Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 9 (207)/2010

Слияние операторов связи

КОРПОРАТИВНЫЕ СИСТЕМЫ

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года

Редакция:

Дмитриев В.Ю.
vlad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

Слободчикова Т.А.
slobodchikova@jet.msk.su

Шедова Е.Л.
eshedova@jet.msk.su

Верстка:
Кулешова Ю.В.

Корректура:
Андрушко О.Ю.

Над номером работали:
Андронов С. Ю.
Баталова Н.В.
Виняр Д.Л.

Издатель:
Компания «Инфосистемы Джет»

Контакты:
тел. (495) 411 76 01
http://www.jetinfo.ru

От редакции

Динамично развивающийся рынок операторов связи даже в кризисные годы показал неплохие результаты. И хотя активность игроков несколько снизилась, компании продолжали вести завоевательные войны, позволяющие в случае победы получить лакомый кусочек — один из сегментов рынка. Тактика и стратегия в этих баталиях могут быть разными: выпуск новых продуктов и услуг, выгодные партнерства, удачные инвестиции и т.д. Одним из довольно распространенных способов среди крупных игроков является поглощение других компаний.

Слияние — довольно выгодный метод с точки зрения расширения своих владений на рынке связи, поскольку позволяет получить как финансовые, так и технологические преференции. Правда есть один нюанс — никогда не знаешь с какими сложностями при этом придется столкнуться и что выиграешь в финале, если вообще удастся до него добраться (примеров схода с дистанции задолго до финишной черты более чем достаточно). Исходя из этих соображений и опираясь на свой опыт участия в подобных проектах, мы решили обозначить наиболее распространенные проблемы процесса объединения операторов связи и наметить варианты их решений. Всех нюансов нам, конечно же, не учесть, но выявить закономерности и помочь минимизировать последствия их разрушительной деятельности вполне под силу.

Помимо непростых вопросов слияния компаний в сентябрьском выпуске дебютная рубрика «Реальная безопасность» посвящена современным средствам защиты для рынка телеком-операторов. О способах защиты от злоумышленников нам рассказала Наталья Баталова, руководитель направления по работе с телекоммуникационными компаниями центра информационной безопасности компании «Инфосистемы Джет».

А ставший уже традиционным «Собеседник» на этот раз встретился с Сергеем Роговым, ИТ-директором группы компаний «Детский мир», который поделился секретом успеха в разработке ИТ-стратегии компании.

СОДЕРЖАНИЕ

ИНДЭКС-БАНК – направление на централизацию

Компания «Инфосистемы Джет» завершила проект по созданию консолидированного центра обработки данных в ИНДЭКС-БАНКе.

Системы управления распределенным вычислительным комплексом и взаимодействия филиалов с центральным офисом со временем требуют модернизации. Это и послужило причиной старта в ИНДЭКС-БАНКе проекта по объединению АБС филиалов на единой вычислительной платформе, которая позволила бы консолидировать базу данных клиентов и счетов в АБС центрального офиса, а также оптимизировала процесс информационного взаимодействия внутри компании.

Руководство Банка приняло решение о построении консолидированного центра обработки данных – высокодоступной платформы для развертывания и функционирования единой АБС. По итогам тендера исполнителем проекта была выбрана компания «Инфосистемы Джет».

Специалисты компании «Инфосистемы Джет» построили распределенный центр обработки данных. Наличие двух территориально удаленных друг от друга площадок: основной и резервной позволяет предотвратить сбои в работе АБС в случае наступления чрезвычайной ситуации на одной из площадок.

Проект состоял из двух этапов: построение и запуск основной площадки, а затем развертывание комплекса резервной, с включением катастрофоустойчивого режима работы распределенного ЦОД. На каждой из площадок размещены вычислительные мощности и система хранения. Развернуто проектное решение по обеспечению доступности построенной системы.

Следующим этапом развития проекта станет постепенный перевод баз данных, счетов и сведений о клиентах на единую платформу с настройкой удаленного доступа к централизованной автоматизированной банковской системе.

В результате Банк получил современное масштабируемое решение для консолидации АБС филиалов, которое позволит «обслуживать» централизованную автоматизированную банковскую систему и оптимизирует процессы взаимодействия внутри финансовой организации.

«Надежный современный центр обработки данных – это завтрашняя гарантия стабильного функционирования банка и непрерывности оказания услуг своим клиентам, – комментирует **директор департамента организационного, проектного и процессного управления ПАО «ИНДЭКС-БАНК» Дмитрий Нечитайло**. – *Основываясь на высоких стандартах европейских банков к построению ИТ-инфраструктуры ЦОД, проектной группой ПАО «ИНДЭКС-БАНК» был проведен детальный анализ существующих решений на рынке услуг построения дата-центров. Как следствие, для реализации проекта выбор был сделан в пользу решения компании «Инфосистемы Джет», имеющей опыт внедрения подобных проектов в СНГ и располагающей штатом высококвалифицированных специалистов».*

«Проект построения ЦОД в ИНДЭКС-БАНКе – это первое решение такого масштаба, выполненное нами в Украине, – комментирует **коммерческий директор компании «Инфосистемы Джет, Украина» Александр Зачешигрива**. – *Созданный центр обработки данных состоит из двух площадок, которые находятся в разных концах города. Это позволяет обеспечить катастрофоустойчивость всего решения – защитить АБС банка от пожара или от перебоев с питанием на одной площадке, а также от ошибок, связанных с так называемым «человеческим фактором».*

В настоящее время построенный комплекс находится на технической поддержке у компании «Инфосистемы Джет».

«Пробизнесбанк» передал на аутсорсинг компании «Инфосистемы Джет» администрирование ИТ-инфраструктуры

ОАО АКБ «Пробизнесбанк» и компания «Инфосистемы Джет» заключили контракт сроком на 5 лет на предоставление услуг по аутсорсингу: администрирование ИТ-инфраструктуры АБС и системы Интернет-банкинга «Интербанк». Работа строится на базе соглашения SLA и детальном регламенте взаимодействия ИТ-команд банка и интегратора. Специалисты ИТ-службы банка избавились от рутинных эксплуатационных процедур и теперь могут сосредоточиться на решении стратегических задач, связанных с развитием бизнеса.

«Пробизнесбанк» является центральным банком финансовой группы «Лайф», которая объединяет в настоящее время семь банков по всей России. Вследствие развития группы и увеличения нагрузки на системы банку стало не хватать собственных ресурсов для обслуживания ИТ-инфраструктуры. «Мы произвели анализ и тщательные подсчеты и пришли к выводу: расходы на собственный штат специалистов по поддержке и администрированию будут значительно выше, чем в случае привлечения внешнего эксперта», — сообщает **Дмитрий Межов, заместитель начальника департамента ИТ ОАО АКБ «Пробизнесбанк»**.

Банк и интегратор уже имели опыт успешного сотрудничества в проекте по созданию ИТ-инфраструктуры для функционирования системы «Интербанк». Благодаря наличию внушительного портфолио подобных проектов и совместному опыту работы именно специалистам компании «Инфосистемы Джет» было доверено взять на аутсорсинг администрирование вычислительных мощностей системы «Интербанк» и АБС «Пробизнесбанка». ИТ-инфраструктура банка построена на базе оборудования IBM, R-Style и других производителей.

Специалисты компании «Инфосистемы Джет» провели первичный аудит ИТ-инфраструктуры заказчика и проанализировали работу ключевых бизнес-систем. На основе выявленных особенностей и требований заказчика было разработано соглашение SLA, по которому допустимое время простоя компонентов инфраструктурных подсистем составляет от 1 до 8 часов в зависимости от степени критичности работы прикладного ПО. Короткие сроки восстановления в случае сбоя гарантируют стабильную работу бизнес-систем банка и обеспечивают их функционирование в соответствии с лучшими мировыми практиками.

Для успешного сотрудничества проектная команда из специалистов обеих компаний разработала детальный регламент взаимодействия, описывающий все зоны ответственности, порядок действий при решении рабочих вопросов и т.п.

«Обратившись к специалистам сервисного центра компании «Инфосистемы Джет», мы избавились от ряда эксплуатационных проблем, получив необходимый результат — стабильно работающие системы, — подчеркнул **Дмитрий Межов**. — *Теперь мы можем сосредоточиться на новой задаче — модернизации ИТ-инфраструктуры с целью увеличения мощности, эффективности и надежности работы наших информационных систем».*

«Для успешно растущей банковской группы очень важно обеспечить поддержку со стороны ИТ. От непрерывной работы ИТ-инфраструктуры напрямую зависит возможность и качество оказания услуг клиентам. Накопленный в подобных проектах опыт позволяет нам быть уверенными в соблюдении всех обязательств договора. Мы готовы обеспечить высокий уровень стабильности работы систем на данном этапе и поддерживать банк в его дальнейшем развитии», — сообщил **Андрей Гешель, руководитель сервисного центра компании «Инфосистемы Джет»**.

Интернет-коммуникации в Евразийском банке под защитой DLP-технологий

В Евразийском банке, одном из крупнейших банков Казахстана, завершен проект по внедрению системы контроля утечек информации на основе Symantec DLP 10.0.

Для крупных банков, каким является Евразийский банк, вопросы предотвращения негативных последствий от информационных утечек и минимизации репутационных рисков являются одними из наиболее приоритетных. В этой связи руководство банка приняло решение усовершенствовать процессы контроля Интернет-коммуникаций. Для решения этой задачи была приглашена компания «Инфосистемы Джет».

В качестве системы предотвращения утечки данных (DLP, Data Loss Prevention) был выбран программный продукт Symantec DLP 10.0 (SDLP). Система позволяет наилучшим образом фиксировать и предотвращать утечку конфиденциальной

информации в режиме реального времени, а также обладает возможностью регистрации и расследования возникающих инцидентов.

«В финансовом секторе вопрос информационной безопасности не терпит компромиссных решений, ведь предметом защиты является не только информация, но и репутация банка, и интересы клиентов. Новое решение, основанное на технологиях DLP, в полной мере позволяет нам соответствовать статусу самого надежного банка Казахстана[1]», — комментирует **Сергей Тимофеевич Глущенко, исполнительный директор АО «Евразийский банк»**.

«9 из 10 ведущих коммерческих и инвестиционных банков мира используют решение Symantec DLP. Мы рады наблюдать, что сегодня ведущие отечественные компании, такие как Евразийский банк, перенимают лучшие мировые практики в области защиты конфиденциальных данных» — отметил **Александр Якунин, региональный менеджер Symantec в Казахстане, Средней Азии и Закавказье**.

«Объединив возможности решения Symantec DLP 10.0 и опыт специалистов компании «Инфосистемы Джет», мы обеспечили Евразийскому банку высокий уровень защиты информации, — комментирует **Кирилл Викторов, заместитель директора по развитию бизнеса компании «Инфосистемы Джет»**. — *Залогом успешного внедрения стала заинтересованность в проекте руководства банка и активное участие квалифицированной команды со стороны банка».*

Компания «Инфосистемы Джет» расширяет свои компетенции по программным продуктам IBM

Компания «Инфосистемы Джет» получила статус авторизованного партнера IBM по СУБД DB2. На данный момент компания обладает высшим партнерским статусом IBM Premier Partner, в рамках которого авторизована по восьми программным продуктам: Internet Service Security, Tivoli Business Automation, Tivoli Enterprise Asset Management, Tivoli Security, WebSphere BPM, WebSphere Core, Information Management Data, DB2.

В настоящее время количество проектов, реализуемых на базе СУБД IBM DB2, на российском рынке увеличивается. Компания «Инфосистемы Джет» планирует наращивать свои компетенции по DB2 и получать расширенные технические сертификации.

Microsoft расширяет рамки сотрудничества с Polycom в сфере объединенных коммуникаций

Microsoft и Polycom заключили долгосрочное стратегическое соглашение о совместной деятельности и разработке решений в области объединенных коммуникаций (Unified Communications - UC). В рамках этого соглашения компании планируют выпустить полностью интегрированные, базирующиеся на UC-стандартах решения, которые будут отвечать потребностям крупных предприятий, среднего и малого бизнеса, а также государственных организаций. UC-решения объединят в себе программные и аппаратные продукты, сетевые технологии и сервисы, которые позволяют заказчикам увеличить эффективность бизнеса при сокращении расходов на командировки, закупку и обслуживание телекоммуникационного оборудования.

У Microsoft и Polycom общий подход к созданию высокопроизводительных бизнес-решений. В его основе лежат общепринятые стандарты и платформы, а также знакомые пользователям инструменты. Расширение сотрудничества двух компаний — это большой шаг вперед к ускорению развития системы объединенных коммуникаций.

Экспертное мнение

Константин Ваксин, старший инженер в группе внедрения голосовых решений: «Партнерство компаний Microsoft и Polycom позволяет получить более широкие возможности по организации видео-конференций и теле-презентаций в формате HD. Проводить их из любой точки мира и «подключать» к обсуждению своих коллег, находящихся в офисе, что, несомненно, не может не радовать конечного заказчика. Данные возможности наилучшим образом помогают оптимизировать решение вопросов, связанных с коммуникациями как внутри самой компании, так и с партнерами по бизнесу за ее пределами».

1 По мнению авторитетного международного издания Euromoney, Евразийский банк был признан «Самым надежным банком в Казахстане» (Best Managed Banks 2009. Most Reliable Bank in Kazakhstan).

NetApp и Symantec – сотрудничество для повышения эффективности информационных систем клиентов

Компания NetApp (NASDAQ: NTAP) объявила об интеграции собственных унифицированных систем хранения данных и решения Thin Reclamation API компании Symantec. Это поможет пользователям SAN автоматически реинициализировать неиспользуемые ресурсы систем хранения данных, а также повысит эффективность работы СХД в целом. Интеграция технологий NetApp и Symantec помогает заказчикам более эффективно управлять хранением данных, реинициализировать неиспользуемые ресурсы на протяжении всего цикла работы с информацией, а также снижать затраты на организацию информационных систем и управление ими.

Использование технологий NetApp в сочетании с простотой и гибкостью ПО Veritas™ Storage Foundation компании Symantec облегчает управление средами SAN и сокращает затраты на энергоснабжение, охлаждение и содержание помещений центров обработки данных. Благодаря сотрудничеству компаний NetApp и Symantec пользователям СХД будет проще планировать использование системы, выделение ресурсов для хранения данных, а также реинициализацию неиспользуемых ресурсов.

NetApp, Cisco и VMware создали комплексное решение FCoE для динамических центров обработки данных

В рамках своего сотрудничества компании Cisco, NetApp и VMware объявили о выходе первого в отрасли сертифицированного комплексного решения FCoE (Fibre Channel over Ethernet) для виртуальной среды VMware. Совместный программный продукт полностью поддерживает технологию FcoE, сокращает количество необходимых кабелей и устройств и помогает консолидировать, виртуализировать и автоматизировать центры обработки данных (ЦОД). Коммутаторы Cisco для ЦОД и системы хранения NetApp® FCoE успешно прошли сертификацию VMware на поддержку виртуализированной среды VMware. Это событие стало важным этапом в распространении протокола FcoE, который помогает заказчикам повышать эффективность динамических центров обработки данных и развивать облачные вычисления.

СТАТИСТИКА

Динамика российского телеком-рынка

2009 год — второй год кризиса, ощутимо сказался на российском рынке телекоммуникаций. Операторы недополучили запланированную выручку, скорректировали инвестиционную политику и заняли выжидательную позицию в отношении сделок слияний и поглощений. Динамика рынка снизилась.

Планы большинства отечественных операторов на 2009 год были серьезно пересмотрены в контексте негативной экономической ситуации в стране и в мире. Как и на другие отрасли российской экономики, на телеком повлияло изменение курсов национальной валюты по отношению к доллару и евро, сложности с кредитованием под проекты модернизации и развития, снижение спроса на ряд услуг как в корпоративном, так и в частном секторе.

Неизбежные колебания

Ушедший год оказал предсказуемо серьезное влияние на динамику роста выручки телеком-операторов. Кроме того, по итогам 2009 г. появилось несколько новых игроков взамен ушедших с рынка. Среди последних — оператор «Сахателеком», купленный «Дальсвязью» в октябре 2009 года.

Громкие «новички» рейтинга — один из активных региональных игроков рынка ШПД, компания «Мультирегион», а также «Скартел» — отечественный WiMAX-оператор, работающий под торговой маркой «Yota». Последний стал одним из главных ньюсмейкером рынка беспроводного ШПД в двух столицах в прошлом году.

Ситуация в российской отрасли связи по итогам 2010 года будет в любом случае отличаться от той, что наблюдалась в «переходные» 2008 и 2009 гг. Реорганизация «Связьинвеста» приведет с большой вероятностью к появлению крупного государственного телеком-оператора, который явно займет одно из лидирующих мест. Сотовые операторы, вышедшие на рынок конвергентных услуг, вероятно, продолжат приобретение региональных активов. Спутниковые операторы связи в 2010 году могут сохранить операционную устойчивость за счет развития проектов цифрового вещания, а также им на пользу пойдет по-прежнему недостаточное покрытие России магистральными каналами. Прогнозируемый Минэкономразвития рост отрасли может составить в 2010 г. около 9%.

Подготовлено по материалам Cnews Analitics (http://www.cnews.ru/reviews/free/telecom2010/)

Некоторые аспекты слияния операторов связи

Сергей Андронов,
директор департамента проектирования, внедрения и сопровождения компании «Инфосистемы Джет»

Даниил Виняр,
руководитель группы перспективных разработок департамента проектирования, внедрения и сопровождения компании «Инфосистемы Джет»

Построение сетей связи, с одной стороны, требует от операторов больших финансовых затрат, а с другой — построенные сети или сооружения, как правило, имеют избыточный ресурс и требуют значительных капитальных вложений. Эти два фактора подталкивают компании к сотрудничеству или слиянию.

Основная цель объединения всегда связана с повышением эффективности функционирования оператора — увеличение доли рынка, прибыли и т.д. Ее достижение не решается исключительно финансовыми средствами. В этом процессе нужно учитывать множество нюансов: организационных, технических и, собственно, финансовых.

Любое слияние — не типовая и нештатная ситуация для любой компании, по этой причине оно всегда сопряжено с различного вида сложностями. Поэтому основные задачи при интеграции: быть психологически готовым к тому, что придется помимо стандартных эксплуатационных процедур заниматься еще и решением нетиповых для повседневной жизни трудностей, понимать основные опасности, которые оно за собой влечет. Лучшей подготовкой к объединению является анализ как мирового опыта, так и опыта российских компаний, прошедших через этот процесс. Использование такого рода наработок позволит получить некий набор сценариев, который поможет выйти из сложной ситуации с наименьшими потерями.

В данной статье, исходя из своего опыта работы на проектах слияния операторов, мы попытаемся обозначить наиболее распространенные проблемы при слиянии и пути их решения.

Организационные проблемы

Как и в любой другой области в процессе объединения операторов есть своя специфика. С точки зрения техники это касается биллинговых систем, доступа пользователей, магистральных компонентов инфраструктуры, систем бэк-офиса. К тому же есть целый ряд организационных сложностей, с которыми можно столкнуться. Компании не являются организационными копиями друг друга, из-за чего при их интеграции возникает ворох проблем.

Начнем по порядку. Чаще всего причиной объединения двух операторов и движущей силой данного процесса служат исключительно финансовые соображения — получение дополнительной прибыли. Но мало кто задумывается о том, что продуманная и проработанная стратегия в части создания оргструктуры при объединении может существенным образом облегчить эту непростую для обеих компаний процедуру. Такой подход позволит избежать сложностей, в том числе технического и технологического плана, таких как пересекающиеся лицензии на междугородную/международную связь, пересекающиеся инфраструктуры, прикладные сервисы, офисные приложения, а также службы, которые все это эксплуатируют. Никому до сих пор не известно, как в процессе слияния решать подобные проблемы. А ведь они в первую очередь носят исключительно организационный характер.

Организация эксплуатации

Менеджмент объединенной компании сталкивается с трудностями организации эксплуатации. Если технические вопросы на уровне ИТ-инфраструктуры решаются путем оптимального использования имеющихся технических средств с применением опыта best practice, то организация служб эксплуатации — очень сложный процесс. В ряде случаев выбор одного отдела на эту роль из двух объединяющихся компаний базируется на том, которое из подразделений сможет лучше обосновать свою нужность и значимость. Подобная ситуация довольно типична и довольно ошибочна с организационной точки зрения. Она ведет к внутренним неурядицам, неразберихе, влекущих за собой простой ИТ-систем.

Организационные проблемы оказывают прямое влияние на работу информационных систем и являются одними из самых распространенных причин снижения динамики развития, а то и полной его остановки. Последствия столь непростительных упущений приводят к увеличению периода нестабильности и как следствие — к потерям доли рынка.

Залог успеха в том, чтобы при слиянии синхронно друг за другом следовало множество процессов, начиная от формулирования различных требований для построения/оптимизации объединенной инфраструктуры, проведения тендера, реализации проекта, заканчивая передачей комплекса в эксплуатацию. Но до тех пор, пока не сложится нормальной оргструктуры, синхронизировать данное n-количество процессов фактически невозможно. Самим операторам довольно непросто подготовиться и провести все необходимые изменения в структуре компании. Для наибольшей эффективности стоит приглашать сторонних консультантов, которые смогут проконтролировать разработку новой бизнес-модели компании с учетом объединяющихся оргструктур и вовремя предостеречь от возможных ошибок.

Кадровый вопрос: а был ли мальчик?

Объединение в большинстве случаев сопровождается кадровыми сокращениями. При отсутствии продуманной кадровой политики сотрудники внутри интегрирующихся компаний перестают выполнять свои обязанности и концентрируются на демонстрации своей значимости и незаменимости в новом рабочем процессе. Здесь каждый пытается отстоять себя. В этой борьбе в ход идут самые разнообразные деструктивные методы, такие как саботаж, итальянская забастовка[1], шантаж руководства (например, отказ передавать необходимые пароли). Стоит отметить, что из года в года способы диверсии становятся все более продуманными. Разработка противодействующих мер занимает достаточно много времени, отвлекая компанию от интеграционных процессов, тем самым увеличивая сроки слияния.

Причины происходящего, как правило, скрываются в отсутствии у людей информации о стратегии развития, о тактических задачах, в реализации которых они принимают участие. Решение о слиянии принимается на уровне финансовых подразделений, которые не задумываются о заблаговременной подготовке персонала и технических служб. Для всех сотрудников компании, кроме финансового отдела и топ-менеджмента, слияние — это скорее наступающие последствия, чем продуманный шаг. А точнее, гром среди ясного неба.

Чтобы избежать описанных выше неурядиц, специалисты обоих операторов должны четко понимать свое место в объединенной компании, цель, к которой они идут, и организационную структуру, в которой им предстоит работать. Безусловно, подобные процессы не могут обойтись без плановых сокращений. Хотелось бы подчеркнуть, что решение о сокращении должно

1 Итальянская забастовка — также наз. обструкция — форма протеста наряду с забастовкой и саботажем, заключающаяся в предельно строгом исполнении сотрудниками предприятия своих должностных обязанностей и правил, ни на шаг не отступая от них и ни на шаг не выходя за их пределы. Иногда итальянскую забастовку называют работой по правилам (англ. Work-to-rule).

быть не просто принято, а в довольно сжатые сроки реализовано. В противном случае сотрудники, оказавшись в «подвешенном состоянии» в уже объединенной компании, наверняка станут зачинщиками диверсий, конфликтов и т.д. Надо сказать, что наиболее опасны не прямые, а косвенные диверсии, которые выражаются в попытках остановки функционирования систем. По опыту наших проектов, наиболее частым случаем является размещение в системе, так сказать напоследок, «бомбы замедленного действия» — определенного набора закладок, которая срабатывает, например, при изменении конфигураций сети новым владельцем. Итог — сбой системы, причем масштаб последствий напрямую зависит от ее уровня критичности.

Именно поэтому организационный характер проблем наиболее травматичен для объединяющейся компании. Его следствием как раз и становятся те технические сложности, речь о которых пойдет далее.

Технические аспекты

Особенности интеграции сетей

Не секрет, что все ИТ-структуры операторов состоят из определенных сегментов: транспортная и магистральная сеть, GSM-часть, «последняя миля» для проводных операторов. С точки зрения «последней мили», особенно если компании работают на разных сегментах рынка, при слиянии особых изменений не происходит. От их объединения пользовательские сервисы существенным образом не меняются, напротив лишь увеличивается спектр услуг. Что касается магистральной части — с нее обычно начинают оптимизацию. Основная задача состоит в том, чтобы объединенная магистраль была готова предоставлять расширенный набор сервисов. Параметры KPI (функциональность сети, параметры ее управления, эксплуатационные расходы и т.д.) не должны быть потеряны, а наоборот — расширены с учетом всех сервисов объединяемых компаний. Именно с этой части технической интеграции начинаются всевозможные сложности.

Они могут быть как на уровне вендоров, потому что магистрали, как правило, построены на оборудовании разных производителей, так и на уровне технологий. Вопрос решается не только о том, какого вендора оставить, но и чью сеть сохранять. Например, не всегда необходимо отказываться от одной сети в пользу другой. В ряде случаев возможно сохранение обоих сетевых сегментов, если компании работали на разных рынках — магистрали могут быть не пересекающимися и эксплуатироваться параллельно.

Критерии информационной безопасности

Проблемы существуют и на уровне ИТ-безопасности. У каждой организации до слияния есть свои — отличные друг от друга политики информационной безопасности. Их не всегда можно интегрировать друг с другом, поскольку они могут быть диаметрально противоположными. В случае объединения потребуется выполнить определенный набор как проектных изысканий, так и технических внедрений для разработки единой политики безопасности объединенной компании. Несмотря на все предосторожности и продуманные шаги, возникает довольно большое количество «дыр», а также инцидентов ИБ. Основная опасность — внешние риски, связанные со злоумышленниками, которые целенаправленно могут использовать факт слияния компаний как уязвимость для проникновения к внутренним ресурсам или организации диверсии.

Вторым источником угроз становятся информационные потери, к которым приводит деятельность самих сотрудников компании. Указанная деятельность может быть как случайной, так и целенаправленной, а потери — как восполнимые, так и невосполнимые.

Основной механизм минимизации рисков ИБ при слиянии компаний — использование методов плавной интеграции с поэтапным устранением возникающих «дыр» и инцидентов ИБ.

Уровни критичности систем

В объединяющихся компаниях может быть разный уровень критичности одних и тех же систем. При неправильном подходе к построению плана устранения неполадок и процессов резервирования важность процессов восстановления тех или иных систем не будет донесена до служб, их эксплуатирующих. Велика вероятность того, что в отсутствии должного информирования сотрудники попросту не будут оперативно реагировать на аварийные ситуации, действуя согласно планам по уровням критичности, установленным в их организации до объединения. Из-за общей несогласованности некоторые процессы или сервисы в новой компании могут быть остановлены на довольно длительное время. Это в свою очередь слу-

жит причиной различного рода издержек. Период нестабильности увеличивается.

Недопущение таких подходов обеспечивается созданием единого информационного пространства для всех специалистов организации, в котором уровень критичности систем является одинаковым для понимания каждого ее сотрудника.

Особенности интеграции бэк-офиса

Ни один оператор связи не обходится без бэк-офиса — прикладных систем, на которых выполняется основная обработка информации пользователей: бухгалтерские операции, кадровые системы, CRM, системы отчетности, оформления заявок, модернизации и развития сети. Когда организации объединяются, как правило, все названные выше функции дублируются. Такое «клонирование» систем на разных аппаратно-программных средствах приводит к потере информации (в одной системе есть данные о поставке, в другой — нет), утрате ее достоверности.

Немаловажным при слиянии будет обратить пристальное внимание на интеграционную часть бэк-офиса, в целях его оптимизации и минимизации повторяющихся процедур. Иначе процессы недостоверности данных приведут к крупным финансовым потерям.

Последовательность процессов интеграции

В большинстве случаев все эти проблемы обязаны отнюдь не техническому происхождению, а организационно-информационному характеру. Поэтому необходимо тщательно продумывать всю процедуры интеграции компаний, начиная с вопросов организации, заканчивая разработкой плана последовательности внедрения интеграционных процессов. Зачастую не существует универсального плана проведения интеграционных процедур, но не стоит подходить к решению этого вопроса с нуля. Наличие достаточно большой базы аналогичных материалов в мировой практике позволяет оптимально кастомизировать план объединения с учетом всех особенностей двух компаний. В большинстве случаев при его составлении выпадает ключевой, на наш взгляд, аспект, который оказывает существенное влияние на работу нового оператора — внутренняя культура каждой из компаний.

У каждого оператора до объединения по-своему происходили различные процессы: эксплуатация текущей инфраструктуры, принятие решений, их выполнение. Когда организации сливаются, это не просто объединение людей, технологий, но и культур, причем весьма непростое и зачастую конфликтное. Все операторы связи в РФ уникальные — они исторически по-разному развивались, а потому у каждого сложились свои традиции абсолютно во всех сферах их повседневной деятельности. Так одним и тем же термином компании могут обозначать совершенно разные структуры. Для одних 1С — бухгалтерия, для других — биллинг. Соответственно, степени критичности простаивания данных систем разные. С этой терминологией постоянно возникает путаница. Поэтому консультантам каждый раз приходится принимать терминологию двух разных сторон и работать медиатором, чтобы объяснять, почему они, сидя за одним столом, произнося одни и те же слова, не понимают друг друга.

Еще один пример — взаимоотношения между департаментами. Взять хотя бы процедуру закупок оборудования. В обеих компаниях она происходила по разному, а сейчас — должна идти по некому единому сценарию. Зачастую оказывается, что в новой структуре присутствует целый пласт людей, не знакомых с новыми правилами и действующих по-старому. Время выполнения задач увеличивается, происходит снижение динамики объединения, и как результат — потеря информации, недополучение коммерческой выгоды.

Для того чтобы новые процессы в объединенной компании заработали настолько же хорошо, насколько это было в каждой из них по отдельности, сначала должно произойти организационное слияние по департаментам и оргструктурам обоих операторов. Только после этого возможно выстраивание новых бизнес-процессов. До тех пор пока структура «шатается», а при объединении в течение длительного времени всегда так и происходит, все процессы нестабильны, и в большинстве случаев они «подвисают».

По нашей оценке, если выравнивание на уровне организационных структур, на уровне политик, процедур, эксплуатационных процессов происходит больше года, можно с уверенностью говорить, что интеграция в целом не состоялась. Объединенную компанию будет «лихорадить» еще достаточно продолжительное время и с разной интенсивностью.

Экономическая эффективность

Одним из критериев эффективности слияния операторов является экономическая оценка — сопоставление той недополученной прибыли с момента слияния (прибыль, упущенная объединенной компанией в период нестабильности) с

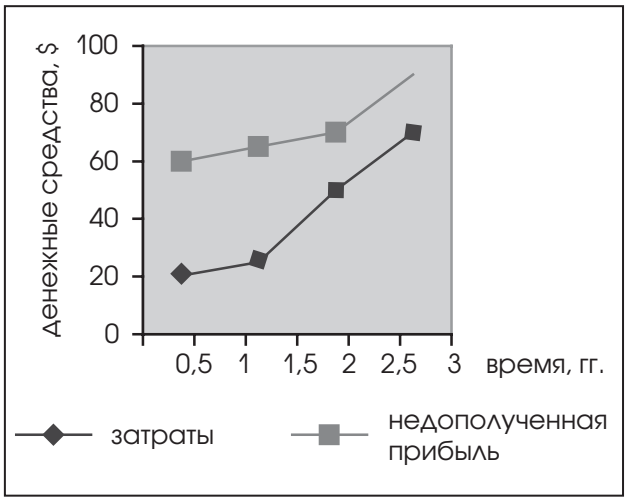

Рис. 1. Сопоставление недополученной прибыли с затратами

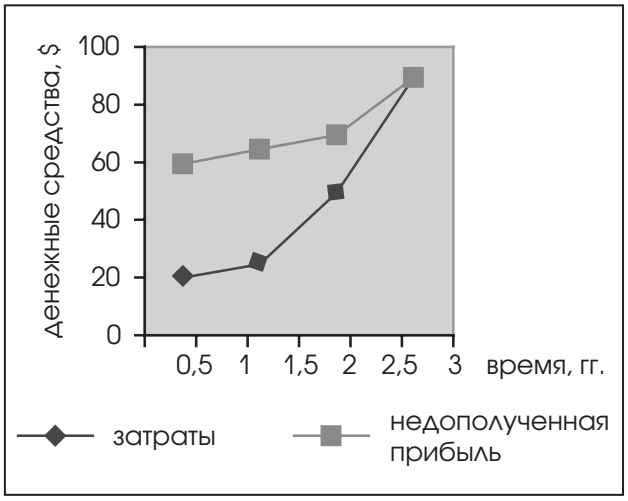

Рис. 2. Сопоставление недополученной прибыли с затратами (благоприятные условия)

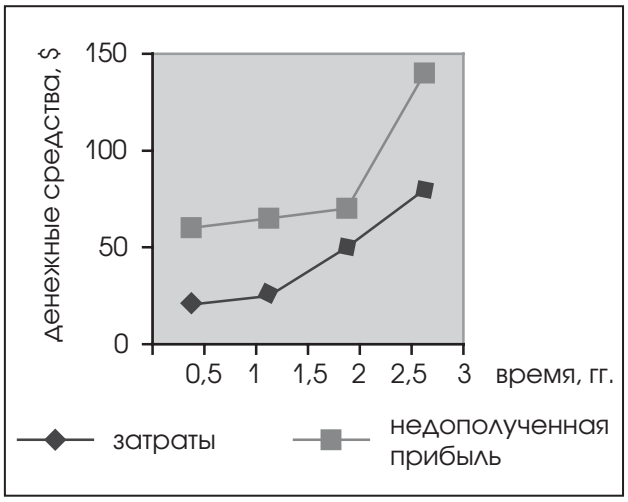

Рис. 3. Сопоставление недополученной прибыли с затратами (в случае неблагоприятного развития событий)

инвестициями, которые были на это затрачены (рис.1). Если она заведомо больше затрат на объединение — лучше было и не начинать. Потом можно годами стремиться компенсировать упущенное. Согласно нашему опыту, если через 2-3 года наблюдается положительная экономическая динамика (рис.2), то процесс слияния был оправдан. При удачном стечении обстоятельств экспоненты встретятся, что означает начало получения прибыли объединенной компанией. Но этого может и не произойти (экспоненты никогда не встретятся, рис.3). Недополученная прибыль будет накапливаться, объединенная компания — не выходить из состояния интеграции и цейтнота. Такое положение можно сравнить с котом, вечно гоняющимся за собственным хвостом.

Совет здесь можно дать один — оценивать и просчитывать экономические нюансы, чтобы оправдать свои финансовые ожидания.

Другой интересный аспект, волнующий многих, связан с лицензиями на предоставление услуг связи. Например, у вас есть несколько МгМн-сетей, которые построены под реализацию лицензионных условий. При слиянии возникает вопрос — на условиях чьей лицензии междугородной и международной связи будет работать объединенная компания? Нужно ли производить повторную приемку узлов в случае, если эти узлы принимались по условиям одной лицензии, а использоваться будут по другой? В России нет никакого специального законодательства или установленного порядка действий в этом вопросе. К тому же надо заметить, что international-шлюзы сотовых операторов и проводных по-разному настроены. Если для проводного оператора любой вызов, пришедший по международному линку, — международный вызов. А для беспроводного — вызов, пришедший от его абонента в роуминге, — не международный вызов. Нельзя просто взять и начать использовать узлы второго оператора для пропуска международного трафика. Необходимо провести довольно серьезные работы по настройке, чтобы все правильно заработало.

Кто виноват и что делать?

Примеры наглядно демонстрируют тот факт, что учесть все технические и организационные вопросы довольно непросто, а сделать это самостоятельно без чьей-либо помощи вообще не представляется возможным. Для эффективного слияния недостаточно аудиторской справки о количестве долгов или доходов. Стоит оценить состояние организационных структур, внутренних

процессов другого оператора. Сравнить и принять решение о том, какие из них более целесообразны в объединенной копании. Лучше заранее переработать нестыкующиеся процессы в каждом из операторов, довести всю необходимую информацию до сотрудников. Реализовать намеченное, не откладывая на потом. Только таким образом возможно сокращение периода нестабильности, который снижает динамику развития оператора в целом и может привести к потере всего достигнутого за долгое время работы.

Наиболее правильно еще до начала процесса слияния приглашать не только бизнес-консультантов, но и технических специалистов, которые подскажут, какие бенефиты можно получить от слияния ИТ-инфраструктур, смогут просчитать, как сократить 12-15 процентов комплекса оргструктуры, но при этом правильно и эффективно организовать необходимые новой компании процессы и подразделения.

Например, компания «Инфосистемы Джет», исходя из своего опыта, знаний мировых примеров best practice, имеет набор стандартных заготовок для решения часто встречающихся проблем. Они касаются как технической части и помогают минимизировать риски при осуществлении технической интеграции, так и административной. Специалистами компании наработана регламентно-административная документация по становлению новой организационной структуры и новых бизнес-процессов в объединенной компании. Это позволяет заказчику избежать бумажной волокиты, поскольку избавляет его от необходимости самостоятельной разработки подобных документов. К тому же, привлечение системного интегратора дает возможность контролировать весь процесс слияния, коррелируя его с лучшими мировыми практиками. Данный подход помогает адаптировать наработанные стандарты best practice под процессы компании с необходимыми параметрами KPI.

Конечно, привлечение сторонних консультантов способно во многом облегчить непростой процесс слияния двух операторов. Но один лишь этот фактор не убережет компании от всех проблем, поскольку для наиболее эффективного объединения требуется в том числе и внутренняя подготовка каждой организации.

Стоит также обращать внимание и на те условия, в которых происходит слияние. Интеграция выгодна лишь в определенной «атмосфере». Если ситуация на рынке, в стране, мире хоть както поменялась, объединение может быть нецелесообразно, как в случае с изменением лицензионных политик, частотных ресурсов или попросту финансового кризиса. Лучше отложить на время идею интеграции, подождать и провести все в более благоприятном «климате».

Сложности в любом случае будут. Но по нашему опыту подобных проектов, с помощью внешних специалистов возможно эффективно провести объединение, выстроив схему предполагаемых проблем и способы их решения. Для этого определяются основные критичные для бизнеса процессы и необходимые сервисы для их поддержки. Предоставляется возможность наглядно продемонстрировать заказчику, что из имеющегося набора инструментов является лучшим в данном конкретном случае. Скажем, если в мировой практике существуют примеры использования дополнительных функций для поддержания тех или иных бизнес-процессов, которые в объединяющейся компании не реализованы, в момент слияния консультанты смогут вовремя подсказать о необходимости их внедрения. Не исключена обратная ситуация, при которой обнаружатся дополнительные бизнес-функции в уже имеющихся процессах одной из компаний, но которые не имеют примеров в мировой практике. Специалисты могут выступить законодателями мод — оптимизировать данный процесс под потребности объединенной компании, тем самым наиболее эффективно выстроив как организационную, так и технологическую систему. Это позволит избежать большого количества критичных для бизнеса ошибок и сократить неизбежные издержки при слиянии двух операторов.

Экспертное мнение

Крупные и динамично развивающие организации в процессе своей деятельности, зачастую, не единожды проходят через слияние с другими компаниями. Некоторыми аспектами специфики объединения среди операторов связи с нами поделился Виталий Задорожный, директор по управлению операционными рисками компании «ВымпелКом».

J.I.: Расскажите, пожалуйста, каковы технологические особенности слияния двух операторов?

В.З.: Как правило, тот, кто покупает — сильнее, мощнее, лучше процессно и функционально организован. Если мы говорим о тех направлениях поддержки бизнес-операций, которыми занимается дирекция по управлению операционными рисками (информационная безопасность, непрерывность бизнеса и управление рисками) — то на моей практике в процессе интеграции двух компаний появлялись большие уязвимости в сфере информационной безопасности, очень серьезно просели KPI по процессу непрерывности предоставления бизнес-услуг, связанных с ИТ. Например, если раньше благодаря работе резервного центра в случае ЧС критичные системы восстанавливались очень быстро, то в процессе интеграции компаний количество критичных систем увеличилось. Все новые системы не имели решения по резервированию, соответственно, процесс непрерывности не мог обеспечить восстановления систем в согласованное с бизнесом время.

J.I.: Помимо исключительно технических аспектов, в каких еще сферах «жизни» компании процесс объединения может преподнести неожиданные сложности?

В.З.: Можно научиться закрывать уязвимости ИБ и запустить проекты по резервированию новых систем, но вот культурный слой — это беда. Нельзя сказать, что корпоративная культура любой из компаний хуже или лучше твоей — они просто разные. Сотрудники мыслят совершенно иными категориями. Обе организации и их ИТ-подразделения прекрасно выполняли задачи, которые перед ними ставились, а вместе так же хорошо работать они просто не могут — одна другую не понимает. Для примирения двух культур оптимально использование арбитра — посредника, у которого есть опыт и видение всех процессов. Необходимо, чтобы он вошел в игру и сказал: «У вас не на все сто процентов прекрасно, а у вас — нельзя сказать, чтобы совсем все плохо. У вас 60%, у вас 40% и я вижу, и знаю, где взять лучше и как собрать в одно».

J.I.: Не бывает проблем без решений. Какие советы можно дать операторам, задумавшим объединение, чтобы избежать серьезных ошибок?

В.З.: Проблем всегда много, причем зачастую их сложно идентифицировать. И очень часто бизнес недооценивает или не видит некоторые элементарные вещи. Именно поэтому для эффективного слияния всех процессов двух компаний принципиально важен практический опыт подобных проектов. «Теоретически уметь колоть дрова» — это здорово, но к результату вряд ли приведет.

Самым правильным будет обозначить возможные проблемы: переписать процессы обеих компаний, разработать некий набор сценариев для локализации уязвимостей. Все предусмотреть, конечно, не удастся, но большую часть из вероятных сложностей можно продумать и быть к ним готовым. Иначе может получиться так, что интеграционный процесс с очень правильными и логичными ожиданиями от синергии и оптимизации закончится запросами дополнительных инвестиций и вакансий и порождением не предполагавшейся интеграционной прослойки.

И не стоит забывать, что если вы не смогли объединиться за полгода — у вас проблемы, а если интеграции не случилось и за год — вы этого не сделаете никогда.

Виталий, спасибо!

РЕАЛЬНАЯ БЕЗОПАСНОСТЬ

Информационная безопасность на новом уровне – тема года для российского телекома

Отрасль связи сегодня развивается очень динамично, и столь же активные процессы идут на рынке решений информационной безопасности для телеком-сектора. Об этом мы беседуем с руководителем направления по работе с телекоммуникационными компаниями центра информационной безопасности компании «Инфосистемы Джет» Натальей Баталовой.

Как Вы оцениваете отношение к проблемам информационной безопасности в телеком-секторе? Какие тенденции в сфере ИБ наблюдаются в российской отрасли связи?

Н.Б.: Проблемам ИБ в телекоме уделяется большое внимание, их важность осознают не только руководители технических подразделений, но и бизнес-руководство, обеспечение должного уровня ИБ относят к важнейшим составляющим успешности компании. Проекты активно финансируются, но при условии обоснованно доказанной финансовой эффективности.

На ситуацию с ИБ в отрасли действуют как внутренние, присущие непосредственно телекоммуникационному бизнесу, так и внешние факторы.

К внешним в первую очередь относится закон «О персональных данных» — операторы активно занимаются такими проектами. Специфика такова, что телекомы эксплуатируют, наверное, самые передовые ИТ-инфраструктуры, в составе которых работает дорогостоящее оборудование и критичные приложения, и при этом владеют огромной массой персональных данных. Строгое следование закону для них не только выливается в огромные инвестиции, но и грозит снижением производительности продуктивных сетей и приложений. Ошибки в проектировании систем защиты персональных данных могут стоить слишком дорого! Поэтому мы придерживаемся сбалансированного подхода, основные принципы которого — «не навредить» и «не тратить средства заказчиков только на формальное соответствие, а строить реально полезные системы».

Создаваемый по инициативе лидеров рынка отраслевой стандарт по защите персональных данных призван учесть специфику бизнеса телекомов, сформулировать понятные требования и облегчить прохождение проверок, которые пока имеют не очень предсказуемые результаты.

Основная «внутренняя» тенденция — обострение конкуренции. С целью удержать рынок и привлечь новых абонентов операторы не только стремятся повысить качество базовых услуг, но и работают над запуском дополнительных сервисов, в том числе в области ИБ. Это можно назвать темой 2010 года в телекоме.

Как вы оцениваете уровень сервисов ИБ, имеющихся в арсенале российских операторов?

Н.Б.: Пока на рынке присутствуют только базовые услуги, реализация которых несколько разочаровывает. Если в комплекте с домашним интернетом продается клиентское антивирусное ПО, то говорить об услуге по большому счету нельзя, так как фактически это дистрибуция антивируса, обслуживание которого ложится на плечи абонента. Несколько операторов продают «родительский контроль», который в действительности позволяет ограничить пребывание в Интернете по времени суток, а доступ к недетским сайтам контролируется довольно примитивными методами, не дающими надежной гарантии качества. А ведь качество услуг — это основа бизнеса операторов!

Радует то, что серьезные операторы вместе с квалифицированными интеграторами и поставщиками разрабатывают более высокоуровневые услуги ИБ. Некоторые из них уже работают в тестовом режиме, так что скоро ожидается их массовый выход на рынок. Мы уже накопили большой опыт таких проектов и сейчас работаем над созданием допуслуг у нескольких операторов.

Домашним пользователям предлагается «Чистый интернет» (антивирус), но организованный на стороне оператора, который и гарантирует качество сервиса. Для построения услуги «Родительский контроль» применяются сложные многоуровневые средства определения контента, обеспечивающие высокую точность фильтрации.

Сервисы безопасности для корпоративных абонентов в большей степени подбираются под конкретного клиента. Помимо антивируса востребована, например, URL-фильтрация — контроль неделовых коммуникаций, позволяющий компании сэкономить на оплате канала и повысить работоспособность сотрудников.

Спрос на какие ИБ-сервисы сейчас явно превышает предложение? Какие услуги ожидают своего выхода на рынок?

Н.Б.: Услуга, которая по нашим наблюдениям востребована, но на рынке почти не представлена — защита корпоративных абонентов от DDoS-атак. Многие компании (банки, например) в результате таких атак регулярно теряют деньги. Операторы же только задумываются о реализации такой услуги.

Мы сейчас начинаем работы у нескольких операторов, имеющих большую базу корпоративных абонентов. Услуга недешевая, но клиенты осознают, что ущерб от атаки обойдется на порядки дороже, поэтому прогноз по проникновению и доходности услуги — оптимистичный.

Еще ряд сервисов для корпорантов может «вырасти» из систем ИБ, эксплуатируемых операторами в своих сетях, при наличии достаточных мощностей — например, Security Operation Center (SOC) и DLP. Например, оператор может уведомлять абонента об атаке на его сеть или попытке передачи вовне критичных данных и предоставлять инструкции по реагированию. Операторы уже думают о выпуске целого пласта подобных услуг. Мы, как системный интегратор, видим большой потенциал в таких проектах.

Большинство ваших клиентов-операторов – крупные компании национального масштаба. Какими специальными средствами решаются проблемы ИБ в таких компаниях?

Н.Б.: В крупных компаниях, «напичканных» средствами защиты, нереально идти по пути простого их наращивания. Здесь остро стоит вопрос управления и контроля ИБ и оптимизации затрат на эти процессы.

В таких условиях необходимо построение процессов оперативного управления ИБ — мониторинга, управления инцидентами, уязвимостями, полномочиями, соответствиями и др. Реализовать их вручную в крупной компании невозможно, и основным средством автоматизации здесь является SOC — комплекс технических средств, который в совокупности с правильно выстроенными процессами, несмотря на свою высокую стоимость, позволит снизить затраты на управление безопасностью и поддержание ее требуемого уровня.

Еще один востребованный класс решений — Identity Management (IdM). Они актуальны в компаниях с большим количеством пользователей и систем, в которых пользователям назначаются полномочия (электронная почта, серверы корпоративных каталогов, серверы баз данных, HR-системы и т.д.). Построение IdM-системы — проект не из дешевых, но такая система позволяет не только навести порядок с полномочиями пользователей, что заметно повышает уровень безопасности компании, но и сэкономить за счет автоматизации ручного труда.

Какие основные задачи стоят сегодня перед телекомоператорами, и что могут предложить системные интеграторы для их решения?

Н.Б.: Среди главных задач крупных операторов — борьба с мошенничеством и потерей доходов.

Один из основных видов мошенничества, который невозможно побороть стандартными фрод-машинами, — нелегальная терминация трафика. Пилотные проекты, проведенные нами во всех регионах в 2009 г., показали, что в среднем треть трафика в России «приземляется» некорректно (от 8-10% в небольших райцентрах до 70% в мегаполисах). Потери крупного оператора достигают сотен миллионов рублей в год. С конца 2009 г. мы ведем коммерческие проекты в ряде операторов и можем похвастаться следующими результатами: только за один квартал прирост выручки зонового оператора составляет десятки миллионов рублей! Таким образом, за короткий период наши проекты окупаются в несколько раз.

Для сокращения потерь доходов из-за некорректной тарификации и других причин (а это 5-20% выручки оператора) используются системы гарантирования доходов (Revenue Assurance, RA). Они стоят недешево, и для их построения требуется серьезное обоснование. Поэтому сначала мы проводим RA-аудит и оценку потерь (сложная и трудоемкая работа, которую, по моим данным, в России сейчас может квалифицированно выпол-

нить только наша компания), и лишь потом начинаем поэтапное внедрение системы, обеспечивающей в первую очередь защиту наиболее критичных для данного оператора зон риска. При таком подходе система RA, несмотря на высокую цену, способна окупиться в среднем в течение года. Это уже поняли многие мобильные операторы, и теперь дело за их коллегами из сектора фиксированной связи.

У мобильных операторов сейчас идет «волна» активностей по защите от смс-фрода: многие подверглись и продолжают подвергаться смс-атакам и терять деньги. Опять же, оптимальный по нашему опыту подход — начать с аудита: провести «срез трафика» и выявить, какие виды смс-фрода имеют место, и тогда решение по защите от него будет экономически оправданным и эффективным.

В последнее время много говорят о системах предотвращения утечек информации. Насколько актуальны DLP-системы в телекоме?

Н.Б.: Сегодня, наверное, нет компаний, в которых не были бы внедрены элементы DLP. Ведь бывают случаи, когда утечки обходятся в сотни тысяч долларов! И телекомы — не исключение. В зависимости от зрелости DLP-функции у клиента наши проекты различаются: от внедрения базового функционала в течение 1 месяца до создания полномасштабной системы, включая построение процессов контроля утечек, в которые помимо подразделений ИБ вовлечены службы экономической безопасности, HR и другие.

В нашем арсенале DLP-продуктов 2-3 лучших, на наш взгляд, импортных средства и собственная разработка — «Дозор», недавно отметивший свое 10-летие и также обладающий мощным DLP-функционалом. Продукт позволяет контролировать содержимое сетевых ресурсов, сообщений электронной почты, социальных сетей, веб-почты, ICQ, создавать «цифровые отпечатки» с документов. Основные отличия «Дозора» — хорошее «понимание» русскоязычного контекста, высокая точность срабатывания, максимально широкий список контролируемых российских ресурсов и мощная система архивирования и поиска, позволяющая хранить переписку в течение требуемого времени и оперативно извлекать нужную информацию при разборе инцидентов.

Интервью опубликовано в журнале «ИКС», сентябрь 2010

Наш «Собеседник» в лице ИТ-директора группы компаний «Детский мир» Сергея Рогова, расскажет Вам о жизни своего департамента, поделится секретами разработки ИТ-стратегии и успешного воплощения ее в жизнь, а также своим взглядом на развитие рынка информационных технологий в России.

J.I.: Какие задачи решает ИТ-подразделение? Как Вы видите его развитие? Существуют ли какие-то особенности в работе подразделения (в постановке целей и задач, их решении), связанные с особенностями бизнес-процессов, бизнеса компании?

С.Р.: Наше подразделение занимается информационными технологиями в области розничной торговли, в частности выполняет ИТ-поддержку бизнеса в группе компаний «Детский мир». С того момента, как в 2006 году я пришел в компанию, ИТ-служба была полностью реорганизована: изменена структура, по-другому построены бизнес-процессы, не без помощи компании «Инфосистемы Джет» по одному из направлений.

Вроде бы, ИТ — всегда одно и тоже: программное обеспечение, оборудование, технологии, вечно непонимающие пользователи, что-то делающие не то, и вечно виноватые во всем айтишники. Такие черты присущи ИТ в любой отрасли. Но своя специфика у нас все-таки есть — это и специализированное программное обеспечение, и технологии розничной торговли — большой объем транзакционной информации, и географическая распределенность компании и ее операционной деятельности (филиалы, в которых необходимо осуществлять техподдержку, находятся в 4-х часовых поясах).

Информационные технологии — инструмент, который подчиняется бизнесу. Требования бизнеса первичны, и они должны быть отработаны ИТ-департаментом профессионально, с использованием лучших мировых практик. Это и есть наша основная функция и задача, поскольку ИТ ради ИТ в бизнесе никому не нужно.

J.I.: Как правильно подойти к вопросу разработки ИТ-стратегии и ее воплощению?

С.Р.: Начинать, конечно, нужно со стратегии компании в целом. Бессмысленно разрабатывать стратегию ИТ, если нет понимания, как будет развиваться организация. Одна из важных составляющих успеха в этом вопросе — умение руководителя ИТ-службы «видеть», что же будет в конце преобразований, к чему нужно привести подразделение. Если с вышеназванным вопросом удалось разобраться, дело за малым — команда специалистов должна уметь декомпозировать это видение на составляющие и правильно их превратить в проекты, посчитать в ресурсах, времени, затратах.

J.I.: В чем, по Вашему мнению, залог успеха эффективного воплощения разработанной стратегии в жизнь?

С.Р.: Во-первых, планы и цели, которые перед собой ставишь, должны быть реалистичны и достижимы. Второе — то, что задумываешь, должно быть нужно бизнесу, а не ИТ-подразделению и его руководителю. Третье — правильный расчет ресурсов. Не стоит строить воздушные замки, если не способен сделать всего запланированного, по самым разным причинам: нет денег, компания не планирует столько заработать, сколько собираешься потратить на ИТ и т.д. Нужно идти в ногу с бизнесом и предоставлять ему те услуги, которые им действительно востребованы.

J.I.: Какие сложности в разработке ИТ-стратегии могут возникнуть? С чем они связаны?

С.Р.: Сложностей много. Внедрение чего-то нового — это всегда не просто. На этапе разработки характерными ошибками могут стать — уход стратегии в технические детали, глубокие проработки. В этом случае можно потерять общий взгляд на ситуацию, стройность самой стратегии — она не гибкая, не информативная и многим не понятна. Срок ее разработки становится слишком велик, и к моменту выхода она уже оказывается никому не нужна. И кому нужна такая стратегия, пускай и

разработанная с привлечением прекраснейших ИТ-специалистов?

Еще один непростой вопрос, на котором можно споткнуться — неправильный экономический расчет. Бюджет все-таки часть стратегии, и последствия, связанные с непониманием, как использовать те или иные средства, могут быть весьма плачевными.

На этапе внедрения, как правило, самое яркое, показательное и наглядное явление, с которым можно столкнуться — это сопротивление персонала. Преодолеть его зачастую бывает непросто.

В нашем случае не могу сказать, чтобы нам что-то сильно препятствовало.

J.I.: Вы говорили, что одним из наиболее распространенных препятствий на этапе внедрения может стать сопротивление персонала. Как Вы решали эту проблему? Какими методами?

С.Р.: Я считаю, что есть несколько доступных методов для решения этого вопроса. И они всем известны. Во-первых, людей нужно заранее информировать о том, какие изменения будут происходить в компании, объяснять, для чего все делается и что получится в результате. Человеку обязательно нужно рассказать и показать, какова конечная цель. К тому же сотрудник должен понимать, что будет служить мерилом ее успешного достижения. И тогда он успокаивается, поскольку будущее перестает казаться столь неопределенным и «туманным».

Второе — обучение. Лучше всего персонал воспринимает такого рода информацию не на слух, а на примере бизнес-кейса. Такую форму подачи информации мы и пропагандируем в нашей компании. Лучше показать, как это будет выглядеть и работать, чем прочитать многочасовую лекцию.

В ходе всего вышеназванного процесса часть персонала по разным критериям: полезности, неспособности, случаям саботажа (бывают и такие), не желанию освоить новую систему — подлежит замене. Как правило, таких не много.

J.I.: На Ваш взгляд, формирование ИТ-подразделения и ИТ-стратегии компании должно происходить в одно и то же время? Или эти два процесса должны идти в определенной последовательности относительно друг друга?

С.Р.: Если начинать становление ИТ в компании с самого начала, я бы рассматривал следующий вариант. В первую очередь должно быть создано ИТ-подразделение, которое закрывает все «горячие точки» бизнеса, чтобы он мог хоть как-то спокойно работать. Когда наиболее критичные области защищены, ИТ-подразделение может заняться разработкой ИТ-стратегии. И уже после ее разработки происходит реорганизация ИТ-службы, оптимизация ее работы.

J.I.: Насколько критична для бизнеса компании бесперебойная работа ИТ-систем и эффективное функционирование всего ИТ-подразделения?

С.Р.: К сожалению или к счастью — сегодня все участки компании «Детский мир» завязаны на ИТ. Бизнес напрямую зависит от бесперебойного функционирования ИТ-систем: начиная от планирования ассортимента, прогнозирования, заказа товара, поставки, хранения и заканчивая оформлением полок и печатью ценников. И самое главное — продажи! Касса — та система, которая никогда не должна останавливаться. Она также зависит от ИТ, поскольку кассовый аппарат — сложный компьютер, который включает в себя и обеспечение продаж, и работу с дисконтными системами, и работу с эквайрингом — это целый узел сплетений ИТ-технологий. Не могу найти ни одного участка в «Детском мире», который не был бы связан с информационными технологиями: и бухгалтерия, и управление финансами, и прогнозирование. Ведь от того, насколько эффективно работают все без исключения ИТ-системы, зависит придут ли к нам покупатели или нет.

J.I.: Не так давно, совместно с компанией «Инфосистемы Джет» было анонсировано завершение проекта по автоматизации процессов поддержки ИТ-услуг. По прошествии времени, не потерял ли проект своей актуальности – востребованы ли внедренные решения в настоящий момент, пользуются ли ими сотрудники? В чем их практическая польза?

С.Р.: Безусловно, востребованы. Сотрудники работают с системой ежедневно, иначе я расписался бы в собственной некомпетентности. К тому же, у нас есть планы по ее развитию.

Прежде всего, внедренные решения позволяют мне измерить качество работы подразделения, поскольку все оперативные коммуникации проходят через Help desk, соответственно, через управление инцидентами. Учитывая особенности этих коммуникаций (никто же не звонит к нам в службу, чтобы сказать: «А у меня все хорошо!»), любой звонок — это всегда стресс, всегда проблема с той стороны. И потому, как мы отрабатываем

такие случаи, зачастую судят о работе всего подразделения.

Помимо прочего, я имею возможность учитывать реальное время реакции, которую демонстрируют мои сотрудники по тому или иному инциденту, время закрытия инцидента. Полученные данные, определенным образом агрегированные, дают возможность определить, достаточно ли количество персонала по отношению к вопросу устранения инцидентов, достаточно ли квалифицированный персонал у меня работает и не только у меня. Если повторяется один и тот же вопрос от одного и того же человека на уровне «включи вилку в розетку», можно говорить о неквалифицированном сотруднике на стороне бизнеса.

Очень много интересной информации можно получить, разбирая полученные данные. Я могу анализировать повторяющие инциденты, в итоге выявлять системные ошибки, отслеживать отказоустойчивость того или иного оборудования по количеству обращений по конкретной единице техники и количеству его ремонтов.

Безусловно — внедренное решение очень полезно, и нам есть куда расти.

J.I.: Как реализованный проект повлиял на повседневную работу сотрудников компании?

С.Р.: Система упорядочивает их работу. Это некий тайм-менеджмент для сотрудника. Он знает, что если к нему «прилетает» определенная задача, то он должен действовать по следующей схеме: первое, второе и третье. Система ему подсказывает, что и как он должен делать, какие формы заполнять — она его «ведет». Сотрудник точно знает, что пока он не закончит с данной задачей, следующие он брать не может. При этом я уверен, что если человек выполняет одну заявку в день — он лентяй. И он знает, что я это знаю. Отсюда хорошая мотивация для работы. Внедренное решение позволяет мне при смене персонала быстрее погружать сотрудников в технологический процесс, т.е тратить меньше времени на обучение. А все потому, что бизнес-процесс прописан, отлажен и всем понятен.

J.I.: Сегодня одними из наиболее востребованных становятся системы защиты баз данных. Как вы считаете, насколько актуальна тема? Как в вашей компании решаются вопросы защиты баз данных?

С.Р.: Данный вопрос никогда не терял своей «остроты» — чем больше база данных, чем сложнее, а с учетом вступления в силу 152-ФЗ «О защите базы данных», он становится еще более актуальным. Мы с этим справляемся, защищаем и средствами самих баз данных, и средствами контроля доступа в сеть, и средствами, которые организовывают VPN-канал, шифрование баз данных.

Инцидентов у нас ни разу не было, то ли надежная защита, то ли люди честные. Были попытки «слива» информации, но не из баз данных. Мы такие случаи периодически отлавливаем. Но в целом — они единичны.

J.I.: Ежегодно на рынке возникают новые темы и направления в области развития ИТ-систем (облачные вычисления, виртуализация и т.д.)? Что для Вас кажется наиболее интересным и перспективным для российского рынка?

С.Р.: Интересно все, что приносит выгоду бизнесу. Я как айтишник попробовал бы поглубже «ковырнуть» и облачные вычисления, и виртуализацию. Для меня интересны технологии, возврат инвестиций для которых с точки зрения бизнеса можно просчитать. В перспективе, мне кажется, пойдет все, что позволит ИТ-подразделениям и ИТ-компаниям предоставлять сервис-ориентированные решения. Так сейчас, например, прослеживаются тенденции по возвращению к мейнфреймам — неким черным ящикам, которые внутри себя содержат комплекс готовых решений. И за этим, на мой взгляд, будущее ближайших 10 лет. Я считаю, бизнес должен получать ИТ-услуги «из розетки». Как мы получаем телевидение, интернет, так он должен получать и услуги. Вы спросите, каким образом все это будут обеспечивать провайдеры? Я думаю, к этому приведут и облачные вычисления, и виртуализация и еще куча технологий, которые сегодня испытываются и интегрируются.

J.I.: И в заключение. Бытует мнение, что если Россия все-таки войдет в ВТО и нам придется соответствовать мировым стандартам, наши интеграторы не справятся и рынок заполнят западные компании. Согласны ли вы с этим?

С.Р.: Нет, я с этим не согласен. Если наших отечественных интеграторов будут не задавливать, а поддерживать и власть, и элита бизнеса — потенциал колоссальный. Более того, наши интеграторы на отечественном рынке не то что должны быть, а могут быть и более того будут успешнее, чем западные. Это связано с целым рядом причин, не только айтишных. Это связано с менталитетом и с подходом к решению задач, и с нахождением общего языка с бизнесом. А уж говорить о том,

что программисты и специалисты в области электроники у нас очень высокого уровня и ценятся во всем мире, даже и не приходится. Правда, реалии таковы, что весь мир активно переключился на Индию и Китай, страны третьего мира, где рабочая сила дешевле. Но это не значит, что у них лучше. Наша страна богата высококвалифицированными специалистами.

Другое дело, что, на мой взгляд, нужно финансировать, поддерживать, повышать контроль над образованием в этой сфере, потому что его качество в области ИТ совсем невысокое. За те 5 лет, которые студенты проводят за партой, столько всего меняется. То, чему они научились, на выходе уже никому не нужно. А содержать современную программу образования в актуальном состоянии очень дорого. Но если мы этого не будем делать, то у нас никогда не будет кадров. Потому что сегодня те, кто выходит на рынок и становится успешным — в основном самоучки, которые добиваются всего за счет таланта. Но я уверен, что мы можем готовить таких же специалистов, а не заниматься поисками уникальных самородков. Но для этого нужно серьезно вложиться. И тогда ИТ в России точно быть!

Сергей, спасибо!

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю.
Редактор: Слободчикова Т.А.
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
e-mail: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555