и декларировал планы внедрения в сервис «Яндекс.Маркет» модели CPA, ориентированной на повышение рекламных доходов. Компания продолжает активное развитие и демонстрирует позитивные операционные результаты. Мы ожидаем, что отчетность, которую «Яндекс» опубликует в конце октября, будет достаточно сильной и способной оказать поддержку котировкам компании.

Существенно более низкий уровень роста, на 1,4%, показали расписки Mail.Ru Group. В отчетный период новостной фон вокруг компании был нейтральным, практически без интересных корпоративных событий. При этом мы ожидаем публикации довольно хорошей отчетности (в третьей декаде октября), что может стать катализатором роста котировок компании. ИКС

Очередные задачи Телекома

К новому сдвигу парадигмы

Окончание. Начало см. «ИКС» № 8-9' 2013, с. 66.



– Доктор, как прошла операция?

– А я не доктор, я – апостол Петр!

Реализация концепции программно определяемых сетей превратит телеком в универсальный инструмент коммуникации. Количественные изменения перейдут в качественные, и вполне возможно, что когда-нибудь телеком сольется со всеобъемлющим интернетом.



Александр
ГОЛЫШКО,
канд. техн. наук

Программно определяемое счастье

Несмотря на то что «революционная» концепция NGN во многом использовала технологии и принципы построения компьютерных сетей, отделив уровень инфраструктуры от уровня сервиса, гибкости и универсальности компьютерной сети в части перераспределения ресурсов, смены функционала и пр. она достичь не сумела. Усложнение сетей и сетевых хранилищ привело к тому, что на первый план сегодня выдвигается управление и ими, и передаваемыми по ним данными. К примеру, по оценке IBM, 20 лет назад в типовом вычислительном центре на эти цели приходилась почти треть затрат, а сейчас – почти две трети. Ныне перед телекомом стоит задача преодоления этого недостатка путем перехода на программно определяемые сети (Software-Defined Networks, SDN – см. также → с. 88), с которыми благодаря виртуализации оператор сможет модифицировать сеть в полном соответствии с собственными нуждами и нуждами своих клиентов. То есть действовать подобно тому, как обычно действуют системные администраторы в компьютерной индустрии.

Концепция SDN делит инфраструктуру на два независимых уровня, где уровень управления (как правило, проприетарный для каждого вендора) отделен от уровня передачи данных. Собственно, управлять современными сетями со многими тысячами серверов, маршрутизаторов, базовых станций, фемтосот и точек доступа Wi-Fi эффективно не удастся никому – потому и возник другой подход. Каждый сетевой элемент с SDN-

функционалом поддерживает специально разработанный протокол OpenFlow для удаленного управления посредством надсетевого SDN-контроллера и ПО, базирующегося на OpenStack.

В целом SDN позволяет создавать поверх текущего слоя инфраструктуры логическую инфраструктуру виртуальных сетей (имеющих, к примеру, для каждого клиента свою конфигурацию), полностью абстрагированную от физического сетевого оборудования с соблюдением аппаратной «межплатформенности» и «вендорнезависимости». Иными словами, каждый сетевой элемент отныне представляет собой этакий «бутерброд» из «неинтеллектуального железа», выполняющего лишь функцию соединения с другим сетевым железом, и загруженного по стандартным процедурам в его память «интеллекта» (ПО, управляемого с помощью SDN-контроллера). Контроллер SDN занимается оркестровкой своих подчиненных и может не только дирижировать сетевыми соединениями и прочими ресурсами, но и, извините за выражение, менять «ориентацию» сетевых узлов в зависимости от текущих потребностей оператора. То есть конечная цель концепции SDN заключается в том, чтобы все сетевые узлы превратились просто в компьютеры, которые по мере необходимости путем дистанционной смены ПО можно трансформировать в маршрутизаторы или переключатели, серверы доступа или серверы приложений (они, конечно, и сегодня представляют собой компьютеры, но пока проприетарные). Так сеть связи становится воистину универсальной и практически неот-

личимой от хорошей компьютерной сети или интернета, а, скажем, технический директор превращается в системного администратора.

Итак, с помощью SDN оператор сможет модифицировать сеть в полном соответствии с собственными нуждами и нуждами своих клиентов. Абстрагирование от сети дает возможность отдавать такие приказы, как «доступ к данной VPN допускается только с безопасного места» или «первым хотелось бы услышать начальника транспортного цеха». Теоретически SDN-контроллер может царить над сетями сразу нескольких операторов, что, в частности, придаст новое и более широкое наполнение концепции виртуальных операторов. Продолжая эти рассуждения в духе виртуализации, аутсорсинга и network sharing, можно даже ограничиться одним национальным инфраструктурным оператором, на базе которого будут существовать (и неплохо себя чувствовать в виде виртуальных операторов) все остальные субъекты рынка, включая ныне здравствующих. И это было бы выгодно для всех (в Европе, например, уже задумались о создании единой сети и для начала собираются отменить роуминг).

Введение SDN позволяет не только более эффективно использовать сетевые ресурсы, но и превратить управление сетями из «искусства избранных» в чисто инженерную задачу, повысить безопасность и предоставить пользователям возможность программно создавать новые сервисы и оперативно загружать их в сетевое оборудование. Иначе говоря, благодаря продолжающейся ИКТ-конвергенции с помощью SDN можно легко создавать и «трубы в облаках», и «облака в трубах», о чем, кстати, придется поразмышлять и регулятору. А, быть может, и не надо размышлять, а надо просто относиться к тем и другим одинаково, потому что разница между облаками и трубами в ряде случаев будет весьма условной.

Разумеется, «традиционным» связистам все это может казаться удивительным, но таковы уж ИКТ-тренды, и, главное, они логичны. Подобные процессы происходят в отрасли не в первый раз. Можно вспомнить, к примеру, сколько лет вершиной в телефонии считался шаговый искатель. Механических аналогов ему в мире не было. И казалось невероятным, что однажды его «похоронят» какие-то потомки арифмометров. А теперь восходящие программно определяемые сети и хранилища данных объединяются в программно определяемое окружение (Software-Defined Environment, SDE). Кто бы мог подумать, что эпоха конвергенции приведет даже не к персональным сервисам, а к персональному ИКТ-окружению. То есть потенциально вся ИКТ-отрасль будет способна подстраиваться под конкретного пользователя сервисами, хранилищами, сетями, качеством и пр.

Что же дальше? По мере претворения в жизнь описанного выше вся ИКТ-инфраструктура превратится в две технологически одинаковые компьютерные сети (отличающиеся лишь своими внутренними «правилами игры»), наложенные одна на другую: операторскую

сеть и интернет. Чтобы попасть в ту или иную сеть (или же получить свою виртуальную сеть либо ЦОД), пользователю будет необходимо, как и сегодня, наладить соответствующие отношения с операторами (скорее всего, виртуальными). И не будет ли дешевле ограничиться одной сетью? Той самой глобальной/национальной информационной магистралью, с которой и началась вся модернизация ИКТ в середине 90-х годов прошлого века.

Конечно, в этом месте читатель вправе усомниться: мол, когда еще это будет у нас, в России. Ответ может быть таким: если вы живете в России, значит, при рождении вы выбрали сложный уровень. Тренды же остаются трендами везде, поэтому перестаньте совершать одни и те же ошибки. Будьте креативными! Совершайте новые!

Колдобины на программно определяемой дороге

Представим, что все оборудование на сети обладает интерфейсом OpenFlow, его ПО не зависит от вендора, а «железо» у всех вендоров стандартно. Вроде бы все довольны, но по иронии судьбы признанные телеком-вендоры могут пострадать при развитии SDN, как страдал от некоторых своих изобретений отец Кабани.

Пока сетевое оборудование с элементами SDN позволяет операторам снижать эксплуатационные расходы и экономить сетевые ресурсы – всем хорошо. Но если со временем все оборудование будет сводиться к неким вендоронезависимым «тупым железкам», а их «интеллект» (открытое ПО) будет доступен для любого поставщика, то уже завтра не в интернете, а непосредственно в операторских сетях будут царить такие серьезные поставщики ПО, как IBM, Google или Microsoft (они ведь тоже занимаются SDN), обыграть которых на их поле отнюдь не просто. И чтобы будущая роль «традиционных» вендоров не ограничилась, это как предполагают некоторые эксперты, лишь производством «тупых железок», они должны постараться что-нибудь придумать в виде некоего промежуточного уровня SDN (например, уровня абстракции или уровня «дирижирования»), который таки будет зависеть от вендора.

Аналогичные процессы вполне ожидаемы и в области SDS (только бизнес – ничего личного). Но именно на эту грань в становлении SDE на сетях будущего следует обратить внимание национальным регуляторам в рамках так называемого технологического нейтралитета, который в грядущие «программно определяемые» времена обретет новый смысл.

Учет и контроль – основа «всеобщего виртуализма»

Увлекаясь виртуализацией, нельзя упускать из виду трафик и доходы. Сегодня контроль трафика вплоть до трафика конкретного пользователя с помощью технологии глубокого анализа пакетов (Deep Packet Inspection, DPI) уже возможен и даже рекомендован МСЭ. Эта технология позволяет провайдерам иссле-

довать и контролировать практически всю информацию, передаваемую по сети: следить за качеством потребляемой услуги, отфильтровывать торрент-трафик или незаконные подключения, а также перехватывать сообщения пользователей. Как и любая технология в нашем мире, DPI может использоваться как в благих, так и в неблагоприятных целях. Однако при этом она (или какая-либо ей подобная) является практически единственным инструментом для всестороннего мониторинга качества сервиса (вплоть до его восприятия пользователем), для поддержки работы СОРМ, для обеспечения информационной безопасности, для установления отношений с другими поставщиками трафика данных (с учетом сетевого нейтралитета) и для «ограждения» собственных владений в глобальной компьютерной сети будущего.

Дело идет к тому, что без этого механизма операторам будет попросту нечего делать в сетях – сервис не контролируется, трафик куда-то девается, клиент уходит, регулятор закидывает логичными неприятными вопросами, да и конкуренты распоясываются...

Никто не уйдет обиженным

Согласно прогнозам футурологов, нас ждет «всеобъемлющий интернет» (Internet of Everything, IoE). Причем на грядущее подключение своих продуктов к IoE современные производители электроники уже начали ориентироваться. Пока сетевой трафик – это прежде всего коммуникации «человек – человек», завтра начнет доминировать трафик «человек – физический объект». А переход к трафику «машина – машина» (M2M) или «физический объект – физический объект» станет настоящей революцией, причем новые сетевые объекты будут возникать тихо и незаметно.

Важнейшее условие реализации IoE – интеллектуальные сетевые функции, выводящие контролируемость, управляемость и масштабируемость сети на уровень, необходимый для поддержки невероятно большого числа соединений (до 50 млрд к 2020 г.), и нам теперь в целом понятно, как эти функции будут организованы. IoE повышает важность и ценность сетевых соединений, и эта ценность определяется не фактом наличия соединений и даже не их числом, а их практическим результатом, ибо он и открывает невиданные ранее возможности.

Проанализировав потенциальный эффект воздействия IoE на экономику в 27 отраслях, специалисты Cisco пришли к выводу, что в течение следующих десяти лет он сулит частному бизнесу во всем мире экономическую выгоду в сумме \$14,4 трлн. По их подсчетам, в ближайшее десятилетие IoE способен увеличить совокупную прибыль мировых корпораций примерно на 21%.

Согласно докладу Gartner «Инновации всеобъемлющего интернета изменят бизнес», когда-нибудь «люди сами станут узлами интернета с пакетом статической информации и активной системой посто-

янной отправки данных». Тут возникнет много вопросов о сохранности персональных данных, защите государственных интересов, свободе личности в мире IoE и пр. По большей части это будут уже не технические вопросы, и разрешить их когда-нибудь люди смогут только сообща. Возможно, мы будем получать сообщения типа: «Ваше письмо помечено как спам и сожжено. С уважением, «Почта России»». Возможно даже, что известная картина Ильи Репина будет именоваться так: «Запорожцы умышленно распространяют непроверенную информацию, порочащую честь и достоинство турецкого султана». А возможно, что и ИКТ-инфраструктура, и все виртуальные операторы будут иметь наднациональный характер и равные регуляторные права на всей планете.

С технической же точки зрения нас будет интересовать следующее: если все в мире подключено к IoE, то нужны ли какие-либо отдельные операторские сети? Иначе говоря, не растворятся ли будущие операторские компьютерные сети в изо дня в день крепчающем интернете? Уже сейчас в сетевых браузерах начинают появляться сервисные «кнопочки-приложения» с качественным голосом, сообщениями, видео и прочим мультимедиа и даже с 3D-печатью, к которым «традиционные» связисты или какие-нибудь выделенные «мультимедийные сети» не имеют практически никакого отношения. Согласитесь, никогда прежде Сеть не материализовывала столько ИКТ-сервисов и даже реальных предметов на основе их 3D-моделей. Уже не только телеком, а вся мировая промышленность собирается модернизироваться до уровня 3D-производства, в основе которого будет лежать IoE. И в этом нет ничего удивительного – просто в очередной раз количество переходит в качество. Потребителю же, как и всегда, важен результат сервиса и его цена, а не его технология.

Как говорил Станислав Ежи Лец, «нехорошо подзревать, когда вполне уверен». И мы должны заранее подготовиться к очередному сдвигу парадигмы, после которого понятие «телеком» может вообще выйти из употребления (вернее, какое-то время перед забвением оно будет обретаться в нишах, как сегодня TDM), трансформировавшись в единый и глобальный «инфоком» или просто в IoE с незатейливым сервисом «ИКТ как услуга». И телефония будущего окончательно превратится в одно из интернет-приложений. Лишь бы сам IoE не исчез однажды...



Конечно, мы нарисовали идеальную картину, и ее скорректирует реальная жизнь, в которой не всегда всё получается и которой не все будут удовлетворены. Но предупрежден – значит вооружен. Правда, как говорил Оскар Уайльд, «в жизни возможны только две трагедии: первая – получить то, о чем мечтаешь, вторая – не получить». Этим будущее и интересно, не правда ли? **ИКС**

Базаданныхмания

Нас решили пересчитать, рубрицировать и систематизировать. Разложить по таблицам, полям и записям. Чтобы было о каждом все учтено и записано. Причем на каждую отдельную базу данных есть разумное и убедительное обоснование.



Михаил
ЕМЕЛЬЯНОВ,
консалтинговое
агентство
«Емельяников,
Попова и партнеры»

ФМС совместно с Росфинмониторингом подготовило законопроект, в соответствии с которым предполагается создать единую базу данных граждан, содержащую, помимо фамилии, имени и отчества, данные о регистрации и месте пребывания, паспортные данные (если гражданину меньше 14 лет – реквизиты свидетельства о рождении и (внимание!) если гражданин умер – данные свидетельства о смерти), номер индивидуального лицевого счета в системе обязательного пенсионного страхования и ин-

формацию о судимости. Особенно радует последнее. Обосновывается тем, что отбывание наказания предполагает снятие с регистрационного учета.

Законопроект возлагает на ФМС обязанность вести адресно-справочную работу по предоставлению информации о регистрации граждан по месту пребывания и по месту жительства. В открытом доступе законопроекта пока нет. Остается только догадываться, кому и как такая информация будет предоставляться. Среди просочившихся сведений – наличие доступа к этой базе у банков, которые давно добиваются такой возможности.

Возможно существенное расширение круга сведений, включаемых в кредитные истории, а также источников их пополнения. Минэкономразвития опубликовало финальную версию изменений в закон «О кредитных историях», которая предусматривает введение обязанности передавать данные хотя бы в одно бюро кредитных историй (БКИ) для микрофинансовых организаций, коллекторов, приобретших долги, конкурсных управляющих при банкротстве кредитора. Право передавать данные в бюро получают любые лица, долг перед которыми подтвержден решением суда, а также кредитные кооперативы. Закон вводит обязанность передачи в БКИ сведений о кредитах и долгах индивидуальных предпринимателей и юрлиц вообще без их согласия. Граждане пока устояли. Но это уже пустая формальность – попробуйте получить кредит без согласия на доступ к кредитной истории.

Руслан Гаттаров, глава комиссии Совета Федерации по развитию информационного общества, предлагает создать в России... естественно, единую базу данных.

На этот раз – по запросам ведомств в отношении персональных данных граждан, что «позволит избежать злоупотреблений при использовании персональных данных россиян». Сенатор высказал предположение, что доступ к ней субъекты могли бы получить через личный кабинет на портале госуслуг. Главная проблема при создании такой базы – чтобы «подобная информация не мешала оперативно-розыскной деятельности».

Минздрав создает базу данных историй болезни с «ограниченным доступом пациентов» через интернет. ФСИН ведет базу дактилоскопических данных адвокатов, и при отказе адвоката предоставить пальчики администрация следственных изоляторов препятствует встрече с подзащитными.

Для обеспечения возможности перехода от одного оператора сотовой связи к другому с сохранением номера создадут единую базу этих самых номеров. Ну а чтобы работа зря не пропала и был какой-никакой задел на будущее, базу создадут с небольшим запасом. Как сообщается, задачей оператора базы данных будет не только перенос номера, но и предоставление запрашиваемой информации как абонентам и операторам связи, так и опять-таки банкам и платежным системам. Общее количество запросов может достигать нескольких миллиардов в день. Довольно неожиданно. Банки, платежные системы...

Глава удостоверяющего центра оператора Yota предложил Дмитрию Медведеву повсеместно внедрить сим-карты с поддержкой электронной подписи и, конечно же, данные обо всех сим-картах гражданина хранить в единой базе данных идентификации.

Уже вижу вопросы: «А что, вы против? Порядка, честности, доступности и т.д.?».

Нет, я за. Но у меня есть условие. Как у субъекта и гражданина. Тот, кто решил эти базы создавать, должен сделать так, чтобы ими не торговали. А если они попадут в продажу – так, чтобы виновные сидели в тюрьме, а организации, этими данными владевшие (а, возможно, и их защищавшие), оказались банкротами или были расформированы.

И напоследок: «Национальная служба розыска», безуспешно судившаяся со своим бывшим сотрудником, который рассказал о методах работы коллекторов правоохранительным органам, активно использовала в своей деятельности базы данных. Перечисляю названия: «Магистраль», «Поток», «Розыск», ЗИЦ, ЦАБ ГУВД Москвы. Вы не знаете, чьи это базы и где коллекторы их взяли? А теперь добавьте к ним все упомянутые выше. И представьте, что они есть не только у коллекторов. Я думаю, богатого воображения для этого не надо.

Мобильная защита для начинающих

Перед любой компанией рано или поздно встает вопрос: не пора ли организовать мобильный удаленный доступ к корпоративным ресурсам? Но как это сделать, не поставив под угрозу бизнес-интересы предприятия?



**Виктория
НОСОВА,**

консультант по
безопасности,
Check Point Software
Technologies

Причины, по которым компании организуют удаленный доступ к своим информационным ресурсам, могут быть разными. В одних компаниях много сотрудников, которые постоянно находятся вне офиса, но должны читать почту и обращаться к определенным данным. Другие открывают доступ к внутренним ресурсам своим системным администраторам. У третьих в штате есть сотрудники, работающие на дому.

Немалое число крупных коммерческих компаний уже предоставляют удаленное подключение своим работникам. Найти подходящее для себя решение удастся и банкам, хотя требования к такой системе у них значительно более строгие. Компании сектора SMB тоже могут выбрать недорогое и подходящее по производительности устройство, на котором, помимо брандмауэра и системы обнаружения и предотвращения атак, будет активирована возможность защищенного удаленного доступа. Сложнее с государственными компаниями: применяемые ими решения должны соответствовать требованиям регуляторов.

Личное или корпоративное

Возможность следовать принципу BYOD (Bring Your Own Device, «принеси свое устройство») зависит как от специфики предприятия, так и от типа мобильного устройства. Если компания решила подключить к своим корпоративным ресурсам смартфоны, то при применении защищенного контейнера особой разницы между личными и корпоративными устройствами нет. В обоих случаях корпоративные данные изолируются от личных, и можно не опасаться утечки или компрометации конфиденциальной информации. Однако госструктуры могут столкнуться с трудностями при описании доверенной среды на смартфоне работника (как, впрочем, и на ноутбуке). Тем не менее в некоторых российских государственных компаниях доступ к корпоративным данным с личных смартфонов уже разрешен. Использование личных смартфонов в финансовых организаци-

ях тоже пока ограничено, поскольку утечка хранящихся у них данных может иметь достаточно серьезные последствия.

Если речь идет о ноутбуке, то обеспечить должный уровень защиты несколько сложнее. Существуют решения, поддерживающие разные политики в зависимости от того, к какой сети подключен ноутбук – домашней или корпоративной. Также можно настроить проверку актуальности баз сигнатур антивирусного ПО, установленного на ноутбуке. Если базы не прошли проверку, то с помощью персонального брандмауэра ко всем ресурсам, кроме ресурса, с которого можно загрузить новые базы, доступ блокируется. После обновления доступ будет открыт. Конечно, на ноутбуке должен быть установлен централизованно управляемый агент, который имеет встроенный персональный брандмауэр, антивирус, функционал шифрования жестких дисков и контроля портов, а не только VPN-клиент для создания защищенного туннеля до VPN-шлюза компании. Если же вы хотите, чтобы на мобильном компьютере сотрудника не оставалось корпоративных файлов, можно воспользоваться зашифрованными USB-носителями, которые запускают защищенный рабочий стол, запрещая перемещение файлов между этим столом и хостом. Для многих компаний такие продукты решают задачу. В финансовых и государственных организациях использование личных ноутбуков сильно ограничено.

Как защитить корпоративную информацию

Наиболее эффективный механизм защиты корпоративной информации на мобильных устройствах – выделение корпоративных данных в защищенный контейнер, обеспечивающий изоляцию корпоративных данных от остальных данных и программ. Пользователь не сможет размещать корпоративные файлы на различных веб-сервисах, таких как Evernote, или в облачных хранилищах данных, например iCloud или Dropbox.

Изыюминка такого подхода состоит в том, что эти ограничения не действуют в отношении личных файлов. Пользователь волен делать со своими документами или фотографиями все что угодно, запускать на своем устройстве любые программы. Этим-то и отличается защищенный контейнер от решений класса Mobile Device Management, которые устанавливают ограничения в рамках всего устройства, не делая различий между корпоративными и личными данными. Такая политика, как правило, приводит к тому, что пользователи начинают изощряться в попытках обмануть систему. Применение же защищенного контейнера снижает риск возникновения подобной инициативы, поскольку для своих личных файлов пользователь может в полной мере задействовать функции, ради которых он приобретал данное мобильное устройство.

Для доступа к самим корпоративным ресурсам необходима двухфакторная аутентификация – сложный пароль (удобнее всего использовать пароль от учетной записи в Active Directory) и сертификат. Сертификат должен быть привязан не только к устройству, но и к пользователю, чтобы с данного устройства мог подклю-

читься к корпоративным ресурсам только тот пользователь, для которого генерировался сертификат.

Достаточно часто пользователи не ставят пароль на все устройство. Чтобы в случае утери такого устройства с корпоративными данными ничего страшного не произошло, всякий раз, когда пользователь открывает защищенный контейнер, устройство должно запрашивать некий PIN-код. Причем весьма желательно, чтобы он был не короче шести символов и состоял не только из цифр. Если злоумышленник найдет такой незащищенный телефон, то прежде чем он сможет получить доступ к корпоративным данным, ему нужно будет подобрать PIN на вход в защищенный контейнер, а пока он это делает, пользователь сообщит администратору о потере своего устройства, тот в два клика отзовет сертификат устройства и прочитает корпоративную почту будет невозможно даже после подбора PIN-кода. Сегодня такой подход должен являться «классикой жанра».

Остальные механизмы, конечно, также могут применяться, но не стоит забывать о том, что необходимо выбрать тот уровень защиты, при котором затраты, угроза взлома и размер возможного ущерба будут приемлемыми.

5 правил внедрения

1 Подойдите к задаче комплексно. Не стоит сначала выбирать решение для подключения смартфонов, внедрять его и настраивать, а потом думать, как защищать удаленный доступ. Неудивительно, если в таком случае получится зоопарк из продуктов, которые работают друг с другом с трудом.

2 Изучите все актуальные на данный момент технологии, взвесьте все за и против. Возможно, вам и не нужно все из того, что есть на рынке.

3 Проанализируйте предлагаемые решения. Возможно, вместо пяти продуктов от разных вендоров вы найдете два-три решения, покрывающие ваши задачи. А может быть, вам повезет, и все ваши потребности удастся охватить одним продуктом.

4 Определитесь с поддерживаемыми операционными системами мобильных устройств. Допустим, у вас 64% смартфонов с операционной системой А, 32% с операционной системой В и всего 4% с операционной системой С (дабы не обидеть вендоров, назовем их так). Если вы можете выбрать одно решение, обеспечивающее подключение и защиту доступа к корпоративным ресурсам с мобильных устройств, которые работают под А и В, то, может быть, просто отказаться от поддержки смартфонов с операционной системой С? Сложно найти решение, которое удобно и полноценно управляло бы любыми мобильными устройствами.

5 Проведите пилотный проект. Создайте тестовую зону, максимально приближенную к «боевой», и протестируйте выбранные решения вместе. Проверьте работу тестируемых решений с уже имеющимися у вас системами – с Active Directory, веб-порталами, серверами электронной почты и т.п. Привлеките к пилотным проектам специалистов вендора или компаний-интеграторов, имеющих опыт внедрения выбранных продуктов.

В любом случае разумный и взвешенный подход поможет вам создать интегрированную систему защиты мобильной среды с централизованным управлением, которая задействует небольшое количество ресурсов.

Человеческий фактор

К сожалению, приходится признать, что уровень осведомленности пользователей корпоративных приложений о безопасности мобильных устройств низкий. Многие до сих пор считают, что для смартфонов нет вирусов и других вредоносных программ; при утере смартфона их больше волнует замена устройства, чем возможная уязвимость корпоративных данных. Пользователи продолжают размещать в облачном хранилище данных файлы с пометкой «конфиденциально» для того, чтобы перекинуть их с корпоративного компьютера или телефона на домашнее устройство, и при этом они думают, что ничего непозволительного не совершают, поскольку этот файл никому, кроме них, не нужен.

Тем не менее никто, как правило, не информирует сотрудников о том, какие корпоративные данные являются конфиденциальными. Однако глупо скрывать от сотрудников вашу политику безопасности – ведь они должны ей следовать. Пользователи должны понимать, разглашение каких данных может поставить бизнес компании под угрозу. Поэтому каждый сотрудник должен знать, для чего на его мобильном устройстве установлены те или иные приложения и как ими правильно пользоваться. ИТ-служба должна не просто ограничить доступ к «интересным» ресурсам, а еще и объяснить, почему доступ к данным ресурсам запрещен, чем они опасны для компании.

Проще всего доводить такую информацию до сотрудников посредством внутренних собраний или тренингов. А еще лучше не давать доступа к конфиденциальной информации, пока пользователь не пройдет некий тест. Успешное прохождение теста должно подтверждать, что пользователь усвоил политику безопасности, принятую в компании, и понимает, какие корпоративные данные надо беречь как зеницу ока, а также то, что не все приложения одинаково полезны. ИКС

Защита по-русски

Идею превентивной защиты данных можно реализовать только «снизу», когда предустановленные средства безопасности становятся частью функциональности аппаратной платформы, уверен Ренат ЮСУПОВ, старший вице-президент Kraftway.



Ренат ЮСУПОВ

– Сегодня проблема безопасности корпоративной мобильной среды актуальна для многих компаний. Насколько, на ваш взгляд, реально создать действительно защищенные мобильные устройства?

– Мы считаем, что для защиты могут быть использованы аппаратные средства самой платформы. Надо лишь добавить

программный стек, который позволит отделить операционную среду на уровне базовой системы ввода-вывода от операционной системы для пользовательских приложений, и наполнить эту среду средствами защиты информации – антивирусами, модулями идентификации, аутентификации, межсетевыми экранами, средствами защиты доверенных сеансов и проч. Это и будет оболочка безопасности, унифицированная для интеграции в любой BIOS. Раньше такую оболочку мы устанавливали на десктопы, потом на тонкие клиенты, а в нынешнем году обеспечили ее переносимость и на мобильные устройства, в ближайшей перспективе она будет перенесена на серверы. Мы с самого начала планировали обеспечить переносимость оболочки на разные платформы, но несколько лет назад не было ясно, смогут ли мобильные устройства работать по тем же принципам, что и ПК. Оказалось, могут.

Универсальная стандартизованная оболочка позволит по единым правилам защищать весь спектр устройств от большинства угроз, за исключением самых низкоуровневых, где обходной путь заложен непосредственно в микросхемах и программно выловить его практически невозможно (но это уже риски компании-производителя: если она будет уличена в подобных действиях, то вряд ли удержится на рынке).

Конечно, мы не в состоянии угнаться за всем количеством ноутбуков и планшетов, которые производятся в Юго-Восточной Азии, но научились по желанию заказчиков оперативно встраивать в эти устройства нашу оболочку. Уже есть ноутбуки, моноблоки зарубежных производителей с оболочкой безопасности, в которую интегрированы российские средства защиты информации. В ближайшее время должны появиться и планшеты.

– Как эта работа соотносится с общемировым трендом превентивной защиты от угроз?

– В текущем году в мире информационной безопасности произошли два важных события. В октябре в

рамках обновления Windows 8.1 идеолог концепции цепочек доверия компания Microsoft запустила режим безопасной загрузки Secure Boot, когда до старта проверяются сертификаты приложений и устройств. В режиме Secure Boot менеджер загрузки UEFI выполняет только подписанный код. На мой взгляд, у Secure Boot на территории России мало перспектив из-за проблем с сертификацией зарубежных средств защиты и сложностей с ввозом криптографических модулей. Встроенные средства шифрования ориентированы на зарубежные стандарты и не поддерживают требования российских регуляторов.

Другую модель безопасности в сентябре этого года анонсировала Intel: перед запуском ОС запускается программный агент, который контролирует происходящие затем процессы. Примерно такой же принцип мы реализовали в нашей оболочке безопасности, но сделали это несколько раньше.

– А саму оболочку не нужно защитить? Например, запатентовать?

– За последний год мы получили около 12 патентов. Забавно, но во многих патентах, а проверялись они в российской и американской патентных системах, мы в некоторых областях обогнали коллег из Microsoft и Intel. При этом в нашей оболочке безопасности со встроенными российскими средствами защиты и режим Secure Boot поддерживается, и на ключах, выработанных по ГОСТу, реализуется стандарт TPM (Trusted Platform Module – криптопроцессор, вырабатывающий криптографические ключи и обеспечивающий защищенное хранение цифровых сертификатов), на который ориентированы многие зарубежные банковские системы.

Другое дело, что получать патент надо в каждой стране, где хочешь продавать свое решение. Однако зарубежные производители устройств с нашей оболочкой безопасности заинтересованы в их продвижении на рынки, где не работают американские стандарты защиты информации, – в Бразилию, Индию, СНГ. Со своей стороны мы готовы предлагать лицензии.

– Вы считаете, средства защиты должны стать частью функциональности платформы?

– Да, они должны быть не наложенными, а предустановленными. Потом методом лицензирования их можно активировать поочередно или все сразу, причем со 100%-ной гарантией совместимости. Мы открыли интерфейс оболочки безопасности для разработчиков программных средств защиты и работаем уже с десятком компаний. Думаю, к середине следующего года все устройства нашего собственного производства (серверы, десктопы, ноутбуки, планшеты) будут выходить со встроенными неактивированными средствами защиты.

Беседовала **Лилия ПАВЛОВА**

72 Е. ВОЛЫНКИНА. Цодопроектирование и цодостроительство: конец вечных вопросов

77 М. БАЛКАРОВ. Liebert PDX: и инновации, и традиции

78 В тренде – комплексные решения для ЦОДов

80 А. ПАВЛОВ, Д. БАСИСТЫЙ. Выбираем площадку для ЦОДа. Правила и риски. Ч. 1

84 И. ГРАНКОВ. Ситуация под контролем

88 Я. ГОРОДЕЦКИЙ. SDN: прорывная технология или маркетинговый пузырь?

90 А. СЕМЕНОВ. Оборудование интерактивного управления: расширение функциональных возможностей

93 Новые продукты

ЦОД проектирование и ЦОД строительство

конец
вечных
вопросов



↑
Евгения ВОЛЫНКИНА

или поздно встает перед многими компаниями. Но прежде чем определиться с его характеристиками, каждая компания должна решить, зачем ей вообще нужен дата-центр. Директор департамента системной интеграции «Инлайн Групп» Андрей Кондратьев отмечает, что соображения, подталкивающие компании к созданию собственного ЦОДа (основного или резервного) или к аренде мощностей коммерческого ЦОДа (опять же для использования в качестве основного или резервного), могут быть самыми разными: необходимость повысить производительность ИТ-инфраструктуры, ее масштабируемость, надежность ее работы и доступность приложений; стремление к централизации данных, снижению затрат на ИТ, минимизации рисков простоя и потери данных, обеспечению мобильности бизнеса и непрерывности бизнес-процессов и даже ускорение доставки отчетов высшему руководству компании. Причем надо отдавать себе отчет в том, что некоторые из этих задач являются взаимоисключающими: повышение производительности ИТ-инфраструктуры и надежности ее работы потребует определенных инвестиций (иногда немалых), что слабо сочетается со снижением затрат на ИТ (во всяком случае в краткосрочной перспективе), а минимизация рисков потери данных противоречит их централизации (все яйца оказываются в одной корзине). Чтобы максимально полно удовлетворить потребности и пожелания бизнеса, мало правильно ответить на вопрос «зачем вам дата-центр», нужно еще и расставить приоритеты: что важнее – надежность, экономия, непрерывность бизнеса, информационная безопасность и т.п.

Быть или не быть?

По-прежнему актуальным для многих компаний остается почти гамлетовский вопрос «строить или арендовать?», которому «ИКС» посвятил тему номера еще в 2009 г. За прошедшие годы поиск ответа на него легче не стал: новые технологии для инженерной и ИТ-инфраструктуры, виртуализация, облака, меняющиеся требования к информационной безопасности, про-

Дистанция между появлением у компании мысли о ЦОДе и ее практическим воплощением может быть и спринтерской, и марафонской. О том, как ее преодолеть с минимальными затратами, говорили участники 8-й международной конференции «ЦОД-2013», организованной журналом «ИКС».

Зачем и почему?

Вопрос о дата-центре, собственном или аутсорсинговом, рано или поздно встает перед многими компаниями. Но прежде чем определиться с его характеристиками, каждая компания должна решить, зачем ей вообще нужен дата-центр. Директор департамента системной интеграции «Инлайн Групп» Андрей Кондратьев отмечает, что соображения, подталкивающие компании к созданию собственного ЦОДа (основного или резервного) или к аренде мощностей коммерческого ЦОДа (опять же для использования в качестве основного или резервного), могут быть самыми разными: необходимость повысить производительность ИТ-инфраструктуры, ее масштабируемость, надежность ее работы и доступность приложений; стремление к централизации данных, снижению затрат на ИТ, минимизации рисков простоя и потери данных, обеспечению мобильности бизнеса и непрерывности бизнес-процессов и даже ускорение доставки отчетов высшему руководству компании. Причем надо отдавать себе отчет в том, что некоторые из этих задач являются взаимоисключающими: повышение производительности ИТ-инфраструктуры и надежности ее работы потребует определенных инвестиций (иногда немалых), что слабо сочетается со снижением затрат на ИТ (во всяком случае в краткосрочной перспективе), а минимизация рисков потери данных противоречит их централизации (все яйца оказываются в одной корзине). Чтобы максимально полно удовлетворить потребности и пожелания бизнеса, мало правильно ответить на вопрос «зачем вам дата-центр», нужно еще и расставить приоритеты: что важнее – надежность, экономия, непрерывность бизнеса, информационная безопасность и т.п.

блемы с электричеством и ситуация на рынке недвижимости добавляют «гири» и «гирьки» на обе чаши весов, к тому же масса этих «гирек» заметно меняется в зависимости от конкретных условий. Причем это тот случай, когда иностранный опыт практически неприменим, там цифры совсем другие. Сложность выбора директор проекта ЕРЦОД «Ростелекома» Александр Мартынюк показал на примере, который на первый взгляд кажется простым: нужно разместить 200 стоек с ИТ-нагрузкой мощностью 5 кВт на стойку в дата-центре уровня Tier III, PUE = 1,5, стоимость электричества – 3,6 руб./кВт·ч, горизонт планирования – 10 лет. Выбор сильно зависит от принимаемых во внимание условий, конфигурации ЦОДа и ИТ-инфраструктуры, использования или неиспользования тех или иных облачных сервисов. Прежде всего единым дополнительным общероссийским условием является практическое отсутствие возможности строительства ЦОДа «с нуля» (во всяком случае в Москве и ближайших окрестностях), что обычно обходится дешевле встраивания его в имеющееся здание. А еще надо учесть российские кредитные банковские ставки (как минимум 12% в год), соображения информационной безопасности, и наконец, стремление некоторых компаний к наращиванию капитализации, от которой напрямую зависят бонусы топ-менеджеров. Последнее не оставляет никаких шансов модели услуг коммерческих ЦОДов, несмотря на возможность бы-



стро начать пользоваться ИТ-сервисами и гораздо более низкий уровень стартовых инвестиций. По идее грамотное использование облачных технологий резко повышает экономическую привлекательность строительства собственного дата-центра при нынешних ценах на аренду виртуальных машин в коммерческих ЦОДах, но сэкономить таким способом могут только крупные компании, потребляющие большие объемы подобных сервисов. Для компаний класса SMB с 30 сотрудниками и стандартным набором бизнес-приложений (бухгалтерия, электронная почта, склад, CRM и т.п.) использование в течение года сервисов IaaS и SaaS облачных провайдеров обойдется почти вдвое дешевле создания собственного мини-ЦОДа. В общем, для российского SMB-сектора, в котором довольно трудно найти компанию, всерьез планирующую свое развитие на 10 лет, вопрос «строить или арендовать» давно решен в пользу ИТ-аутсорсинга, а для «крупняка» пока более выгодны инвестиции в CAPEX.

К «истокам»

Как это делать по всем правилам, у нас давно знают – в соответствии со стандартами всем в цодостроительных кругах известной организации Uptime Institute, деятельность которой уже обросла многочисленными мифами. Развенчать их пытался управляющий директор российского отделения Uptime Institute Алексей Солодовников, отметивший прежде всего, что публика склонна сильно завышать возраст стандартов Uptime, намекая на их устарелость и неадекватность современным реалиям: «Приходилось даже слышать, что Uptime Institute существовал еще во времена строительства Днепрогэса». Кроме того, некоторые почему-то считают, что уровни надежности Tier Uptime совпадают с соответствующими уровнями стандарта ТИА-942, тогда как общее у них только слово «Tier». Как напомнил А. Солодовников, первая редакция стандарта, касающегося уровней надежности Tier, была опубликована не так уж давно – в 1996 г., а в 2008 г. она претерпела полную ревизию. Именно тогда из стандарта была убрана все схемы и таблица с конкретными характеристиками дата-центров различных уровней Tier, такими как размещение в отдельном здании с такой-то толщиной стен и с машинными залами с такой-то высотой фальш-полов, наличие двух вводов электроснабжения от внешних сетей для Tier IV, определенный уровень резервирования того или иного инженерного оборудования и т.д. Несмотря на прямое указание в сопровождающем тексте, что это не требования, а просто типичные параметры реальных дата-центров, построенных в соответствии со стандартом, очень многие воспринимали их именно как обязательные к исполнению. После ревизии изменился и механизм внесения изменений в стандарт – теперь это делается после голосования членов сообщества Uptime Institute Network, объединяющего владельцев дата-центров (в их число входят DataSpace и Сбербанк).

Известная сертификация проектов дата-центров и готовых площадок тоже началась после ревизии, а



именно в 2009 г. В тот год сертификаты разных уровней Tier получили 10 проектов и всего одна площадка из шести стран. С тех пор популярность этой процедуры заметно выросла, и количественно и географически: в 2010 г. ее прошли 26 проектов (в том числе первый в России) и 4 площадки из 12 стран, в 2011 г. – 38 проектов и 9 площадок из 18 стран, в 2012 г. – 68 проектов и 26 площадок, а за неполный 2013 г. – 71 проект и 23 площадки разных уровней, от Tier II до Tier IV. Так что на сегодняшний день сертифицировано более 200 проектов и еще 180 находятся в работе, а всем, кто только собирается подавать документы на сертификацию, рекомендуется во избежание недоразумений и мифов читать первоисточники на сайте Uptime Institute и консультироваться у сертифицированных проектировщиков ATD (Accredited Tier Designer) и специалистов ATS (Accredited Tier Specialist), благо их в России уже в общей сложности 85 человек.

Исключения и правила

Как уже было сказано, в российских реалиях строительство дата-центра в чистом поле является скорее исключением, чем правилом. Подавляющему большинству потенциальных заказчиков придется иметь дело с размещением ЦОДа в готовом – и зачастую довольно старом – здании, которое в случае крупного дата-центра, скорее всего, придется перестраивать (под небольшой ЦОД можно без особых проблем переоборудовать помещение и в стандартном офисном центре). Как рассказал главный инженер проекта ADM Partnership Александр Овчинников, строительство ЦОДа с подведенной мощностью от 10 МВА в черте крупного города – это практически всегда демонтаж или реконструкция старого здания. Оптимальный вариант – здание бывшего завода: в этом случае на участке обычно наличествует хорошо развитая инфраструктура, конструкции здания имеют достаточную несущую способность, есть довольно большая территория между корпусами, где можно разместить некоторые инженерные решения, в ближайших окрестностях нет жилых домов, что означает отсутствие жестких требований к шуму и выхлопам дизель-генераторных уста-

новок, а транспортная доступность для персонала при этом сохраняется. Но в любом случае необходим технический аудит площадки под ЦОД – с обследованием фундаментов, колонн, перекрытий и кровли и оценкой затрат на реконструкцию. Кроме того, необходимо провести градостроительную оценку территории (если согласно генплану в обозримом будущем по соседству будут построены жилые дома, то нужно уже сейчас готовиться к проблемам), обмерить помещения (даже если документация сохранилась, расхождения между бумагой и реальностью у нас обычное дело), выполнить аудит инженерных систем и т.д., и т.п. И если очень повезет, то может оказаться, что реконструкция выбранного помещения обойдется гораздо дешевле нового строительства, и эта реконструкция ничуть не помешает при соответствующем уровне проектирования и строительства получить сертификаты Uptime Institute и на проект, и на готовую площадку.



В помощь заказчику

Но должным образом организовать проектирование и строительство ЦОДа очень непросто. Оптимальные модели этого процесса обсуждаются на отраслевых мероприятиях уже не первый год. Долгое время российские заказчики считали лишним звеном консультантов, но это заблуждение пару лет назад наконец-то ушло в прошлое. В необходимости привлечения профессиональной проектной компании у заказчиков теперь тоже сомнений нет. Что же касается общей конфигурации потенциальных участников проекта, то директор по проектированию группы компаний ALTIUS Евгений Ломов предлагает три возможные схемы проектирования и строительства ЦОДа. Первая, которая на сегодняшний день считается традиционной, предусматривает разработку консультантом технического задания (ТЗ) на проектирование, сдачу его заказчику, который, в свою очередь, передает ТЗ выбранному генеральному подрядчику, после чего генподрядчик выбирает генерального проектировщика и управляет всем процессом создания ЦОДа, от проектирования до построения. Плохо в этой схеме то, что генподрядчик получает слишком много полномочий и может воспользоваться ими в ущерб интересам заказчика.

Вторая схема с теми же участниками предполагает выбор заказчиком и генпроектировщика и генподрядчика и активное участие заказчика во всем процессе, в частности, в получении правоустанавливающих документов и исходно-разрешительной документации. Схема всем хороша, но требует от заказчика достаточно глубоких знаний в области проектирования и строительства дата-центров и возлагает на него массу хлопот, не говоря уж об ответственности за соблюдение сроков и бюджета проекта. Если же глубокие знания и опыт заказчика еще только предстоит получить, то, по мнению Е. Ломова, лучше работать по третьей схеме, в которой реализуется гибрид технического заказчика и генпроектировщика. В этой схеме нет генподрядчика, а есть подрядчики для разных этапов работ, которых выбирает сам заказчик; контролирует же весь процесс управляющая компания, выступающая в роли технического заказчика. Такая схема позволяет заказчику избежать лишних затрат и страхует от попыток подрядчиков сократить свои издержки в ущерб заказчику, используя более дешевые, а значит, менее надежные решения.

О необходимости ввести в процесс проектирования и строительства ЦОДа технического заказчика говорит и технический директор центра инженерных систем IBS Константин Зиновьев. Технический заказчик должен обладать достаточными компетенциями, чтобы выступать в качестве «переводчика» с технического языка на финансовый и обратно между инвестором, заказчиком и проектировщиком. Тогда он сможет избавить заказчика от общения с многочисленными подразделениями проектировщика, с техническими специалистами поставщиков оборудования и с внешней экспертизой, что не только ускорит принятие и технических, и финансовых решений, влияющих на скорость проектирования и строительства, но и повысит качество проектирования. Технический заказчик должен стать координирующим центром всех работ по проекту, сохраняющим нужный баланс между всеми участниками. В частности, он не позволит строителям перетянуть одеяло на себя, поскольку на стоимость строительства с подводом коммуникаций в общем бюджете, включающем расходы на создание ЦОДа и стоимость владения им в течение 10 лет, придется около 10%. В идеале участие грамотного технического заказчика позволяет сэкономить на оптимизации проектных решений до 30% от капитальных затрат на строительство дата-центра при сохранении высокого качества общего решения. Причем, по подсчетам IBS, для дата-центра с 300 стойками средней мощностью 7 кВт от выбора первоначальных проектных решений (и значит, от проектной команды) зависит более 80% общей стоимости владения ЦОДом в течение 10 лет.

Примерно такой ЦОД (на 300 стоек) для размещения вычислительных ресурсов правительства Москвы строила для ОАО «Электронная Москва» компания R-Style. Оказание электронных услуг населению требует бесперебойной работы информационных систем и, следовательно, надежной серверной и инженерной инфраструктуры. И при этом, как отметил директор департа-

мента инженерных систем и телекоммуникаций R-Style Вячеслав Тихонов, государственный заказчик, который наконец-то начал считать деньги, требует оптимизации издержек на размещение оборудования и его эксплуатацию. Характеристики ЦОДа, заявленные заказчиком, соответствуют довольно крупному по российским меркам проекту: общее энергопотребление 5–7 МВт, 200–300 серверных шкафов с тепловыделением от 5 до 15 кВт с возможностью организации в машинном зале высоконагруженных зон, надежность уровня Tier III, масштабируемость и этапность строительства (потому что у госзаказчика бюджеты часто планируются только на год вперед). Для пущей безопасности объекта подбирали отдельно стоящее здание. Кроме того, от здания требовалось расположение в границах Москвы (чтобы использовать административный ресурс для решения разных вопросов), достаточность энергетических мощностей (получение такого количества электричества даже с административным ресурсом – дело долгое и непростое), возможность реконструкции и наличие собственника, готового вкладываться в эту реконструкцию.

При выборе технологических решений для инженерной инфраструктуры создатели не слишком ориентировались на коэффициент энергоэффективности PUE, а ставили во главу угла низкие затраты на эксплуатацию, но при этом обращали внимание на экологичность, поскольку для правительства Москвы этот ЦОД должен выполнять еще и имиджевые функции. Так что в итоге в дата-центре были установлены динамические роторные ИБП, чиллеры с фрикулингом и рядные доводчики в закрытых холодных коридорах. Несмотря на то что первый этап строительства с заменой перекрытий, установкой всей инженерной инфраструктуры и оборудованием первого машинного зала на 40 стоек занял всего 9 месяцев, главной ошибкой создатели ЦОДа считают принятое решение реконструировать существующее здание, а не строить новое.

Модульность и мобильность

Совсем другая задача стояла перед компанией «Аэрофлот», которая решила построить свой резервный ЦОД. Как рассказал начальник отдела серверных комплексов департамента вычислительной инфраструктуры и телекоммуникаций «Аэрофлота» Алексей Быстров, коммерческого дата-центра с нужными характеристиками и гарантией последующего масштабирования арендованных стоек найти не удалось, поэтому поначалу решили разместиться в одном из собственных зданий. Однако оценка предстоящей модернизации помещения и реконструкции имеющихся инженерных систем показала, что это будет слишком долго и дорого, после чего возникла идея использования модульного ЦОДа. Для ее реализации в качестве подрядчика привлекли компанию «Техносерв», которая имеет опыт подобных проектов и несколько разработанных законченных решений для модульных дата-центров.

По словам главного специалиста отдела инженерных решений «Техносерв» Александра Переведенцева, модулем в данном случае является комплект из сервер-

ного блока, в который устанавливается активное оборудование, и инженерного блока, обеспечивающего жизнедеятельность этого оборудования. В проекте для «Аэрофлота» на площадке размером 25×30 м был построен двухэтажный комплекс, состоящий из четырех серверных блоков общей емкостью 56 стоек по 10 кВт каждая, четырех инженерных блоков, блока гарантированного электроснабжения, складского и диспетчерского блоков. Причем на возведение и запуск в эксплуатацию этого более чем полумегаваттного ЦОДа понадобилось всего 5,5 месяцев.

Но скорость возведения не единственное достоинство модульных дата-центров (а также их ближайших «родственников» – контейнерных ЦОДов). Они хороши еще и тем, что их сборка (или как минимум сборка составляющих их блоков) производится на заводе из стандартных конструкций, с соответствующим контролем качества, тестированием и отладкой, что, в свою очередь, сокращает время запуска ЦОДа в эксплуатацию на площадке заказчика. Модульные и контейнерные дата-центры компании Cannon недавно начала продвигать на российский рынок компания «Телеком-Монтаж». Они тоже разрабатываются по индивидуальным проектам, но на базе опробованных и протестированных серийных решений. Как отметил заместитель генерального директора «Телеком-Монтаж» Михаил Саликов, размеры такого модульного ЦОДа могут, в зависимости от потребностей заказчика, варьироваться в очень широких пределах – от 10 до 1000 кв. м, причем его конструкция предусматривает возможность расширения без остановки дата-центра, быструю разборку, переезд и сборку на новом месте. Поддерживается также функция удаленного мониторинга и управления работой ЦОДа. Поскольку устанавливается он на улице, то нет необходимости выделять место для инженерного и ИТ-оборудования внутри зданий, тратиться на переконфигурацию и отделку помещения, а также на согласование всех этих работ в разных инстанциях. Производитель также гарантирует низкие эксплуатационные расходы, устойчивость к взлому, защиту от проникновения воды и пыли. О качестве исполнения изделий от Cannon говорит хотя бы





то, что их крупными заказчиками являются структуры НАТО и министерство обороны Великобритании.

Продолжает совершенствоваться мобильные ЦОДы и российская компания TeleCore. В ее портфеле уже есть несколько типовых моделей мобильных дата-центров, построенных на базе стандартных 20- и 40-футовых контейнеров, в которых размещается от 5 до 10 стоек мощностью до 10 кВт на стойку. При этом каждый поставленный ЦОД «затачивался» под требования заказчиков по количеству серверных стоек, уровню резервирования инженерных систем и общей подводимой мощности. Последняя разработка TeleCore – мобильный дата-центр мощностью 110 кВт: в 40-футовом контейнере размещены 11 серверных стоек с энергопотреблением 10 кВт каждая. Для охлаждения в этом ЦОДе используются моноблочные прецизионные кондиционеры с режимом фрикулинга общей мощностью 116 кВт, которые вынесены на внешнюю стенку контейнера (по желанию заказчика кондиционеры могут комплектоваться пароувлажнителями). Мощность установленных ИБП составляет 160 кВт, уровень резервирования систем ИБП и кондиционирования – N+1. По словам коммерческого директора TeleCore Антона Лабышкина, пока 110 кВт – это максимальная полезная мощность для контейнеров таких габаритов, нарастить ее не позволяют параметры имеющихся на рынке кондиционеров, так что заказчику, которому требуется более мощное решение, придется увеличить количество контейнеров. Общий недостаток модульных ЦОДов по сравнению с традиционными стационарными – более высокая цена в расчете на одну серверную стойку, но зато их можно намного быстрее начать эксплуатировать. Например, ЦОД от TeleCore можно запустить в эксплуатацию на площадке заказчика уже через 4 месяца с момента начала проектирования, а при необходимости – без особых проблем перевезти на другое место. И таких ЦОДов в контейнерах разных размеров и разной комплектации стоит по стране уже больше 40 штук.

Переезды и катастрофы

Еще один немаловажный вид проектирования и строительства – проектирование переезда ЦОДа. В случае дата-центров это обычно означает не просто перевозку «мебели» в виде стоек с оборудованием, а переезд с минимальным прерыванием бизнес-процессов. Именно такой переезд пришлось пережить ЦОДу «Русславбанка». Как рассказал заместитель начальника управления информационно-технического обеспечения банка Алексей Бунто, при подготовке переезда офиса банка из одного здания в другое для дата-центра рассматривалось два варианта: создание серверной комнаты на новом месте и аренда коммерческого ЦОДа. Однако оказалось, что на серверное помещение в новом здании офиса могли выделить только 15 кВт электроэнергии, т.е. его пришлось бы строить отдельно, что означало последующие затраты на обслуживание и проблемы с расширением через несколько лет. Поэтому был выбран вариант размещения ИТ-инфраструктуры в коммерческом дата-центре и разработан план миграции

без остановки критических бизнес-процессов и с минимальным простоем остальных сервисов. Для организации переезда специально были куплены блейд-система, СХД, ленточная библиотека, сетевое оборудование и необходимое ПО, арендованы два гигабитных канала. Все это позволило, не трогаясь с места, перенести в коммерческий ЦОД все виртуальные машины и более 20 Тбайт данных. И лишь после перевода на новое место основных бизнес-приложений были проведены демонтаж, перевозка, установка в стойки и подключение к сети оставшегося оборудования.

Кроме того, в последнее время все больше компаний берутся за выполнение сходных с переездом операций при создании катастрофоустойчивых распределенных дата-центров – которые способны продолжать работу в ситуациях массового выхода оборудования из строя. Построение таких дата-центров при любой их конфигурации – дело очень недешевое, поэтому, как отмечает директор департамента главных инженеров проекта ГК «Компьюлинк» Руслан Усов, для реализации подобного проекта необходимо объяснить заказчику необходимость и экономическую обоснованность функционала катастрофоустойчивости в терминах непрерывности бизнеса. Создавая такой ЦОД, нужно понимать, что он должен поддерживать жизненный цикл управления непрерывностью, который состоит в периодическом повторении четырех ключевых процессов – подготовка к катастрофе, реагирование на нее, восстановление и совершенствование бизнес-процедур, направленных на обеспечение непрерывности бизнеса. При этом нужно найти баланс между затратами на поддержание катастрофоустойчивости и потерями бизнеса в случае катастрофы с учетом времени полного восстановления всех бизнес-процессов. В принципе ИТ-отрасль уже имеет весь инструментарий для построения катастрофоустойчивых систем с использованием технологий консолидации и виртуализации вычислительных ресурсов, кластерных систем, технологий удаленной репликации и непрерывной защиты данных, и заказчик может построить катастрофоустойчивый ЦОД либо самостоятельно на собственной ИТ-архитектуре, либо с использованием площадок коммерческих дата-центров и услуг облачных провайдеров.



По подсчетам аналитиков, российский рынок коммерческих дата-центров – один из самых быстрорастущих сегментов ИТ-рынка. По данным iKS-Consulting, в 2013 г. его объем увеличился на 28% и составил 9,1 млрд руб. Этот рынок тянет за собой и рынок проектирования и строительства дата-центров: в 2013 г. введено в строй 12 крупных и средних коммерческих площадок общей площадью машинных залов 5100 кв. м, а в 2014 г. ожидается сдача в эксплуатацию еще 10,5 тыс. кв. м. По площадям крупных ЦОДов нам пока далеко до мирового уровня, но радует, что рынок хорошо растет и на нем есть место и для «больших», и для «маленьких» – что и продемонстрировали участники конференции «ЦОД-2013». ИКС

Liebert® PDX

и инновации,
и традиции

Новая линейка прецизионных шкафных кондиционеров Liebert® PDX убедительно доказывает, что даже в традиционных задачах охлаждения помещений есть место для усовершенствований, которые выводят оборудование на уровень, соответствующий требованиям времени.

Технологии виртуализации существенно повышают эффективность использования ресурсов дата-центров за счет гибкого объединения разных приложений на одном сервере. Следующий шаг на этом пути – переход к облачным вычислительным системам, представляющим собой распределенные сети ресурсов и мощностей, масштабируемые по запросу. Однако с новыми технологиями вычислений помимо очевидных преимуществ сопряжены определенные проблемы. В частности, значительно возрастают требования к инженерному обеспечению ЦОДов.

В ответ на этот вызов компания Emerson Network Power вывела на рынок новую линейку фреоновых прецизионных шкафных кондиционеров Liebert® PDX. Эта линейка в очередной раз подтверждает лидирующие позиции компании в области систем охлаждения современной ИТ-инфраструктуры. Благодаря реализованным в ней инновационным решениям Liebert® PDX соответствует всем требованиям, предъявляемым сегодня к системам охлаждения:

- высокая энергоэффективность;
- уверенная работа при высокой плотности тепловыделения нагрузки в сочетании с системами контейнеризации воздушного потока;
- способность стабильно поддерживать работу при быстрых изменениях нагрузки.

В линейке Liebert® PDX используются высокоэффективные электрокоммутируемые вентиляторы, которые за счет изменения скорости вращения уменьшают расход электроэнергии и оптимизируют воздушный поток в соответствии с текущей нагрузкой. Новый дизайн и материалы лопастей позволяют подавать воздух максимально эффективно. Управление производительностью кондиционеров дает возможность снизить потребление электроэнергии, адаптироваться к текущему уровню на-

грузки, продолжить работу при временной перегрузке. В результате повышается как энергоэффективность, так и надежность системы в целом.

Liebert® PDX поддерживает увеличенные диапазоны допустимых температур как наружного воздуха, так и воздуха внутри помещения, что упрощает использование этих кондиционеров с современными системами контейнеризации коридоров, в частности со Smart Aisle™, оригинальным решением компании.

Как и в более ранних продуктах, в Liebert® PDX имеется штатная возможность установки пленума подмеса наружного воздуха, управляемого контроллером кондиционера. Благодаря этому, если допускают условия установки оборудования, можно использовать приточный воздух для частичного или полного «свободного охлаждения», не ухудшая параметров воздуха в помещении. Основное внимание при реализации этой опции уделено сохранению прецизионности кондиционера, то есть от ее задействования точность поддержания температурного и влажностного режима не страдают. Достигается это за счет наличия дополнительного датчика температуры и влажности подмешиваемого воздуха и управления регулируемыми клапанами, расположенными как на пути подмешиваемого воздуха, так и на пути воздуха, поступающего от оборудования. Допускаются разные варианты взаимного расположения путей подачи воздуха, что упрощает дизайн системы.

В зависимости от пожеланий заказчика для поддержания влажности в кондиционерах могут быть применены увлажнители всех основных технологий: и традиционные электродные, и инфракрасные, способные работать на воде с нестандартной проводимостью, и ультразвуковые, экономящие электроэнергию, но наиболее требовательные к качеству воды.



К удачным усовершенствованиям новых моделей относится и увеличенная допустимая длина фреоновых трасс, упрощающая их установку в стесненных условиях. А расширенный модельный ряд облегчает подбор оборудования для конкретной задачи.

Подобно другим продуктам компании, Liebert® PDX использует фреон R410A, не наносящий вреда экологии. Благодаря тому, что этот фреон высокоэффективен с точки зрения физического процесса охлаждения, появилась возможность уменьшить размеры шкафов, что также облегчает подбор и размещение оборудования.

Для построения отказоустойчивых систем будут полезны штатные опции двойного ввода и встроенного ИБП для контроллера.

Для управления, как и в других современных продуктах компании, используется хорошо зарекомендовавший себя оригинальный контроллер iCom, устанавливаемый в каждом кондиционере. Групповая работа, в наиболее подходящем для конкретной задачи варианте, обеспечивается простым объединением всех машин между собой по сети Ethernet. До 32 машин разных типов могут быть объединены в одну группу, к которой, в свою очередь, можно дополнительно подключить до 16 графических дисплеев. Этого с запасом хватит для сколь угодно сложной конфигурации управления.

Внешний мониторинг и управление доступны за счет возможности установки карт открытых протоколов, Web/SNMP, MODBUS и других.

Подготовил **Михаил БАЛКАРОВ**,
технический эксперт,
Emerson Network Power, ATD, CDCDP



www.emersonnetworkpower.eu

В тренде – комплексные решения для ЦОДов

В подостроении растет спрос на комплексные решения от поставщика, имеющего компетенции во всем спектре инженерных систем ЦОДа. Такой подход позволяет удовлетворить высокие требования заказчиков по надежности, масштабируемости, управляемости, энергоэффективности, удобству эксплуатации и срокам реализации проектов. Решения Rittal полностью подтверждают эту тенденцию.

Стойка TS-IT

Идеальная ИТ-стойка должна обеспечивать безопасную среду для серверов и другого оборудования, возможность модификации без больших затрат, удобный ввод и организацию кабелей, оптимальное соотношение цена/производительность. Стойка TS-IT, основывающаяся на всемирно известном каркасе Rittal TS 8, отвечает всем этим требованиям.

Заказчик может выбрать стойки разных размеров, с перфорированными дверями либо с обзорной дверью спереди и стальной сзади. Задние двери двустворчатые, что экономит пространство и облегчает доступ к оборудованию. Также имеются стойки со степенью защиты IP 55.

ность снятия показаний, универсальность и масштабируемость – вот главные критерии для выбора системы мониторинга. Система мониторинга CMC III от Rittal включает инновационные решения в сфере мониторинга ЦОДов, которые позволяют осуществлять непрерывный контроль жизненно важных функций дата-центра в режиме онлайн. Основной принцип действия прост: при помощи датчиков в серверных стойках и ЦОДе измеряются температура и влажность воздуха, скорость воздушного потока и другие параметры. Измеренные значения консолидируются и обрабатываются в центральном блоке системы. Доступ к ним пользователь может получить через веб-интерфейс. Также есть возможность интеграции в вышестоящие по иерархии системы управления ЦОДа

Rittal – The System.

Faster – better – worldwide.

Make IT easy.

RiMatrix S: стандартизированный и сертифицированный модульный ЦОД.

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

FRIEDHELM LOH GROUP

Каждая стойка оснащена двумя настраиваемыми 19-дюймовыми монтажными уровнями и составной крышей с оптимизированными щеточными кабельными вводами, расположенными параллельно боковым стенкам. Благодаря исключительно простой регулировке монтажных уровней, выполняющейся без применения инструментов, и компактным аксессуарам стойки можно легко адаптировать под индивидуальные требования. Аксессуары также можно добавлять или заменять без применения инструментов. Все металлические компоненты стойки электрически объединены, что гарантирует выравнивание потенциалов и надежное заземление. Имеется центральная точка заземления. Крыша уже подготовлена для установки панели вентиляторов.

Система мониторинга ЦОДа

Максимальная надежность, моментальная реакция системы, экономичность, простота запуска и обслуживания, высокая точ-

с помощью протокола SNMP, например в ПО Rittal RiZone. Генерация сигналов тревоги обеспечивает своевременное информирование администратора о выходе значений за допустимые пределы по e-mail или посредством SMS-сообщений.

Важнейшее нововведение – использование шины CAN-Bus (Controller Area Network). Эта шина поддерживается центральным процессорным блоком и интеллектуальными датчиками Rittal, применение переходных блоков не требуется. Датчики CAN-Bus подключаются к процессорному блоку последовательно: в каждой ИТ-стойке устанавливаются датчики CAN-Bus, которые соединяются шинным кабелем с датчиками в соседних шкафах. Поскольку датчики подключаются напрямую к процессорному блоку CMC III, снижается стоимость, обеспечиваются простота монтажа и обслуживания и масштабируемость системы в целом.

Rittal предлагает новое решение и в области датчиков: два важнейших – датчик температуры и инфракрасный датчик доступа для двери – интегрированы в стандартный процессорный блок. Добавлена визуализация состояния каждого датчика: его можно определить без доступа к веб-интерфейсу. При этом СМС III гибко расширяется по модульному принципу: доступны блок управления с восемью цифровыми входами и четырем релеиски выходами, счетчики расхода электроэнергии и датчики фиксации актов вандализма. К одному процессорному блоку можно подключить до 32 интеллектуальных датчиков. Кроме того, в СМС III появились две новые функции: датчик перепада давления, который контролирует степень изоляции холодного коридора ЦОДа, и поддержка счетчиков электроэнергии с выходом S₀Bus, что позволит определять энергопотребление отдельных устройств или стоек.

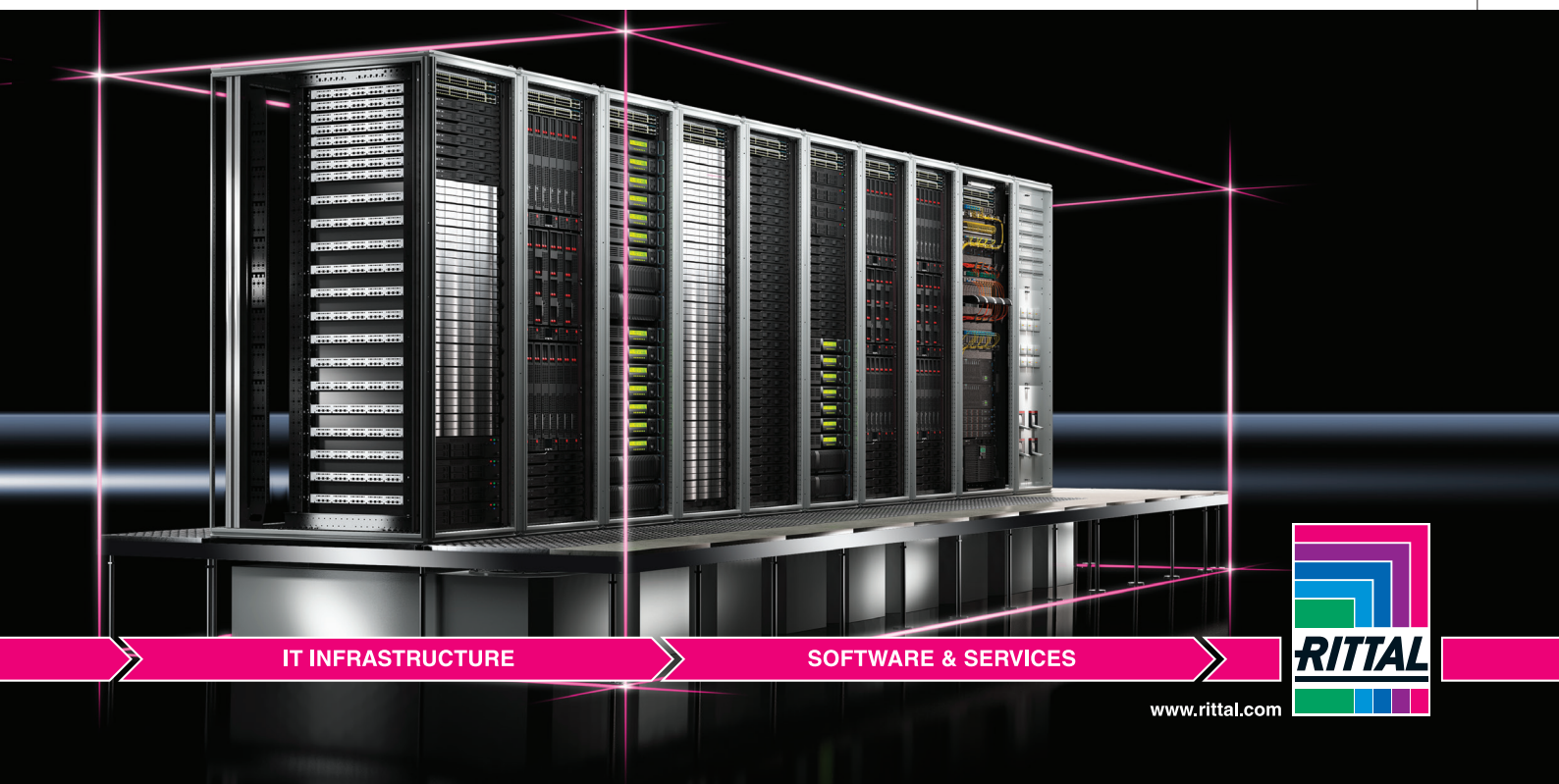
RiMatrix S – революция в построении ЦОДов

В последние годы Rittal активно развивает направление готовых комплексных решений для создания инженерной инфраструктуры ЦОДа. В рамках концепции выпускается целая серия интересных продуктов, рассчитанных на потребителей разного масштаба.

В нынешнем году компания Rittal на выставке «СвязьЭкспокомм» представила готовый модульный центр обработки дан-

повысить плотность монтажа серверных и сетевых компонентов, для RiMatrix S компания Rittal разработала новую систему контроля микроклимата, которая полностью размещается под фальшполом (система охлаждения по принципу Zero-U-Space Cooling-System, ZUCS). Воздухо-водяные теплообменники располагаются непосредственно под серверными стойками. Их вентиляторы подают воздух через перфорированную нижнюю панель в холодную зону перед стойками. Так как двери и боковые стенки серверных шкафов затруднили бы воздухообмен, в системе RiMatrix S применяются открытые стойки. Для эффективного разделения холодных и горячих потоков воздуха в стойках установлены изолирующие перегородки. Резервирование системы контроля микроклимата по схеме N + 1 обеспечивает высокую готовность.

Самый младший вариант ЦОДа RiMatrix S – Single 6 – это линейка из шести серверных стоек и одной дополнительной стойки для сетевого оборудования. Более крупный вариант ЦОДа Single 9 включает восемь серверных стоек и одну стойку для сетевого оборудования. Варианты Double 6 и Double 9 содержат удвоенное количество оборудования, которое располагается в две линейки. Существенная особенность системы – возможность комбинирования нескольких RiMatrix S для создания крупных ЦОДов: можно быстро и без проблем либо составить зеркальную конструкцию с общими зонами



IT INFRASTRUCTURE

SOFTWARE & SERVICES

www.rittal.com



ных – RiMatrix S, ставший стандартизированной компонентой ИТ-инфраструктуры Rittal. В решении RiMatrix S впервые в мире воплощена концепция стандартизированного оборудования ЦОДа. Если до сих пор центры обработки данных проектировались индивидуально для каждого заказчика с соответствующими затратами времени и средств, то модуль RiMatrix S позволяет создать весь ЦОД из оборудования под единым артикулом.

RiMatrix S представляет собой готовый центр обработки данных, включающий следующие стандартизированные компоненты: серверные и сетевые стойки TS-IT, системы распределения питания внутри стоек, управления микроклиматом и энергоснабжением, системы защиты от перенапряжений, а также средства мониторинга. Весь ЦОД целиком изолируется модульной оболочкой от объема основного помещения. Чтобы

холодного и горячего воздуха, либо выстроить модули в ряд. Модули RiMatrix S одинаково хорошо подходят для сооружения нового центра обработки данных в здании с дополнительным отделением коридоров или для установки вне здания в высоком контейнере. Наконец, эта мировая новинка от Rittal позволяет легко расширить существующий ЦОД, а также может использоваться в помещении повышенной безопасности.

ООО «Риттал»

125252, Москва, ул. Авиаконструктора
Микояна, 12, БЦ "Линкор", 4 этаж
тел. (495) 775-0230, факс (495) 775-0239
info@rittal.ru, www.rittal.ru

Выбираем площадку для ЦОДа

правила
и риски
Часть 1



Андрей ПАВЛОВ,
генеральный директор,
«Датадом»



Дмитрий БАСИСТЫЙ,
независимый
консультант

Правильный выбор площадки для дата-центра может заложить основу его коммерческого успеха. Неправильный – создать постоянные проблемы в ходе эксплуатации, не говоря уж о финансовых потерях. На какие факторы обратить внимание заказчикам, впервые вовлеченным в процесс выбора? Как, учитывая опыт предшественников, не упустить важные мелочи?

В поисках стандартов и лучших практик

За годы практики в отрасли строительства ЦОДов авторы много раз сталкивались с задачей выбора и оценки площадок, на которых планируется строительство дата-центров. Заказчики, приступая к строительству, задают специалистам одни и те же вопросы (но, заметим, почти всегда – несмотря на полученные рекомендации – делают одни и те же ошибки). Эти вопросы в первую очередь вызваны отсутствием более или менее формализованной методики выбора подходящей площадки, общепринятой и признанной экспертным сообществом.

Есть общеизвестные документы, в которых принято искать правила или требования к площадкам и зданиям для размещения ЦОДов. Из них можно назвать следующие:

- Uptime Institute Data Center Site Infrastructure Tier Standard: Topology (Стандарт топологии инженерной инфраструктуры ЦОД Uptime Institute);
- Uptime Institute Data Center Site Infrastructure Tier Standard: Operational Sustainability (Стандарт операционной устойчивости ЦОД Uptime Institute);
- TIA-942. Telecommunications Infrastructure Standard for Data Centers (TIA-942. Стандарт телекоммуникационной инфраструктуры ЦОД);
- ANSI/BICSI 002-2001 Data Center Design and Implementation Best Practices (ANSI/BICSI 002-2001. Лучшие практики проектирования и строительства ЦОД).

Стандарт топологии Uptime Institute в текущей версии от 2012 г. не содержит ни одного требования к зданию или площадке. В ранних версиях, когда стандарт еще назывался классификацией, в приложении к нему была информационная таблица с основными характеристиками ЦОДов, которые отвечали требованиям Tier, но не являлись обязательными. В этой таблице единственным параметром здания был его тип – отдельное или разделяемое с другими арендаторами.

Стандарт операционной устойчивости Uptime Institute в текущей версии от 2013 г. содержит раздел 2.2 «Характеристики здания» и раздел 2.3 «Расположение площадки». Из раздела 2.2 ограниченно полезными для задачи выбора площадки могут быть требования достаточности площадей и наличия специальных зон в офисном блоке ЦОДа и свободных зон вокруг здания, а также требования выделенного здания для ЦОДа. А вот в разделе 2.3 присутствуют более конкретные требования: риски наводнения, ураганов, торнадо, сейсмической активности и вулканической деятельности, близости к аэропортам и военным авиабазам, воздействия прилегающих территорий, риски транспортных коридоров.

Стоит обратить внимание на то, что все эти параметры площадки в стандарте зафиксированы как риски, с указанием значений, которые позволяют отнести каждый из названных типов к категории «высокого риска» или «низкого риска». Теоретически, если предположить, что заказчику при выборе необходимо учитывать только те риски, которые перечислены в стандарте Uptime Institute, то задачу можно решить в рамках данного стандарта. Но не стоит забывать, что эти требования служат для определения уровня операционной устойчивости функционирования ЦОДа, а никак не для выбора площадки под строительство.

Известный и широко используемый стандарт TIA-942 содержит раздел 5.3.4 «Архитектурный проект», в котором перечислены требования к архитектурно-планировочным решениям машинных залов и несущим способностям перекрытий. Кроме этого, в таблице 8 приложения G собраны требования к конструктиву здания, к удаленности его от опасных объектов и активностей, к элементам территории ЦОДа, сейсмические требования и др. Все они подразделяются по Tier, т. е. имеют различные значения в зависимости от уровня Tier.

Известный документ класса «лучшие практики» ANSI/BICSI 002-2001 Data Center Design and Imple-

mentation Best Practices не содержит ни единого прямого требования, которое можно было бы использовать при формировании методики выбора здания или площадки для строительства дата-центра. Это неудивительно: в документе собраны наставления по проектированию и строительству, задача выбора – вне сферы его применения.

Все перечисленные выше документы (стандарты и лучшие практики) ни по отдельности, ни в совокупности не позволяют, по нашему мнению, сформировать детальный перечень требований и рекомендаций, следование которым позволило бы решить поставленную задачу – выбрать площадку для ЦОДа, проанализировав все важные элементы (не только технической природы). Получается, что каждый раз заказчику (или для заказчика) приходится придумывать новую процедуру выбора, основываясь на информации из открытых источников, предполагаемых параметрах объекта, консультациях с экспертами отрасли, а также на собственном опыте.

К сожалению, именно на финальных этапах создания объекта – стадиях строительства и передачи в эксплуатацию – становятся очевидны все проблемы, связанные с неверным выбором площадки, но очень часто оказывается, что решать их уже поздно, а если не поздно, то дорого или очень дорого.

В этой статье мы попытались декомпозировать процесс выбора здания/площадки под строительство дата-центра, а также привлечь внимание к особо важным деталям и параметрам оценки потенциальных объектов для размещения. Мы надеемся, что эта статья поможет создать формальный каркас, на основе которого можно будет строить любую заказную, нестандартную методику выбора площадки для строительства ЦОДа, просто собрав нужные кирпичики-элементы в конструкцию-последовательность, которая в наибольшей степени отвечает первоначальным задачам и ожидаемым результатам.

Подготовка: бизнес-требования

Первым шагом в поиске площадки под дата-центр должна стать формализация бизнес-идеи будущего дата-центра. От заказчика требуется ответить на ряд ключевых

при создании бизнес-плана вопросов: например, какие услуги ЦОДа он будет предоставлять рынку и в каком объеме? Каков целевой сегмент клиентов? Какие каналы сбыта будут наиболее эффективными? Какую схему ценообразования предполагается использовать? И наконец, какие объемы инвестиций может себе позволить заказчик?

Ответы на эти вопросы позволяют определить основные технико-экономические и географические характеристики будущего ЦОДа (см. табл. 1). Необходимо также учесть возможность долгосрочной аренды либо полного выкупа площадки, в зависимости от выбранной бизнес-модели.

Определив характеристики будущего ЦОДа (в зависимости от предполагаемой бизнес-модели, от структуры услуг и клиентов), заказчик может в большой степени формализовать техническое задание на поиск подходящей площадки, которое уже можно будет разослать специализированным агентствам недвижимости без дополнительных пояснений. Это значительно упростит процедуру поиска площадки, поможет избежать лишних визитов на не отвечающие требованиям объекты.

Далее, после подбора конкретных площадок, удовлетворяющих первичным требованиям технического задания, необходимо будет провести обследование каждого объекта с целью детальной проверки их технико-экономических характеристик и оценки возможности размещения на них оборудования дата-центра.

Выбор площадки: требования к зданию

Особенности здания

Первоочередным вопросом при выборе площадки будет следующий: что за здание, собственно, мы имеем, и какой объект можно в нем разместить? Попробуем декомпозировать эти вопросы в ряд существенных для строительства дата-центра элементов.

Наличие площадей под технологические системы и офисные помещения. Потребность в дополнительных площадях офисного и технологического назначения может различаться в зависимости от выбранной бизнес-модели и уровня надежности дата-

Результаты формализации бизнес-требований к будущему ЦОДу	
Задаваемые бизнес-планом параметры ЦОДа	Что позволяют определить
Количество стоек и их энергетические характеристики	Оценить необходимые объемы площадей под машинные залы и потребности в электрических мощностях
Коэффициент энергоэффективности (PUE)	Оценить потребность в электрических мощностях и в площадях под размещение инженерного оборудования. Зафиксировать требования к конструктивным особенностям здания
Количество технического и управленческого персонала (в зависимости от бизнес-модели и операционной модели эксплуатации)	Оценить потребность в офисных и иных вспомогательных помещениях
Места возможного размещения дата-центра	Локализовать географическую область поиска подходящей площадки под строительство
Нагрузочная способность перекрытий	Определить применимые технологические решения и потенциально возможные показатели энерговооруженности ЦОДа



центра. Например, в дата-центре высшего уровня отказоустойчивости требуется существенно больше технического персонала, чем в ЦОДе с более слабыми характеристиками. Большой штат инженерной службы потянет за собой потребность в большем количестве офисных помещений, мест для отдыха и т. д. Работа в сегменте крупнооптовых продаж, скорее всего, выльется в необходимость создания офисов для дежурных служб клиентов, а мелкооптовый и розничный бизнес потребует увеличения штата службы безопасности и числа дежурных инженеров для сопровождения клиентов в машинных залах.

На потребность в площадях влияют и выбранные технологические решения. Например, если планируется использовать в ЦОДе систему холодоснабжения на жидкостном хладагенте, это потребует устройства отдельного помещения под хладоцентр, в то время как для фреоновых машин подойдет и более компактное здание.

Возможность размещения энергоэффективного оборудования. Отдельно хочется выделить тему использования энергоэффективных решений для системы холодоснабжения. По сути это подзадача оценки наличия необходимых площадей, но ее решение может составлять отдельную проблему.

Заказчики, которые ставят перед собой цель создания высокоэнергоэффективного ЦОДа, должны отдавать себе отчет в том, что практически любое подобное решение строится в рамках тренда отказа от фреонового или жидкостного хладагента (не включая системы чиллерного фрикулинга) в пользу теплообмена воздуха в дата-центре с наружным воздухом. Решений такого плана достаточно много, но их основная особенность – существенные габаритные размеры. Теплоемкость воздуха существенно меньше, чем у типовых хладоносителей, а скорости подачи воздуха в ЦОД имеют вполне конкретные ограничения, и получается, что размеры теплообменников и воздушных коробов могут быть сравнимы с размерами машинных залов. Поэтому если за основу приняты значения показателя PUE ниже 1,3, требуемые площади под дата-центр могут удвоиться, что, соответственно, повлечет за собой большие капитальные и операционные расходы. При этом вписать подобную систему удастся далеко не в каждое здание.

Нагрузка на перекрытия. Эта характеристика может на корню загубить идею организации ЦОДа во многих зданиях. Дело в том, что распределенная нагрузка на перекрытия в типовом дата-центре составляет порядка 1 т/кв. м, а сосредоточенная нагрузка от шкафов аккумуляторных батарей и иного оборудования может достигать и 1,5 т/кв. м. С другой стороны, современные офисные здания рассчитываются на нагрузку в среднем до 300 кг/кв. м, а жилые здания – и того меньше. Именно поэтому все инвесторы стараются заполучить под дата-центр бывшие здания производственного назначения – фабрики, заводы и АТС. Помимо приемлемых проектных показателей нагрузочной способности такие здания могут иметь и большой энергетический потенциал.

Но с проектными параметрами нужно быть осторожным, так как существует эмпирическое правило: каждый год жизни здания отнимает до 1% первоначальной нагрузочной характеристики. Поэтому подобранное здание семидесятих годов с начальной нагрузочной способностью 1500 кг/кв. м к текущему моменту может потерять до 40% своей надежности и иметь реальное значение этого параметра в 900 кг/кв. м. Это означает, что обязательным требованием при выборе здания должна быть инструментальная проверка данного параметра, с последующей оценкой стоимости работ по усилению, либо получение достоверной информации от собственника здания. Таким образом удастся избежать существенных непредвиденных расходов на поздних этапах строительства либо рисков полного отказа от строительства объекта.

Нагрузка на кровлю. Данный вопрос становится особенно существенным, когда заказчик планирует размещать на крыше здания внешние блоки системы кондиционирования. Большинство построенных в советское время зданий не предназначалось для установки на кровле значительного количества технологического оборудования, и типовая нагрузочная способность выбиралась из расчета от 100 до 200 кг/кв. м – этого было вполне достаточно для размещения маломощного вентиляционного оборудования.

Внешние блоки системы холодоснабжения, в зависимости от выбранной технологии охлаждения, создают нагрузку от 50 кг/кв. м для фреоновых систем и до 500 кг/кв. м для чиллеров, что существенно превосходит среднюю нагрузочную способность кровли зданий старой постройки. Исходя из этого правила, мы рекомендуем, как и в случае с перекрытиями, заказать инструментальное обследование и на основании его результатов принимать решение о целесообразности строительства ЦОДа в таком здании.

Необходимость выноса имеющихся коммуникаций. При обследовании здания важно не упустить из виду, что при устройстве машинных залов и прочих технологических помещений все транзитные коммуникации, которые не относятся к инженерии ЦОДа (вода, электроснабжение, канализация и пр.), должны быть вынесены за пределы этих помещений. Таким образом снижаются риски прорыва коммуникаций в помещениях дата-центра, с нарушением работоспособности оборудования, а также риски, связанные с проведением профилактических работ на коммуникациях, что потребует допуска в помещения посторонних лиц.

На этапе обследования следует уточнить наличие транзитных коммуникаций, необходимость и технологическую возможность их переноса, что позволит учесть данную статью в расходах на капитальное строительство и уберечь себя от финансовых и технологических рисков.

Пути проноса оборудования. В нашей практике были случаи, когда неопытные заказчики, выбирая помещения под дата-центр, невнимательно изучали габариты путей проноса оборудования, а впоследствии

оказывалось, что пронести в ЦОД крупногабаритное оборудование, такое как блоки системы кондиционирования и ИБП, просто невозможно. Или же приходилось разбирать стены, поднимать оборудование не на грузовом лифте, а через оконные проемы и т. д., что делало весь процесс существенно дороже.

Мы рекомендуем во время обследования здания, предварительно оценив максимальные массогабаритные характеристики серверного и инженерного оборудования, пригласить на объект компании, профессионально занимающиеся такелажными работами, и совместно с их специалистами оценить как возможность, так и сложность и стоимость работ по проносу оборудования на места установки. Это позволит детализировать бюджет строительства и избежать ситуации, когда придется полностью отказаться от проекта.

Арендаторы/совладельцы по соседству. При выборе помещения под ЦОД особое внимание необходимо уделить соседям-арендаторам или совладельцам здания. Если по соседству располагаются опасные производства или над будущим дата-центром находятся помещения с мокрыми процессами, следует предусмотреть организацию защиты от их негативных влияний, а при невозможности ее организовать – совсем отказаться от данного помещения. Следует также помнить, что арендаторы не вечны, и на место нынешних соседей может прийти компания с иным бизнес-профилем, поэтому имеет смысл на начальных этапах переговоров с арендодателем выяснить его арендную политику и проговорить условия и ограничения на сдачу в аренду соседних помещений.

Возможность создания внутренних периметров безопасности. Риски соседства могут быть сопряжены не только с технологическими опасностями, но и с организационными. Заказчик изначально должен оценить возможность создания периметров безопасности дата-центра и организации маршрутов движения сотрудников и клиентов. Если планировка здания не позволяет сделать обособленный вход в помещение машинного зала и иные помещения ЦОДа, обеспечить охраняемые проходы в данные помещения, это существенно повышает риски внешнего вторжения, а значит, уменьшает маркетинговую привлекательность объекта для потенциальных клиентов.

Мы неоднократно, к примеру, сталкивались с ситуацией, когда вход в машинный зал был организован со стороны коридора, находящегося в общем пользовании, либо через офисные помещения ЦОДа был организован проход в общие с соседями туалетные комнаты. На этапе выбора помещения следует детально выяснить, можно ли исключить подобные ситуации, путем изучения планировочных решений и переговоров с арендодателями.

Расположение здания

Расположение здания – немаловажный фактор успешности и финансовой целесообразности проекта ЦОДа, оно в большой степени формирует маркетинговую привлекательность будущего объекта. Обсудим де-

тально, какие элементы этой характеристики следует учитывать.

Пути подъезда и подвоза оборудования. Ситуация в российском бизнесе ЦОДов такова, что клиенты все еще предпочитают иметь отдельный, по возможности не затрудненный проезд к зданию на общественном либо личном транспорте. Как известно, дорожная ситуация у нас способна сильно осложнить жизнь, и привлекательность той или иной площадки дата-центра для клиентов при прочих равных условиях может существенно зависеть от транспортной составляющей. Поэтому необходимо стремиться, чтобы площадка располагалась недалеко от основных транспортных магистралей и в пешей доступности от остановок общественного транспорта. Конечно, требование близости к магистралям существенно лишь для ЦОДов с преобладанием розничного бизнеса, но помимо удобства клиентов следует учитывать наличие путей подвоза резервного топлива в случае аварийных ситуаций.

Как и в случае с путями проноса оборудования в помещение ЦОДа, важно помнить о путях подвоза оборудования к самому зданию дата-центра. Случалось, невнимательный заказчик обнаруживал, что грузовой автомобиль с контейнером ДГУ не в состоянии заехать на объект, когда тот уже стоял перед въездными воротами на территорию.

Каналы связи и связанная канализация. Наличие в здании каналов связи не всегда является серьезным критерием при выборе объекта. Операторы связи с удовольствием подведут свои линии к новому ЦОДу, который является для них генератором трафика, – но так дела обстоят в густонаселенных районах с хорошо развитой связанной инфраструктурой. Если здание под ЦОД расположено в удалении от магистральных каналов связи, их прокладка станет дополнительной статьей расходов в бюджете строительства.

Аналогично кабельной канализации под электролинии, прокладка линий связи обойдется существенно дешевле при наличии кабельных каналов, поэтому при обследовании желательно также получить сведения об этих коммуникациях.

Надежность площадки как резервной. Если речь идет о создании резервного ЦОДа, местоположение площадки под строительство следует оценивать и с точки зрения отказоустойчивости. Эта комплексная характеристика складывается из рисков одновременного возникновения аварийных ситуаций на основной и резервной площадке, вызванных общими причинами. Например, не стоит рассматривать ЦОДы, где энергоснабжение основной и резервной площадки организовано от одного источника генерации либо для обеих площадок используется единый магистральный канал связи.

Возможность создания внешних периметров безопасности. При обустройстве внешних периметров для начала необходимо создать условия для контроля допуска лиц на территории внешних площадок инженерных систем. Площадки ДГУ и внешних блоков

системы кондиционирования должны быть защищены от несанкционированного проникновения. Кроме того, было бы нелишним не размещать такие площадки вблизи дорог внутреннего пользования, поскольку случаи наезда транспорта на оборудование исключить нельзя.

Зачастую наиболее эффективный способ минимизировать данные риски – это полностью отгородить внешние площадки ЦОДа, в том числе парковочные места клиентов и сотрудников, от зон, доступных другим арендаторам здания. Поэтому заблаговременное обсуждение возможного планирования территории может существенно повысить защищенность дата-центра от внешнего физического воздействия.

Окружение. Опасным может быть соседство не только внутри здания ЦОДа, но и вне этих площадей. Высотные здания по соседству могут стать источником потенциальных рисков для оборудования. Еще не забыта история с одним из московских дата-центров, который был вынужден временно приостановить оказание услуг после того, как во время урагана на внешние блоки системы кондиционирования упал рекламный щит с соседнего, более высокого здания.

Не забудем и такое частое в России явление, как тополиные рощи, которые в период цветения могут стать постоянной головной болью эксплуатационных подразделений дата-центра...

Сейсмоактивность и подтопление. Возможно, сейсмоактивность – не столь существенный фактор при выборе помещения под строительство в рамках одного города или области, но при создании резервного ЦОДа на значительном удалении от основного он может стать достаточно весомым. Например, при выборе между несколькими равноценными площадками предпочтение, естественно, стоит отдать тем, которые находятся вне сейсмоопасных зон. Помимо более высоких рисков разрушения дата-центра под воздействием стихийных сил это обусловлено и существенным увеличением затрат на строительство объекта, поскольку приходится применять дорогостоящие сейсмоустойчивые технические решения.

Более очевидный и распространенный риск – подтопление ЦОДа. Различного типа водоемы – распространенное явление в российской действительности, и при изучении той или иной площадки под строительство необходимо получить информацию о максимальном уровне воды в ближайших водоемах. Необходимо также оценить риски попадания дождевых и сточных вод в помещения и на территорию ЦОДа, если он находится в низине. **ИКС**

О прочих важных факторах при выборе площадки для ЦОДа, а также о том, как выявить связанные с ними риски и управлять ими, читайте в следующем номере «ИКС».

Ситуация под контролем

Системы ситуационного управления – программные надстройки к интегрированным системам физической защиты – в острых ситуациях помогают исключить человека и связанные с ним ошибки из процесса принятия решения.



Илья ГРАНКОВ, эксперт, «АРМО-Системы»

Интегрированные системы безопасности на объекте объединяют подсистемы видеонаблюдения, контроля и управления доступом, ОПС, обеспечивая их совместную работу. На практике интегрированная система безопасности, моно- или мультибрендовая, организует взаимодействие

подсистем из одной сферы в автоматическом или автоматизированном режимах. В первом случае автоматика способна, например, инициировать запись видео системой телевизионного наблюдения по сигналу тревоги от датчика системы охранной сигнализации. Во втором – на события реагирует оператор, получая всю информацию на своем рабочем месте.

Решения класса Physical Security Information Management (PSIM) – это своего рода «шапка», программный комплекс, взаимодействующий с каждой подсистемой. PSIM-системы реализуют весь функционал автоматической и автоматизированной работы подсистем, причем не только видеонаблюдения, СКУД



и ОПС, но и инженерных, геопозиционных, систем телефонии, коммуникации и др.

PSIM-решения не рассчитаны на применение на небольших предприятиях с малым количеством подсистем (тем более на те, где отсутствует оперативная диспетчерская как таковая), на объектах малого и среднего масштаба в них просто нет необходимости. Сфера их применения – действительно крупные объекты, такие как аэропорты, вокзалы, промышленные предприятия, где ежедневно количество событий, классифицируемых как тревожные, измеряется десятками, сотнями и тысячами. Все они «атакуют» неожиданно, требуют незамедлительной реакции, и оператор оказывается буквально под перекрестным огнем. Держать в голове все сценарии событий физически невозможно, к тому же большая часть ответных реакций регламентируется различными нормативными актами, законодательством, внутренними положениями и др. Вероятность критической ошибки возрастает, на сопоставление своих действий с регламентами и самопроверку у оператора уходит время, а решение, даже абсолютно верное, но принятое с опозданием, может привести к значительным материальным потерям или даже к гибели людей.

Говоря упрощенно, основная задача PSIM-системы состоит в том, чтобы исключить оператора из процесса принятия решения. Это, конечно, не означает, что человек оказывается отстраненным как ненужное звено, – нет, исключается именно человеческий фактор и возможные связанные с ним ошибки. Скажем, в силу ряда причин оператор может неверно расставить приоритеты и сделать неправильные выводы о степени критичности ситуации, недооценив уровень угрозы.

PSIM-система обеспечивает представление ситуации посредством единого унифицированного интерфейса, на основе информации, собираемой от установленных на объекте подсистем, и позволяет работать с ситуацией в развитии от начала до конца. Например, если срабатывает датчик утечки, но пожара пока нет, то сценарий реагирования будет один, а если поступает новый сигнал о том, что произошло возгорание, изменяется уровень критичности и алгоритмы реакции.

Датчиками для системы PSIM являются все устройства, от которых может поступать информация о происходящем. В данном случае ее задача – в первую очередь обеспечить корректное представление ситуации для оператора на основе анализа сигналов, поступающих от датчиков, а затем незамедлительно предложить оператору варианты выхода из ситуации, максимально автоматизировав этот процесс. В системе уже заложена логика реакции на события, и каждый следующий шаг она может выполнять автоматически при подтверждении оператором сигналов от датчиков (например, автоматически будет набираться телефонный номер пожарной охраны, скорой помощи, активироваться связи между подсистемами и т.д.).

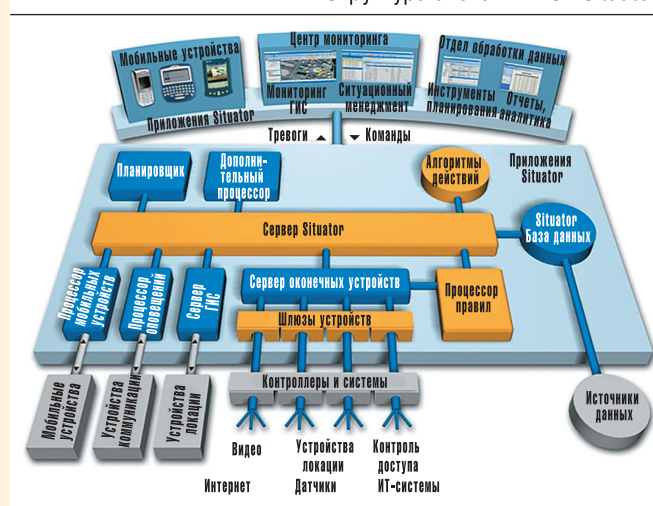
Система PSIM минимизирует вероятность того, что ситуация начнет развиваться непредсказуемо, направляет оператора на верный путь действий на каждом

этапе, исключая тем самым ошибки, и сокращает до минимума затраты времени на ответные действия. Но каждая из подсистем на объекте, будь то охранно-пожарная, инженерная или любая другая, продуцирует гигантский объем данных, и у каждой есть свой сектор ответственности. Как их объединить? Эту задачу и решает система ситуационного менеджмента. Рассмотрим решения, которые предлагают ведущие мировые производители.

Координация действий

Одно из решений для ситуационного менеджмента – программная платформа NICE Situator, разработка компании Orsus, в 2009 г. приобретенной NICE Systems. В платформу интегрированы продукты более 150 известных марок, среди которых AXIS, Bosch, Cisco, Honeywell, IBM, JVC, Nedap, Pelco by Schneider Electric, Simplex Grinnell, Skype, Sony, Xtralis и др. Более того, возможна поддержка оборудования любого производителя, удовлетворяющего требованиям заказчика или интегратора. Это PSIM-решение работает в различных отраслях по всему миру; в России, в частности, оно используется в Сочи в рамках проекта «Безопасный город».

Структура системы NICE Situator



Система многофакторного ситуационного менеджмента служит для обработки, реагирования, изучения и анализа ситуаций. ПО обрабатывает и анализирует в реальном времени разнородные потоки данных, например видео, телефонные звонки, сигналы от датчиков, данные мобильных приложений и др. Система обеспечивает своевременное получение сигнала о возникновении тревожного события, предоставляет информацию о месте и времени происшествия, определяет алгоритмы реагирования и координирует действия сотрудников охраны.

Чтобы создать целостную оперативную картину, NICE Situator позволяет соотнести данные с камер наблюдения, сигналы от датчиков, а также скоординировать системы связи, управления доступом, пожарной сигнализации, VoIP, Интернет-ресурсы, технологические процессы и др., обнаруживая возможные и теку-

щие связи между ситуациями, которые на первый взгляд кажутся несвязанными.

Интуитивно понятный интерфейс обеспечивает визуализацию ситуации: в реальном времени отображаются сигналы тревоги и информация, поступающая от всех компонентов интегрированного решения. Программный интерфейс объединяет функции геоинформационных систем (ГИС) и систем автоматизированного проектирования (САПР). Благодаря этому NICE Situator способна автоматически отображать различные информационные слои (планы этажей, карты, фотографии, чертежи, трехмерные модели и др.), а также контролировать все подсистемы, активность на объекте, деятельность сотрудников и т.д. в рамках единой рабочей среды.

NICE Situator является открытым решением и может работать на базе уже имеющейся в организации ГИС-инфраструктуры. Эта платформа позволяет автоматизировать отдельные задачи и сложные системные процессы, предусматривает автоматизированные планы реагирования для разных происшествий и сценариев, а также модификацию и корректировку моделей поведения по мере развития событий. В частности, есть возможность перенаправления задач и уведомлений, которые не были обработаны надлежащим образом в заданный промежуток времени, другим сотрудникам (операторам) и на другие ресурсы.

Разные оперативные службы могут пользоваться NICE Situator одновременно. За счет оригинальных средств формирования отчетов (автоматического и по запросу) и работы с ними упрощается подведение итогов и ведение ситуационных расследований.

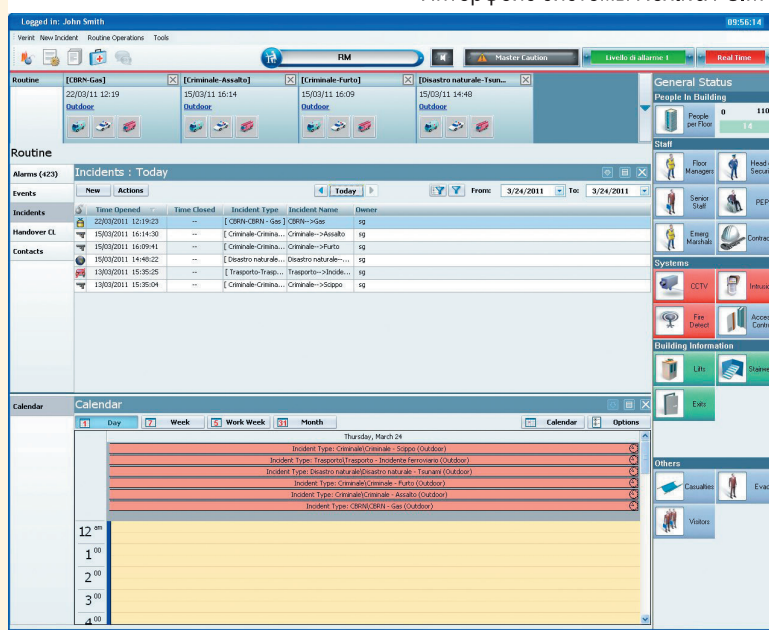
Одна из задач системы – упорядочить перекрестные связи событий и реакций различных подсистем; более того, она предоставляет возможность программирования этих связей, т. е. реального управления ситуацией. При инсталляции NICE Situator специалисты всесторонне исследуют объект, рассматривают потенциально возможные угрозы и, оперируя набором доступных информационных каналов, разрабатывают вероятные сценарии развития ситуации и алгоритмы реакций в соответствии с действующими регламентами и нормативными документами. Поэтому каждый проект, реализованный на базе NICE Situator, уникален в том, что касается внедрения и эксплуатации.

Комплексный подход

Решение Nextiva PSIM разработано американской компанией Verint Systems, имеющей многолетний опыт создания комплексных систем реагирования на события. Такие системы работают в центрах ситуационного управления на крупных объектах по всему миру, в числе которых аэропорты и морские порты, нефтехимические предприятия и др.

Компания имеет в своем арсенале и программные средства, и аппаратные решения. В продуктовую ли-

Интерфейс системы Nextiva PSIM



нейку Verint входят управляющее ПО для систем видеонаблюдения с поддержкой видеоаналитики, а также камеры стандартного и мегапиксельного разрешения, фиксированные и поворотные, для помещений и в уличном исполнении; видеоэнкодеры, декодеры и другое оборудование.

Nextiva PSIM объединяет подсистемы защиты периметра, детектирования вторжений, видеонаблюдения, контроля доступа, коммуникаций, BIS (интегрированные системы управления зданием) и т.д. Среди ее функций – мгновенное оповещение о подозрительных событиях, централизованный и децентрализованный мониторинг, управление с помощью системных процедур и стандартов, возможности планирования в чрезвычайных ситуациях, разбора ситуаций и анализа реальных событий.

Система реализует несколько этапов ситуационного менеджмента. Так, на этапе планирования могут прорабатываться сценарии развития штатных и чрезвычайных ситуаций, процедуры реагирования, оптимальное расположение датчиков. На этапе обучения операторов и персонала оттачивается навык получения информации через единый интерфейс и быстрого реагирования, в том числе с помощью виртуального моделирования ситуации. Этап мониторинга в реальном времени подразумевает непрерывное отслеживание текущей ситуации и контроль исполнения сценариев реагирования, а этап составления отчетов обеспечивает подбор всей необходимой информации для постанализа происшествия и «разбора полетов».

Благодаря масштабируемой архитектуре система поддерживает одновременную работу множества пользователей, просматривающих видео и другие данные из разных мест (датчиков и подсистем), обеспечивая системную приоритизацию задач. Даже если эти пользователи территориально разделены, они могут

оперативно обмениваться данными и эффективно взаимодействовать.

Среди основных особенностей Nextiva PSIM можно выделить трехмерный многоуровневый интерфейс пользователя, позволяющий координировать информацию из разных источников. На одном экране оператора могут отображаться видео, фото, географические карты для локализации места события, любая текстовая информация, аудио, телефонные номера и т.д. Двух- и трехмерные карты позволяют задействовать множество слоев для иллюстрации зон охвата камер и датчиков, например улиц, и очерчивания границ опасных областей, сообщать о потенциальных направлениях распространения угроз в режиме реального времени (в частности, при стихийных бедствиях). Со своего рабочего места оператор может взаимодействовать с несколькими пунктами одновременно, контролировать происходящее в них и принимать меры.

Внимание к деталям

Программный продукт Surveillint был разработан компанией Proximex, которую в 2011 г. приобрела Tyco Integrated Security (ранее известная как ADT Security Services). Это полнофункциональное PSIM-решение используется на многих крупных объектах, в числе которых порт Long Beach и международный аэропорт в Сан-Диего (США).

В зависимости от специфики конкретного объекта программный комплекс может решать разные задачи. В первую очередь это интеграция всех имеющихся подсистем и использование единой надстройки для управления ими. В частности, система способна эффективно взаимодействовать с подсистемами IP-видеонаблюдения Cisco, контроля доступа Lenel, видеоаналитики Agent VI, а также с IP-камерами AXIS, IQinVision и других производителей.



Surveillint ведет мониторинг ситуации на объекте в режиме 24x7, собирает информацию от всех подсистем, анализирует поступающие данные, соотносит их друг с другом и с заранее установленными политиками и процедурами реагирования на те или иные события – и незамедлительно оповещает оператора о значимых происшествиях. Тем самым система позволяет задействовать все источники информации о событии, сократить до минимума время принятия решений, повысить эффективность работы каждого из сотрудников службы безопасности.

Единый интерфейс пользователя Centralized Console позволяет в буквальном смысле слова развернуть перед оператором картину происходящего и обеспечить ему доступ в один клик к любому из источников информации, будь то визуализация ГИС (включая отслеживание перемещающихся объектов на карте), просмотр живого и записанного видео одновременно, ручное манипулирование PTZ-функциями камер и др. Кроме того, функция EZ Track позволяет автоматически сопровождать перемещающиеся объекты с помощью нескольких камер наблюдения. Чтобы обеспечить максимальную осведомленность оперативных сотрудников о ситуации и согласовать их действия с центром мониторинга, используется приложение PocketSurveillint для смартфонов.

Контроль ситуации и всех подсистем объекта, автоматический сбор информации от разных источников, ее обработку и инициализацию сценариев реагирования в соответствии с предустановленным набором правил, политик и процедур обеспечивает компонент Business Logic Manager.

Surveillint представляет собой открытую, масштабируемую платформу, рассчитанную на тысячи датчиков, с автоматическим обнаружением новых устройств в системе. Наличие Proximex SDK позволяет интегрировать в систему дополнительные подсистемы и устройства, как вновь приобретенные, так и уже функционирующие на объекте заказчика.

Оценивать перспективы PSIM-решений на российском рынке безопасности достаточно сложно. Часто бессистемный подход к эксплуатации объектов – несогласованность действий различных подразделений и служб, отсутствие строгих стандартов оснащения и полноценно проработанных регламентов, оговаривающих действия персонала в определенных ситуациях, – ведет к процветанию разного рода компромиссов, мешающих широкому применению таких систем. Недооценивается и экономическая эффективность внедрения и использования PSIM-решений, которая достаточно велика, несмотря даже на их высокую стоимость. Тем не менее подобные системы уже функционируют на некоторых объектах – и их востребованность и оправданность применения становятся все более очевидными. ИКС

SDN прорывная технология или маркетинговый пузырь?



Ярослав ГОРОДЕЦКИЙ,
генеральный директор,
CDNvideo

отделено от устройств передачи данных и реализуется программно отдельными элементами сети. Таким образом, сеть SDN представляет собой набор «безмозглых» коммутаторов, которыми управляет «умное» управляющее устройство, называемое контроллером (см. также → [с. 43](#)). Информацию о том, как именно маршрутизировать трафик, контроллеры, в свою очередь, могут получать от внешних приложений, что делает возможным создание сколь угодно сложных сетевых сервисов.

Подход к построению SDN кардинально отличается от сегодняшних принципов создания сетей передачи данных: SDN – это сеть с централизованным управлением, тогда как современные сети предполагают наличие множества «умных» маршрутизаторов, которые самостоятельно определяют маршруты трафика, основываясь на информации, получаемой по протоколам маршрутизации (BGP, OSPF и т.п.) от соседних узлов. ПКС избавляет от необходимости иметь уровень управления (Control Plane) в каждом сетевом устройстве, что, очевидно, удешевляет и это устройство, и сеть в целом.

Преимущества и недостатки

Строго говоря, в концепции централизованного управления сетью ничего нового нет – около 10 лет назад похожую трансформацию переживали голосовые сети, когда управление от отдельных АТС было передано программным коммутаторам (softswitch). Выгоды централизованного управления понятны – это меньшая стоимость оборудования и ПО в расчете на узел сети, более простое управление, возможность легкого запуска дополнительных сервисов одновременно на всей сети.

Но у централизации управления есть и недостатки. Прежде всего, это меньшая отказоустойчивость (живучесть) сети: при выходе из строя управляющего элемента или потере связи с ним «безмозглый» периферийный узел может стать совершенно бесполезным, в то время как при самоуправлении он легко адаптировался бы к изменившейся ситуации. Кстати, спор о том, какое управление лучше – централизованное или децентрализованное, продолжается много лет, и отнюдь не только применительно к

Программно определяемые сети (SDN) обещают изменить принципы построения IP-сетей операторов связи и предприятий. Что нужно для того, чтобы эта технология не осталась лишь модным поветрием?

Что такое SDN

Программно определяемыми сетями (SDN, Software-Defined Networks, вариант перевода – программно конфигурируемые сети) называют сети передачи данных, в которых управление трафиком

сетям связи – я хорошо помню спор на эту тему в средствах массовой информации в конце 80-х годов при обсуждении выбора между социализмом и капитализмом.

Миллиардная сделка

История программно определяемых сетей короткая, но захватывающая. Концепция SDN впервые была выдвинута в 2005 г. профессором Стэнфордского университета (США) Ником Маккененом. Сам Ник во время визита в Москву рассказывал, что поначалу его проект был встречен производителями телекоммуникационного оборудования в штыки: так, в штаб-квартире Cisco ему долго доказывали, что предложенная им сетевая архитектура принципиально неработоспособна и заниматься ею – пустая трата времени. Правда, в других крупных ИТ-компаниях, например в Microsoft, его, наоборот, поддержали.

Чтобы проверить жизнеспособность концепции, Ник и его единомышленники разработали прототипы контроллера и коммутатора и перевели на архитектуру SDN кампус Стэнфордского университета. Проект был успешно реализован, после чего его инициаторы и идейные вдохновители основали стартап Nicira. Разработками этого стартапа заинтересовалась компания VMware, лидер рынка виртуализации серверов, увидевшая в SDN средство виртуализации корпоративных сетей. В итоге VMware купила компанию Nicira за \$1,26 млрд – лишь в пять раз дешевле, чем стоил мобильный бизнес Nokia при его покупке Microsoft.

Сверхуспешная продажа Nicira, сделавшая ее основателей мультимиллионерами, изрядно повысила интерес к технологии SDN и стала катализатором серии покупок крупными вендорами стартапов, занимающихся программно определяемыми сетями. К настоящему времени такие сделки совершили и Cisco и Juniper – компании, которые несколько лет боролись против SDN, решили возглавить процесс их распространения по миру. Сейчас в их продуктовых линейках есть и SDN-совместимые IP-коммутаторы, и контроллеры, которые они рекомендуют для установки операторам связи.

SDN в работе

Однако говорить о том, что крупным производителям удалось перехватить инициативу на рынке SDN, не стоит. Основная масса реально работающих программно определяемых сетей реализована не с помощью их продуктов, а на основе программного обеспечения с открытым кодом и внутренних разработок компаний, решивших внедрить SDN. Больших успехов на этом поприще добился японский оператор NTT, который использует SDN как раз для того, чтобы сокра-

тить затраты на приобретение и обслуживание продуктов крупных западных производителей телекоммуникационного оборудования и снизить зависимость от них. Поэтому NTT разработал собственный контроллер сетей Trema и на его базе строит свои IP-сети, пользуясь при этом дешевыми SDN-совместимыми коммутаторами NEC. Уже сейчас на рельсы SDN переведены четыре крупнейших телекоммуникационных узла NTT в Азии.

Самой же заметной реально работающей SDN стала сеть компании Google, которая по этой сети распространяет весь свой IP-трафик, составляющий около 7% мирового трафика. SDN позволила Google отказаться от тех ограничений, которые накладывают в своих решениях традиционные производители. С помощью разработанного Google контроллера можно перебрасывать трафик между дата-центрами так, как это удобно и выгодно: например, направлять трафик на тот ЦОД, который ближе к пользователю или где есть нужный пользователю контент, а при перегрузке одного из ЦОДов – снять с него трафик и перераспределить между другими дата-центрами.

Не стоит в стороне от процесса внедрения SDN и Россия. Некоторые хостеры активно ее используют для балансировки входящего трафика. В частности, это сделала компания Hosting Community, входящая в холдинг РБК. Крупные операторы, такие как «Ростелеком», также начали присматриваться к SDN и создают рабочие группы, исследующие эту технологию. Вообще, SDN – хороший шанс для российских компаний. Ведь если производить железо мы никогда особенно не умели, то наши программисты – одни из лучших в мире, и на рынке ПО Россия вполне конкурентоспособна. В архитектуре SDN достаточно рыночных ниш, которые могли бы занять российские разработчики. Это и создание контроллеров для разных типов сетей, и написание сетевых приложений, работающих поверх уже созданных контроллеров.

Открытый поток

В формальном определении программно определяемых сетей протокол OpenFlow не упоминается, однако SDN и OpenFlow – близнецы-братья: в мире нет практически ни одной SDN, которая не была бы построена на этом протоколе. Правда, некоторые производители иногда называют программно определяемыми сети, которые вместо OpenFlow используют проприетарные механизмы управления, но я бы рассматривал это лишь как попытку угодить за модой. Точно так же лет пять-семь назад на любое телекоммуникационное решение наклеивался ярлык «IMS ready» («готов к работе на сети IMS»), хотя мало кто из продавцов этих решений в действительности думал, что когда-нибудь дело дойдет до подключения их продуктов к настоящей, полностью соответствующей стандарту сети IMS.

Протокол OpenFlow нужен для того, чтобы извне управлять трафиком на сетевых устройствах, как правило – на IP-коммутаторах (т.е. на Ethernet-коммутаторах, работающих на 3-м уровне модели OSI). Он позволяет внешнему управляющему устройству (контроллеру OpenFlow) формировать коммутационную матрицу на сетевом устройстве: добавлять туда дополнительные строки и принимать

запросы для определения, куда следует маршрутизировать неизвестные пакеты. То есть контроллер OpenFlow выполняет ту же функцию, какую в обычных маршрутизаторах выполняет уровень маршрутизации (Routing Plane) – мозг любого маршрутизатора, который с помощью протоколов маршрутизации вычисляет оптимальные маршруты. При этом один контроллер OpenFlow может заменить собой множество «мозгов», рассредоточенных в маршрутизаторах по всей IP-сети.

Протокол OpenFlow – открытый стандарт, поэтому использовать его в своих устройствах может любой производитель телекоммуникационного оборудования. Уже сейчас этот протокол поддерживают многие производители Ethernet-коммутаторов. Первыми это стали делать NEC и BigSwitch, чуть позже – Pronto и Marvell. Затем к ним присоединились IBM, Brocade и HP, и только после этого о поддержке OpenFlow заявили лидеры рынка IP-коммутаторов – Cisco, Juniper и Extreme Networks.

Контроллеров OpenFlow на рынке также достаточно, причем некоторые из них реализованы на основе программного обеспечения с открытым кодом: они распространяются по лицензии, разрешающей бесплатное использование ПО, но запрещающей его модификацию и продажу. К таким контроллерам относятся NOX и POX, разработанные первопроходцем SDN, компанией Nicira; контроллер Beacon, управляющий первой в мире SDN Стэнфордского университета; Floodlight, разработанный компанией BigSwitch.

Открытость протокола OpenFlow позволит в перспективе превратить коммутаторы с поддержкой OpenFlow в товары широкого потребления и, соответственно, снизить цены на них до минимума. Вкупе с наличием бесплатных контроллеров OpenFlow это существенно удешевит построение сетей передачи данных по сравнению с сегодняшним уровнем.

За всеобщую интернетизацию

Именно дешевизна и простота программно определяемых сетей могут, на мой взгляд, стать драйверами их распространения по всему миру для построения дешевых сетей доступа в интернет. SDN обладают потенциалом для того, чтобы ликвидировать цифровое неравенство на нашей планете. Нынешние технологии эту задачу не решают, ведь сейчас подключение к интернету имеет лишь около трети населения Земли.

Важно, чтобы SDN не стали, подобно упомянутой концепции IMS, очередным маркетинговым пузырем, надуваемым производителями и продавцами оборудования. Чтобы этого не произошло, покупатели SDN-решений из числа операторов связи должны требовать полного соответствия приобретаемых решений стандартам OpenFlow, тестировать их совместимость с оборудованием, программными контроллерами и сетевыми приложениями сторонних производителей. Без этого развитие SDN лишится своего изначального смысла – технологической открытости сети. И из технологии, способной изменить принципы построения телекоммуникационных сетей, SDN превратятся в очередную красивую упаковку для продажи моновендорных решений. ИКС

Оборудование интерактивного управления

расширение
функциональных
возможностей



Андрей СЕМЕНОВ,
технический директор,
RiT Technologies,
докт. техн. наук

О востребованности систем интерактивного управления (СИУ) на массовом рынке говорит явное их упоминание в последних редакциях базовых стандартов, причем при создании масштабных кабельных систем их применение становится обязательным.

Технические предпосылки совершенствования СИУ

Классические СИУ в соответствии с требованиями профильных стандартов не взаимодействуют с цепями передачи информационных сигналов и внедряются в кабельную систему методом наложения, точно вписываясь в ее структуру. Этому немало способствует иерархическое построение СКС. На среднем и верхнем уровне системы интерактивного управления вне зависимости от ее конкретного исполнения всегда используются активные устройства: сканеры и объединяющие их в единую систему управляющие мастер-устройства или их функциональные аналоги, а также сервер базы данных. Большая часть этих устройств через соответствующие порты подключается к ЛВС предприятия.

СИУ создавались как средство поддержки администрирования СКС и максимально полной автома-

Оборудование интерактивного управления используется при построении СКС более двух десятилетий и сегодня занимает прочное место на физическом уровне информационных систем. За прошедшее время оно «поумнело», уменьшилось в размерах и «доросло» до начала процесса стандартизации.

тизации рутинных функций. Стабильность структуры кабельной системы обуславливает низкую загрузку вычислительных ресурсов СИУ даже при выполнении всех нормативных процедур администрирования. В результате у типовых интеллектуальных устройств, применяемых в данной сфере, имеются значительные и, что существенно, в принципе неиспользуемые резервы вычислительных мощностей. Эти ресурсы вполне могут быть направлены на решение различных сервисных задач без ущерба для остальных функций.

Возможность маневрировать вычислительными мощностями весьма востребована в современных информационных системах. Например, в крупных аппаратных, не говоря уже о ЦОДах, очень важен контроль и регулирование параметров окружающей среды, поскольку даже их небольшие отклонения от оптимальных значений ощутимо влияют на функционирование ИТ- и телеком-оборудования и заметно снижают эксплуатационную доступность объекта в целом.

Поскольку количество отслеживаемых физических величин не превышает десятка, а изменяются они не чаще нескольких раз в секунду, как программная, так и аппаратная сторона реализации их контроля не представляет особой сложности. Датчики систем контроля различных параметров технических помещений серийно выпускаются промышленностью. На

рынке имеется огромный выбор этих компонентов со стандартизованным интерфейсом, а их взаимодействие с оборудованием более высокого уровня осуществляется по широко распространенным протоколам.

Улучшение массогабаритных параметров контроллеров

Контроллеры первых поколений, выполненные как полномаштабные 19-дюймовые корпусные устройства, устарели не столько физически, сколько морально. Приближение этих устройств к местам установки датчиков (в широком смысле этого слова) и укорачивание за счет этого соединяющих их линий способствует улучшению массогабаритных параметров контроллеров и позволяет расширить функциональные возможности СИУ.

Наиболее перспективным видится исполнение контроллера в форме навесного устройства и установка его непосредственно на коммутационной панели. Место установки может выбираться в центре (например, для изделий Panduit) или на краю (для оборудования Surtec) оборотной стороны лицевой пластины.

Ценность подобного решения повышается тем, что отказ от 19-дюймового исполнения корпуса контроллера экономит посадочные места конструктива. В современных информационных системах последние становятся дефицитным ресурсом из-за роста

объема составляющего их оборудования.

Тем не менее нацеленное на экономию посадочных мест исполнение класса zero-U, основанное на сохранении традиционного фактора корпуса контроллера в сочетании с его установкой на задние монтажные направляющие, большого распространения не получило. Дело в том, что такое решение заметно ухудшает условия визуального наблюдения оптических индикаторов и дисплея контроллера. Кроме того, в некоторых СИУ на контроллерах располагаются элементы управления, к которым системный администратор должен иметь непосредственный доступ.

Еще один вариант класса zero-U – вынос штатного места установки контроллера в вырезы боковых панелей-заглушек – устраняет указанный недостаток. Однако он тоже не слишком популярен, поскольку требует радикальной перестройки конструкции шкафа.

Увеличение информативности сигналов взаимодействия

Эффективность функционирования СИУ во многом определяется количеством и информационной наполненностью сигналов, которые управляющий контроллер отдает системному администратору при наступлении различных штатных и нештатных событий и выполнении рабочих заданий на изменение конфигурации СКС. Подсистема современной СИУ, реализующая эту функцию, представляет собой развитый многоканальный комплекс, который на физическом уровне включает в себя следующие разновидности индикаторных элементов и извещателей:

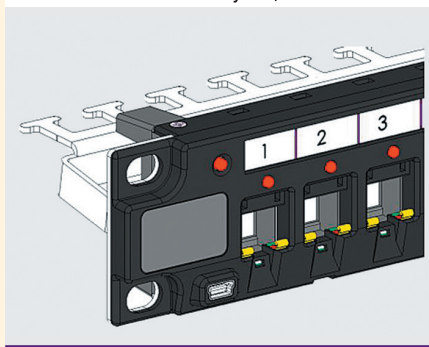
- отдельные для каждого порта коммутационной панели оптические индикаторы преимущественно классического светодиодного типа (применение для этой цели жидкокристаллических индикаторов, иконок с задней подсветкой и пр. часто описывается в патентных документах, но в серийных

изделиях встречается буквально в единичных случаях);

- групповые оптические индикаторы различного функционального назначения коммутационных панелей и контроллеров (см., например, рис. 1);
- акустические однотонные извещатели;
- полномасштабные многострочные жидкокристаллические дисплеи матричного типа на сканерах.

Основные усилия разработчиков, естественно, направлены на совершенствование оптических индикаторных элементов. Даже одиночный индикатор может превратиться в многофункциональное устройство – за счет различной частоты его включения-выключения при работе в мигающем режиме. Также используются многоцветные светодиоды (скажем, в решении Panduit), а одновременное включение-выключение нескольких отдельных элементов обеспечивает групповую индикацию и т.д.

Рис. 1. Индивидуальные и групповые индикаторы коммутационной панели



Для текущей индикации могут применяться и внешние устройства типа планшетных компьютеров, что весьма выгодно из-за наличия у последних большого цветного дисплея и сенсорной клавиатуры. Взаимодействие с контроллерами осуществляется по радиointерфейсу либо через разъемы mini-USB (в частности, в системе CenterMind от RiT Technologies).

К важным отраслевым достижениям можно отнести начавшееся нормирование в области оптической индикации. Стандартом де-факто стало включение отдельных

индикаторных элементов только парами. Их постоянное свечение означает необходимость соединения портов, тогда как мигающий режим работы отмечает разрываемое соединение.

Решения в области интерконнекта

Внедрение системы интерактивного управления СКС в случае построения коммутационного поля по схеме интерконнекта, весьма привлекательной из-за высокой результирующей плотности портов (выигрыш порядка 20% по сравнению со схемой кроссконнекта), сопряжено с большими сложностями. Эти сложности обусловлены отсутствием даже зачатков стандартизации фактора лицевых панелей коммутаторов за исключением, может быть, использования в качестве интерфейса гнезд модульных разъемов RJ45. В результате установка там датчиков подключения коммутационных шнуров превращается в серьезную инженерную проблему.

Первоначально внедрение СИУ в схему интерконнекта обеспечивалось простым переносом панельных компонентов датчика подключения на лицевую пластину коммутатора. Для этого, как правило, применялась заказная гибкая полоска с соответствующими токоведущими проводниками, которая устанавливалась на штатное рабочее место клеевым способом (в частности, в изделии TE Connectivity). Реже встречается исполнение данного элемента в форме жесткой наклейки (например, в продукции немецкой компании ТКМ).

Очевидные недостатки этих решений побудили специалистов разных компаний искать пути к их устранению. В данной области были проведены большие объемы НИОКР, однако указанная проблема и по сей день полностью не решена. Тем не менее отрасль предлагает потребителям ряд довольно удачных решений.

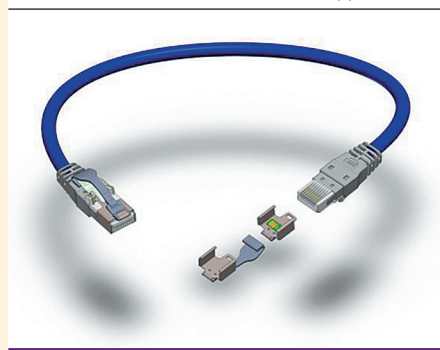
СИУ для схемы интерконнекта делятся на несколько групп, которые на уровне аппаратной части отличаются друг от друга преимуще-

щественно местом расположения датчика подключения шнура к коммутационной панели.

В одном случае осуществляется полный вынос всех элементов датчика подключения на коммутационный шнур (таковы, например, шнуры типа Enhanced Interconnect Patch Cord системы PViQ от Panduit). Само подключение фиксируется по срабатыванию контакта толкателя.

Второе решение основано на вставках в розеточные гнезда коммутатора (система CenterMind компании RiT Technologies, рис. 2). Оно может работать даже с оптическими портами коммутаторов на основе модулей SFP.

Рис. 2. Коммутационный шнур со вставкой-датчиком



Третий вариант представляет собой организатор поддерживающего типа с установленными на нем панельными элементами датчика подключения. В этом случае шнуровая часть датчика выносится с вилки на кабель, а согласование с формфактором лицевой пластины корпуса коммутатора производится за счет гибкости кабеля шнура.

Во всех перечисленных случаях шнур имеет несимметричную форму и может подключаться к коммутатору только одним концом.

В системе PViQ компании Panduit предусмотрена возможность подключения по схеме интерконнекта с использованием симметричного шнура. Для этого коммутационная панель СКС оборудуется дополнительным 25-м портом, через который СИУ взаимодействует с коммутатором ЛВС при активизации рабочего задания. Это позволяет установить однозначную связь между

портами коммутатора и панели и выполнить соответствующее переключение.

Инвентаризация ресурсов

Централизованная база данных СИУ может использоваться для инвентаризации ресурсов информационной системы. Этому способствуют следующие обстоятельства:

- СИУ в процессе функционирования при наличии соответствующих настроек и программных модулей осуществляет сбор данных не только о панелях и их соединениях, но и о коммутаторах и других активных IP-устройствах;
- в базу данных при соответствующей разметке ее полей может быть введена информация о большом количестве самых разнообразных устройств.

Процесс инвентаризации заметно упрощается, если в качестве отчетов используется широко распространенное ПО, например Crystal Report. Одновременно на верхних уровнях информационной системы должны быть произведены соответствующие настройки по обращению к различным базам и формированию сводного отчета.

Упрощение процедур эксплуатации

Одной из проблем СИУ первых поколений была их невысокая дружелюбность к пользователю. Это, в частности, выражалось в сложной схеме передачи информации от оборудования к ответственному специалисту, а процесс ее восприятия, по крайней мере на первых этапах эксплуатации системы, требовал от администратора развитого воображения. Чтобы сделать программный интерфейс СИУ интуитивно понятным, их создатели широко используют наработки из массовых программных продуктов, в том числе привычный интерфейс с типовым расположением окон, иконок и управляющих кнопок и обычные для графических редакторов и САПР комбинации горячих клавиш.

Кроме того, при работе с графическим интерфейсом широко применяется технология *drag and drop*, а само управляющее ПО снабжается развитым набором средств защиты от некорректных действий. Примерами могут служить блокировка попытки прямого соединения оптической и медножильной панелей, запрет на формирование рабочих заданий в случае отсутствия свободных портов или перегрузки шкафа по потребляемой мощности и т.д. На аппаратном уровне шаги в указанном направлении сводятся преимущественно к отказу от соединения по полевой шине RS-485 в пользу IP-сетей. С учетом использования в RS-485 и ЛВС типа Ethernet единого типа разъема RJ45 это эффективно блокирует непреднамеренную ошибку.

Для уменьшения времени реакции системы на запрос вводится понятие сайтов и зон коммутации. Это дает возможность резко снизить количество переборов в процессе анализа БД соединения.



Современные СИУ характеризуются высокой степенью стандартизации основных технических решений и элементов интерактивного управления, что способствует расширению их функциональных возможностей.

В настоящее время СИУ становятся полноправными компонентами информационно-вычислительных систем и берут на себя решение ряда задач нижнего уровня не только собственно ИВС, но и смежных областей инженерного обеспечения, а также технической безопасности.

СИУ могут использоваться не только по прямому назначению, но и для инвентаризации ресурсов физического и более высоких уровней информационной системы предприятия.

Элементы интерактивного взаимодействия с системным администратором становятся все более разнообразными и обеспечивают передачу заметно большего объема информации. ИКС

Поворотные видеокамеры Full HD

Видеокамеры высокой четкости с дистанционным управлением Sony SRG-120DH и Sony SRG-300H предназначены для проведения видеоконференций, дистанционных лекций и семинаров, трансляции событий, телемедицины.

Обе модели способны формировать и передавать изображение с разрешением Full HD с высокой скоростью передачи кадров (1080/60p), оснащены бесшумным механизмом PTZ, стандартными интерфейсами HDMI и могут управляться через сеть с помощью протокола VISCA, посредством команд которого поддерживается до 16 позиций предустановок (регулировка цвета, изменение скорости поворота/наклона и др.). Ко всем функциям камеры полный доступ с интуитивно понятным интерфейсом предоставляется с персонального компьютера.



Высокое качество изображения в камерах серии SRG обеспечено чувствительным сенсором Sony Exmor CMOS. Для обработки изображения задействованы технологии расширения динамического диапазона View-DR и подавления шумов XDNR. View-DR позволяет получить изображение даже при сложных условиях освещения площадки, система XDNR понижает уровень шумов и обеспечивает четкость неподвижных и перемещающихся объектов при плохом освещении. Для неподвижных объектов применяется трехмерное динамическое шумоподавление, для движущихся объектов – двухмерное шумоподавление. В результате изображение сохраняет информативность и детальность в условиях контрастного освещения, а также четкое изображение как подвижных, так и неподвижных объектов при слабом освещении.

Модель SRG-300H может быть установлена как на столе, так и на потолке (есть переключатель перево-

Высокое качество изображения в камерах серии SRG обеспечено чувствительным сенсором Sony Exmor CMOS. Для обработки изображения задействованы технологии расширения дина-



рота изображения). Камера имеет 30-кратный оптический зум в дополнение к 12-кратному цифровому. Разрешение – 800 ТВ-линий (центр). Минимальная освещенность, необходимая для работы камеры, – 1,4 люкс (F 1,6, 50 IRE, 30 fps). Горизонтальный угол обзора – 65°, угол поворота $\pm 170^\circ$, угол наклона $+90/-20^\circ$. Для управления предусмотрены интерфейсы LAN/RS-422 и RS 232 C.

Модель SRG-120DH оснащена 12-кратным оптическим и 12-кратным цифровым зумом. Разрешение – 1000 ТВ-линий (центр). Минимальная освещенность – 1,8 люкс (F 1,8, 50 IRE, 30 fps). Горизонтальный угол обзора – 71°, угол поворота $\pm 100^\circ$, угол наклона – $\pm 25^\circ$. Для управления используется интерфейс LAN/RS 232 C.

В продажу камеры SRG-300H поступят в ноябре, SRG-120DH – в декабре текущего года. В комплект поставки аппаратуры первой модели входит пульт дистанционного управления, сетевой адаптер, VISCA RS-422 соединитель 9P, монтажный комплект для крепления к потолку. Конфигурация аппаратуры SRG-120DH ограничивается пультом дистанционного управления и сетевым адаптером. Пульт дистанционного управления через протокол IP может управлять 112 видеокамерами, в системе можно использовать до пяти контроллеров.

«Сони Электроникс»: www.sonybiz.ru

ИБП с программной адаптацией МОЩНОСТИ

Модульная модификация ИБП Eaton 93PM, предназначенная для серверных комнат и ЦОДов, представляет собой трехфазный ИБП с двойным преобразованием энергии, который может содержать от одного до четырех силовых модулей мощностью 50 кВт (т. е. максимальная мощность одной сборки может достигать 200 кВт). Однако для более тонкой адаптации мощности ИБП к имеющейся нагрузке мощность каждого модуля может быть снижена программными средствами до 40 или 30 кВт. Таким образом можно получить несколько моделей ИБП мощностью 80, 100, 120, 150, 160 и 200 кВт.

Выходной коэффициент мощности ИБП 93PM равен 1, поэтому его реальная мощность равна выходной (50 кВА = 50 кВт). Микропрограммное обеспечение ИБП позволяет подключать в параллель до восьми таких устройств.



В режиме двойного преобразования КПД 93PM – 96,7% (по данным измерений тестовой лаборатории). Начиная с нагрузки 20% КПД этого ИБП превышает 95%, а при нагрузке более 25% становится константой, равной 96,7%, что позволяет не отключать избыточные модули во время работы. В режиме сохранения энергии (ESS, Energy Saver System) заявленный КПД составляет более 99% при нагрузке, превышающей 20%.

ИБП 93PM также характеризуется компактностью (150 кВт мощности помещаются на площади 0,5 кв. м) и простотой обслуживания. Для его установки вплотную к стене разработан специальный короб с вентиляторами, которые выводят горячий воздух вверх.

Продажи в России ИБП 93PM должны начаться в течение осени текущего года.

Eaton:

+7 (495) 981-3770

Высокопроизводительный межсетевой экран

Межсетевой экран нового поколения Altell Neo 340 с функциями UTM (фильтрация трафика, шифрование, обнаружение и предотвращение вторжений, защита от спама и вредоносного ПО, контент-фильтрация) предназначен для защиты информации в крупных территориально распределенных холдингах и центрах обработки данных.

Устройство обеспечивает защиту при больших нагрузках, например при постоянном криптографическом шифровании всего потока данных компании или масштаб-

ной DoS-атаке: производительность межсетевого экрана достигает 18 Гбит/с, скорость шифрования ГОСТ – до 1,4 Гбит/с.

Altell Neo 340 отличается высокой плотностью интерфейсов – до 64 портов RJ45 GbE и SFP GbE или до 16 портов SFP+ 10GbE в восьми модулях в устройстве высотой 2U – и наличием сертификатов ФСТЭК России по классам защищенности межсетевых экранов МЭ2/МЭ3/МЭ4 и уровням отсутствия недекларированных возможностей НДВ2/НДВ3 и ФСБ России по классу защищенности межсетевых экранов МЭ4.

Altell:

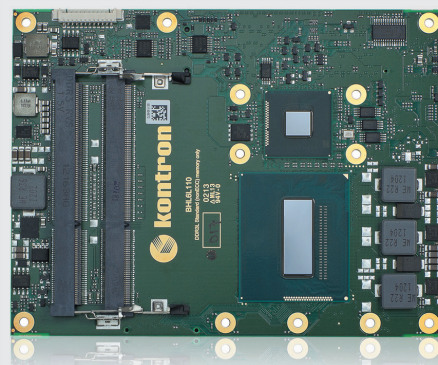
+7 (495) 664-2240



«Компьютер-на-модуле» с повышенной графической производительностью

«Компьютер-на-модуле» COMe-bHL6 производства Kontron поддерживает работу до трех независимых дисплеев с разрешением до 4K (UltraHD) и обладает в два раза более высокой графической производительностью по сравнению с предшественниками.

COMe-bHL6 формата COM Express с распиновкой Type 6 доступен в нескольких исполнениях: от бюджетного варианта на процессоре с низким энергопотреблением до версии с четырехъядерным процессором Intel Core i7 с частотой до 4 x 2,4 ГГц. Модули оснащены чипсетом Intel Mobile QM87, несут до 8 Гбайт оперативной памяти DDR3, семь разъемов PCI Express x1 и один интерфейс PEG x16, совместимы со стандартными устройствами с интерфейсом PCI Express. Периферийные устройства, не требующие большой пропускной способности, могут подключаться через интерфейсы SPI и LPC. Интерфейсная функциональность включает в себя 4 x SATA 3, 1 x Gigabit Ethernet, 4 x USB 3.0, 4 x USB 2.0 и два последовательных порта.



Для вывода графики на несколько дисплеев служат три двухрежимных порта DisplayPort++, обеспечивающих работу с интерфейсами HDMI, DVI и DisplayPort 1.2. Для промышленных приложений будут полезны сторожевой таймер и часы реального времени.

Продукт COMe-bHL6 предназначен для встраиваемых систем промышленного, информационно-развлекательного, медицинского и другого назначения.

«РТСОфт»: +7 (495) 967-1505



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

ARINTEG Тел/факс: (495) 221-2141 E-mail: sales@arinteg.ru www.arinteg.ru с. 19	EMERSON NETWORK POWER Тел.: (495) 981-9811 Факс: (495) 981-9810 E-mail: sales@emerson.com www.emersonnetworkpower.com . с. 77	E-mail: sales@etegro.com www.etegro.com с. 11	KRAFTWAY Тел.: (495) 969-2400 Факс: (495) 645-8087 www.kraftway.ru . . .3-я обл.	RITTAL Тел.: (495) 775-0230 Факс: (495) 775-0239 E-mail: info@rittal.ru www.rittal.ru . . с. 27, 78–79
DATAPRO Тел/факс: (495) 775-7423 E-mail: info@datapro.ru www.datapro.ru . . .4-я обл.	ETEGRO TECHNOLOGIES Тел./факс: (495) 380-0288	ITK Тел.: (495) 780-0038 Факс: (495) 542-2224 E-mail: info@itk-group.ru www.itk-group.ru с. 13	POWERCOM Тел.: (495) 651-6281 Факс: (495) 651-6282 www.pcm.ru с. 60–61	SONY ELECTRONICS Тел.: (495) 258-7667 Факс: (495) 258-7650 www.pro.sony.eu с. 17

Указатель фирм

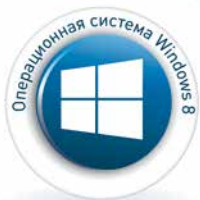
«1С-Битрикс» 57	Invensys pls 14	Surtec 90	«Дом.гу» 18	«ПингВин Софтвр» 57
ABR Investments B.V. 14	Invintel B.V. 14	Swisscom 51	«Емельяников, Попова и партнеры» 52, 67	«Промзаказ» 16
ADT Security Services. 87	IQinVision 87	TE Connectivity 91	«За рулем» 8	ИТ ФГУП «Радиочастотный центр Центрального федерального округа» 8
Agent VI 87	Juniper. 88	Tele2. 12, 17, 62, 63	ИВК 8, 48	«Ратмир Телеком» 14
Allied Telesis 56	JVC 85	Tele2 Russia Holding AB . . . 17	«ИВК-Интернешнл» 8	РАЭК 14
Altell 94	Kontron 94	Tele2 Россия. 14	«Инвенсис Проусесс Системс» 14	Банк «Россия» 62
ALTIUS 74	Kraftway 70	TeleCore 76	«Инлайн Групп» 72	«Ростелеком» 12, 14, 16, 30, 33, 41, 62, 63, 72, 89
Appercut Security. 25	Lenel. 87	Telefonica 52	«Информационные спутниковые системы» им. М. Ф. Решетнева» 21	«РТСофт» 94
Apple 32	LETA 26	Telenor. 62	«Инфосистемы Джет» . . . 19, 26	«Русславбанк» 76
AT Consulting. 58	Mail.Ru Group 16, 63	Telstra 51	«КиноПоиск» 63	ФГУП РТРС 21
Autodesk 14	Marvell 89	Thales Alenia Space. 21	ГК «Компьюлинк» 76	РЦТО ККТ 14
AXIS 85, 87	Maxiten Co Limited 63	T-Systems CIS 57	ФГУП «Космическая связь» 16, 20	Сбербанк 73
B2B International 25	MAYKOR 14, 61	Tyco Integrated Security . . . 87	КРОК 58	«Связной» 12
BigSwitch 89	Microsoft. 28, 35, 43, 65, 70, 88	Unify 12	«Лаборатория Касперского» 16, 25	«Северсталь» 62
Bosch 85	Motorola 19	Universum Space Technologies 21	«Леги» 43	«Сеть компьютерных клиник» 61
British Airways 14	NEC 89	Uptime Institute. . 9, 10, 73, 80	ЛНТ 14	СибЦККТ. 14
Brocade 89	Nedap 85	Verint Systems 86	МГТС 16	АФК «Система» 62
Cannon 75	Netbynet 14	Verizon 51	МГУ им. М.В. Ломоносова . 15	«Скартел» 63
CDNvideo 88	NICE Systems 85	VMware 17, 57, 88	«Мегафон» 1, 13, 14, 30, 33, 63	«СмартЛабс». 16
Check Point Software Technologies 68	Nicira 88	Xtralis 30, 63, 67	«Медицина» 8, 54	СМП Банк 26
Cisco. 14, 24, 51, 66, 88	Nokia 88	Yota 30, 63, 67	ГУЗ особого типа ВО	«Собинбанк». 63
Citrix 32	NTT 88	«Аванпост». 19	«Медицинский информационно-аналитический центр» . . 8, 49	«Сони Электроникс». 93
Compendium. 14	Optima Consulting 57	«Авантаж» 18	Медицинский информационно-аналитический центр РАМН. . 44	«Т2 Рус Холдинг». 17
DataSpace 16, 73	Oracle 14	«Авиастар-СП». 19	«Медлайнсофт» 56	«ТАНА – телемедицинские системы» 8
EADS Astrium. 20	Orange. 51	«АйТи». 32, 43	ГК «Медси» 55	«Телеком-Монтаж». 75
Eaton 94	Orsus 85	«АКАДО Телеком» 55	МТС 1, 12, 13, 16, 33, 41, 43, 62	Технический центр
Echopass. 14	Panduit. 90	«Аладдин Р. Д.» 53	МТС-Банк 63	Интернет 16
EMC 18	Pelco by Schneider Electric . 85	«Арамо-Системы» 84	МТП 30	«Техносерв Консалтинг» . . . 59
Emerson Network Power . . . 77	Phonebloks. 19	«АрселорМиттал Темиртау» 18	НПО «Национальное телемедицинское агенство» . 8	«ТехноСерв Тянь-Шань» . . . 12
EPSP 1	Ponemon Institute 25	Ассоциация организаций оборонно-промышленного комплекса – производителей медицинских изделий и оборудования 51	«Нерюнгри телеком» 33	«Техносерв» 18, 75
Esri CIS 59	Powercom 60	Ассоциация развития медицинских информационных технологий 47	ФГУП НИИР 21	«Триколор ТВ» 12
Eutelsat 21	Pronto 89	«Аэрофлот» 75	«Новая телефонная компания» 33	ТТК 12, 18, 33
Extreme Networks 89	Proximex 87	БЕЛТЕЛ 18	«ОМНИ-ТО» 14	«УЗ Промсвязь» 16
Gaika Group 28	RiT Technologies . . 18, 91, 92	Бюро медицинской статистики . 8	«Оргтехносервис» 14	УК «Финам Менеджмент» . . . 62
Garsdale Services	R-Style. 74	«Восточный Экспресс банк» . 16	«Орион-Экспресс». 33	«Фуджифильм-РО» 56
Investment Limited 63	RU-CERT. 16	ВТБ 17	«Открытые технологии». . 18, 58	ЦНИИ организации и информатизации здравоохранения 45
Gartner. 66	Samsung 32	ВТИ 14	НКО «Открытый город» . . . 28	ЦНИИС 13
Genesys 14	SAP CHG 14	«ВымпелКом» . . . 12, 13, 16, 30, 33, 62	«Первый канал» 21	«ЦРТ-Сервис» 61
Google 28, 65, 89	Saudi Aramco 10	НИУ ВШЭ 14		«Экспресс сеть» 33
Graitec. 14	Schneider Electric SA . . . 14	«Гелиос-ТВ» 33		«Электронная Москва». . . 74
Group-IB 16	Siemens Enterprise Communications 12	«Датадом» 80		«Энергия САТ» 20
Honeywell 85	Simplex Grinnell 85			«Яндекс». 16, 63
Hosting Community. 89	Skype 85			
HP 89	Sony 85, 93			
Huawei. 12	Sourcefire 14			
IBM 46, 64, 65, 85, 89	SPIRIT 57			
IBS 58, 74	Staples. 14			
InfoWatch 25, 53				
Intel 15, 70				

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.



Kraftway рекомендует Windows 8.

ВАШИ ДАННЫЕ ПОД ЗАЩИТОЙ

Новый защищенный моноблок Kraftway Studio KM64 с интегрированными в BIOS средствами защиты информации предназначен для использования в государственных и корпоративных информационных системах.

На моноблок на базе процессора **Intel® Core™ i5** устанавливается операционная система **Windows 8**.

Узнайте больше на **www.kraftway.ru**





**РЕШЕНИЕ
ЛЮБЫХ ЗАДАЧ**
SOLUTION FOR EVERY CHALLENGE

www.datapro.ru