За прошлый год количество DDoS-атак на государственные и коммерческие инфраструктурные институты выросло на 178% | 14

ИТ

Тематическое приложение к газете **Коммерсантъ**

Информационные технологии

Четверг 27 марта 2014 №51 (5324 с момента возобновления издания) **kommersant.ru**

15 Мобильным операторам рекомендуют оптимизировать трафик

16 На что банки тратят ИТ-бюджеты

16 «Сбербанк» научился распознавать лица

Борьба с энтропией

По предварительным оценкам IDC, российский ИТ-рынок за прошедший год не изменился, а в первом полугодии 2014 года может сократиться на 5–15%.

— обзор рынка —

Еще три года назад эксперты прогнозировали триумфальное восстановление российского ИТ-рынка после кризиса, а итоги 2011 года давали все основания для подобных надежд: рост тогда, по оценкам IDC, составил 13,3% в долларовом выражении. Однако уже в 2012 году, когда рынок подрос всего на 3,9%, стало понятно, что эпохе двузначных цифр пришел конец. Эксперты связывают наметившееся тогда замедление с ухудшением экономического климата.

Российская отрасль ИТ вслед за общемировой переживает эпоху кардинальных инфраструктурных перемен, когда развитие новых технологий приводит к изменению потребности клиентов и как результат к изменению архитектуры рынка в целом. Совпадение этих двух факторов — экономического (и геополитического) кризиса и тектонических сдвигов внутри самой отрасли — ставит перед компаниями непростые задачи, от решения которых будет зависеть дальнейшая судьба их бизнеса.

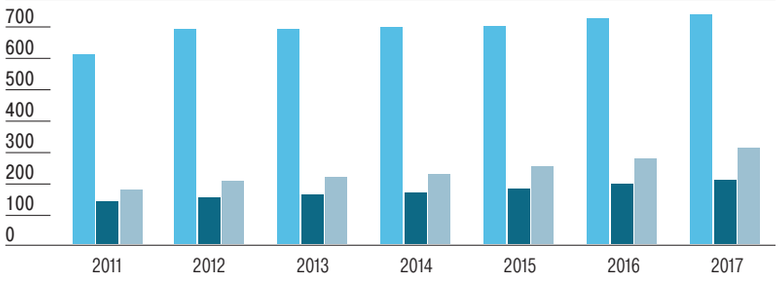
«Впервые за два прошедших десятилетия, исключая кризисы 1998 и 2008–2009 годов, динамика ИТ-рынка в 2012–2013 годах описывается цифрами, близкими к нулю, тогда как ИТ-компании за долгие тучные годы считали ежегодный рост в 20–30% абсолютно нормальным»,— резюмирует тенденцию последних нескольких лет председатель совета директоров ГК «АйТи» Тагир Яппаров.

По словам директора IDC по исследованиям в России и СНГ Елены Семеновской, компания пока продолжает уточнять результаты 2013 года по мере того, как участники российского рынка подводят итоги своей работы за год. Тем не менее уже сейчас понятно, что общая картина остается неизменной: рынок ИТ в прошлом году не рос. «Если говорить о цифрах, то с учетом колебания курса рубля в долларовом выражении рынок сократился на 1%,— отмечает госпожа Семеновская.— С учетом возможных уточнений я бы сказала, что рынок значительно не изменился в своем объеме: не было ни роста, ни драматичного падения. Хотя инвестиции в отдельные сегменты рынка, такие, как рынок серверов, заметно сократились».

Она подчеркивает, что основными причинами замедления рынка, которое началось во второй половине прошлого года, также стали общеэкономические факторы: замедление роста российской экономики, сокращение инвестиций в ИТ в связи с расходами на Олимпийские игры со стороны госсектора, сокращение количества компаний в сегменте малых и средних предприятий, снижение спроса со стороны домашних пользователей.

Что касается ближайших перспектив, они также не внушают оптимизма. «С начала года мы неоднократно пересматривали цифры,— отмечает Елена Семеновская.— Сейчас уже можно сказать, что в первой половине 2014 года роста не будет. Степень сокращения рынка ИТ будет зависеть от многих факторов и может составить в худшем сценарии от 5% до 15%. К экономическим факторам добавляются политические и геополитические риски, а также изменения в законодательстве, связанные с применением федерального закона №44-ФЗ «О контрактной системе» государственными организациями. Можно надеяться, что вторая половина года окажется более продуктивной, и в целом рынок ИТ не сократится значительно».

ДИНАМИКА ИТ-РЫНКА В РОССИИ (МЛРД РУБ.) ИСТОЧНИК: IDC BLACK BOOK, 2014.



ДИНАМИКА РЫНКА ПО В РОССИИ (МЛРД РУБ.) ИСТОЧНИК: IDC BLACK BOOK, 2014.

Экономические и геополитические потрясения совпали с не менее глобальными переменами внутри самой ИТ-отрасли.

«В течение последних 20 лет большинство крупных игроков работало в модели перепродажи зарубежных продуктов и решений, выстраивая вокруг этих решений свои сервисы: системную интеграцию, техническую поддержку, консалтинг, обучение,— рассуждает Тагир Яппаров.— За последние несколько лет развитие технологий начало формировать принципиально новые модели потребления ИТ корпоративными заказчиками. Например, сегодня мы видим, что на повестке дня не владение всей информационной системой, а аренда ресурсов и программного обеспечения. Еще пример — так называемая мобильная революция, сильно изменившая наши представления о корпоративном рабочем месте и корпоративных информационных системах. Все это приводит к снижению объемов закупок традиционного оборудования (прежде всего ПК и серверов) и ПО и, как следствие, услуг интеграторов конечными корпоративными потребителями».

Генеральный директор компании КРОК Борис Бобровников также выделяет тенденцию перехода от поставок оборудования к услугам и прогнозирует возможное сокращение объемов ИТ-рынка именно за счет первого. «В результате если и будет спад, то в среднем процентов на десять и именно в поставках оборудования,— отмечает он.— Услуги останутся на прежнем уровне».

По предварительным оценкам IDC, рынок серверов сократился в прошлом году на 26%, ПК — на 30%, при этом продажи планшетов выросли. В целом же рынок оборудования в прошлом году впервые показал отрицательную динамику: его объем сократился по итогам года на 2,2% (для сравнения: в 2012 и 2011 годах его рост составлял 7,2% и 10,3% соответственно с учетом валютных колебаний).

Несмотря на то что распределение долей между основными сегментами в структуре российского ИТ-рынка пока существенно не меняется — как ожидается, по итогам 2013 года около 60% доходов пришлось на оборудование и примерно по 20% на ИТ-услуги и ПО, очевидно, что рынок поставок оборудования становится вторичным и низкомаржинальным. Это значит, что интеграторам необходимо делать ставки на принципиально новые продукты и сервисы.

Точки роста

Если коротко охарактеризовать те требования бизнеса, которые уже определяют новый ландшафт ИТ-отрасли и останутся структурообразующими в ближайшие пять лет, то это, как и в последние год-два, аренда ресурсов, обработка данных и мобильность. Компании-заказчики должны уметь оперировать огромными объемами самой разнородной информации, обязаны иметь доступ к рабочему месту в любой точке планеты, где есть интернет, и при этом не хотят — а зачастую не могут себе позволить — тратить средства на покупку и поддержание «железа» и ПО там, где все это можно арендовать.

«На пересечении этих основных тенденций возникает портрет системного интегратора будущего,— рассуждает председатель правления IBS Сергей Мацоцкий.— Этот интегратор будет больше заниматься софтом, чем „железом“. Задачи, которые он будет решать,— это прежде всего интеграция различных данных из множества источников, организация систем хранения и анализа этих данных, интеграция между множеством различных приложений в «облаке» и on-premise. Все эти задачи существуют уже сейчас и будут существовать через пять лет. Значит, наши услуги будут востребованы. Все ли системные интеграторы смогут поймать эти тренды и перестроиться — не уверен, но время покажет».

Согласно прогнозам IDC, объем информации, хранящейся во всем мире, с 2009 по 2020 год увеличится в 44 раза. Как ожидается, ежегодный рост рынка технологий и услуг, связанных с интеграцией и анализом больших объемов бизнес-данных (Big Data), до 2017 года составит 27%, что в шесть раз превышает прогнозируемые темпы роста всей отрасли ИКТ. Все больше разнородной информации из разных источников вовлекается в корпоративный оборот, как структурированной, так и неструктурированной. Это требует от интегратора развития совершенно новых компетенций и моделей, а значит, открывает новые возможности для быстрорастущего бизнеса в таких сегментах, как ритейл, страхование и финансы, телекоммуникации.

с16

Безопасный интеллект

В период экономического спада желающих поживиться чужим добром становится все больше. Киберпреступность набирает обороты и самоорганизуется в эффективные структуры. Поставщики аппаратных и программных средств противопоставляют интеллектуальные средства защиты, обеспечивающие непрерывность бизнес-процессов. Сегмент информационной безопасности (ИБ) сохраняет рост на фоне общего спада в ИТ-отрасли.

— сектор рынка —

На прошедшей в феврале в Сан-Франциско конференции по ИБ RSA Security Conference-2014 чаще всего можно было видеть на вывесках и слышать на выступлениях слово «intelligent» («умный, интеллектуальный») по отношению к средствам информационной безопасности.

Это отражает некий продуктовый тренд, которому пытаются следовать маркетологи компаний, выпускающих соответствующие программные и аппаратные средства. Владимир Гайкович, глава компании «Андэк», рассказывает, что атаки киберпреступников стали целенаправленными, распределенными во времени и использующими разноплановые методы для преодоления защиты.

Целью этих атак, как правило, является кража денег. Охота за одной жертвой может продолжаться месяцами, за это время хакер пытается нащупать дыры в защите и пробует различные способы взлома системы безопасности, а после проникновения в систему ведет себя осторожно, ожидая момента для совершения хищения.

По мнению аналитиков, надежно защититься от таких нападений с помощью межсетевых экранов, систем обнаружения атак, антивирусов и других стандартных средств невозможно. Современная система защиты должна непрерывно контролировать действия пользователей и программ, сигнализируя администраторам о подозрительных ситуациях.

По мнению поставщиков, интеллектуальность средств защиты как раз и заключается в том, чтобы на основе данных от разнородных средств защиты строить модели поведения пользователей и программ и на основании отклонений от них судить о наличии той или иной проблемы.

Антон Чувакин, директор по исследованиям в области ИБ американской компании Gartner, говорит, что инновации, которые показывают на конференции RSA, как правило, начинают появляться у корпоративных пользователей спустя два-три года после анонса. По опыту прошедших лет в России первые внедрения новых технологий случаются еще спустя два-три года. То есть пока нет речи о массовом внедрении комплексных интеллектуальных систем защиты в российских компаниях.

При этом киберпреступники сегодня как никогда организованны и технологически подкованы. Питер Анаман, глава отдела по онлайновому пиратству Microsoft Cybercrime Center, во время конференции Play It Safe Day рассказал о ботнете Citadel, который был организован как хороший бизнес. Хакер, который проживает предположительно на территории РФ или Украины, по прозвищу AquaBox организовал веб-сервис, в который были приглашены порядка 90 киберкриминальных групп. Через сайт они получали обновления вредоносного ПО, техническую поддержку, могли купить дополнительные ресурсы для организации атак и т. д. Так, даже неискушенный в технологиях злоумышленник мог с легкостью организовать DDoS-атаку.

По словам Александра Лямина, генерального директора компании Qrator Labs, защищающей от DDoS-атак, сегодня устроить серьезное нападение такого рода можно, используя всего лишь пять-десять серверов. При этом, по словам господина Лямина, 90% сетей операторов в РФ не готовы к подобным вторжениям. Это значит, что при возникновении атаки достаточно высокой скорости, могут отключаться целые сегменты российской части интернета.

Другая угроза, которая приводит к потерям огромных сумм денег — утечки информации. В аналитическом центре Zecurion Analytics посчитали, что по этой причине в 2013 году российские и зарубежные компании потеряли более $25 млрд. Причем в 30% случаев к этому привела деятельность хакеров или внутренних инсайдеров. Общий ущерб от внутренних инцидентов информационной безопасности вырос на 25% по сравнению с 2012 годом и составил чуть более $25 млрд.

Рост объемов ущерба от утечек данных указывает на то, что компании не уделяют защите информации должного внимания, вследствие чего теряют колоссальные деньги. Так, в среднем по миру убыток от одной утечки составил $32 млн, в России размер финансового ущерба несколько меньше, а вот максимальные потери от одного инцидента составили более 4 млрд рублей.

Владимир Ульянов, руководитель аналитического центра Zecurion, говорит, что в 2014–2016 годах стоит готовиться к увеличению краж персональных данных из банков. Мошеннические схемы, связанные с эквайрингом пластиковых карт, становятся все более эффективными и позволяют злоумышленникам быстро монетизировать полученную информацию.

Непрерывный рок-н-рол

На рынке средств информационной защиты существует большое количество продуктов, которые реагируют на какие-то отдельные виды угроз. Такой подход уже устарел, но многие компании продолжают им пользоваться. При этом ситуация постепенно сдвигается, и корпоративные заказчики понемногу начинают понимать преимущества комплексных интеллектуальных систем защиты, обеспечивающих непрерывность бизнес-процессов.

Аркадий Прокудин, заместитель руководителя Центра компетенции информационной безопасности компании «АйТи», говорит, что сегодня передовой подход в области ИБ, когда человек создает процессы, а защиту осуществляют системы в автоматическом режиме. То есть создается самозащищающаяся инфраструктура, так как человек не в состоянии успеть на все среагировать в реальном времени.

И, конечно, при построении таких систем на первое место выходят интеллектуальные системы защиты. «Современный крупный клиент понимает, что, поставив межсетевой экран и антивирус, защиты организации не добьешься. Необходимо подходить комплексно к проблеме. Сегодня уже недостаточно системы, которая автоматизирует выполнение рядовых функций защиты. Настало время решений, автоматизирующих целые процессы»,— говорит господин Прокудин.

Михаил Башлыков, руководитель направления информационной безопасности компании КРОК, отмечает, что уровень зрелости и заказчиков, и поставщиков растет. Помимо базовых средств информационной безопасности компании внедряют сложные системы защиты, которые должны учитывать особенности бизнес-процессов и бизнес-систем. «Управление ИБ — это процесс. И его нужно строить по общепризнанным стандартам (ISO-27001, ГОСТ) с учетом специфики организации. При оценке эффективности этого процесса также часто учитываются вопросы непрерывности бизнес-деятельности»,— сказал он

Дмитрий Титков, менеджер по работе с финансовым сектором компании Check Point Software Technologies, говорит, что компании ищут способы более эффективной защиты, стремясь при этом к удобству управления и простоте использования. «Сегодня нужно воспринимать комплексный подход к ИБ как некоторую философию системы, которая бы была интеллектуальной и гибкой, при этом сохраняя непрерывными бизнес-процессы. Именно такой подход был применен в этом году компанией Check Point в концепции Software-Defined Protection — новой архитектуре безопасности, которая помогает соответствовать одновременно и размытым границам корпоративного периметра, и динамике эволюции угроз»,— продолжает господин Титков.

ЕВГЕНИЙ ПАВЛЕНКО

Вопросы информационной безопасности становятся только острее

Сегодня стало понятно, что любая защита данных или инфраструктуры — это постоянный процесс, который меняется и совершенствуется во времени (как у заказчика, так и у производителей средств безопасности). Если этого не происходит, появляются дыры в защите.

Аркадий Прокудин рассказывает, что раньше заказчики хотели от систем управления ИБ, чтобы она помогала управлять настройками оборудования из одной точки. Но сегодня задачи куда шире. Современный заказчик не просит, а требует выстроить у него информационную безопасность как процесс и автоматизировать его. А это сделать непросто, потому что в процесс управления ИБ включены и управление активами организации, и управление рисками и множество других подпроцессов.

По мнению Сергея Земкова, управляющего директора «Лаборатории Касперского» в России, странах Закавказья и Средней Азии в настоящее время основа роста рынка ИБ — это комплексные продукты, которые обеспечивают безопасность данных компании во всех аспектах деятельности, имеют централизованное управление, удобны и экономичны.

По его словам, набирают популярность системы Security Intellegence, причем в первую очередь так называемые Security Cloud — защитные решения, находящиеся в «облаке» и доступные заказчикам через интернет. Такие системы, как, Kaspersky Security Network, наделены большим количеством «интеллекта», а их перенос в «облако» позволяет системе оперировать большими объемами данных и получать доступ к большим вычислительным мощностям и, таким образом, быстрее реагировать на самые актуальные угрозы и атаки в киберпространстве. По словам господина Земкова, сегодня уже многие крупные компании принимают решение об использовании подобных интеллектуальных систем внутри собственной IT-инфраструктуры.

Ищи ветра в поле

Вопросы безопасности становятся все острее не только из-за роста активности и организованности киберкриминала. Влияют и другие факторы, о которых рассказал на IDC IT-Security RoadShow в Москве главный исследователь-аналитик IDC Михаил Попов. Среди них: усиливающийся тренд Bring Your Own Device и мобильность, распространение «облаков», повышение активности компаний в социальных сетях. Именно в этих областях, а также в сфере инструментов работы с Big Data аналитик IDC видит поле для деятельности разработчиков средств защиты. Это сегменты, за счет которых рынок ИБ в России и мире будет развиваться в ближайшие годы.

Конфиденциальные данные организаций, которые хранятся на персональных мобильных устройствах, находятся вне контроля ИТ-отделов и остаются крайне уязвимыми. Согласно исследованию Check Point «Влияние мобильных устройств на безопасность информации», каждая шестая компания в мире потеряла в 2012 году от утечек через мобильные устройства более $0,5 млн, а в 42% организаций ущерб превысил $100 тыс.

Драйверами рынка ИБ выступают сегодня решения по защите «облачных» инфраструктур, виртуальных сред, а также мобильных технологий, получающих все большее распространение. Он ожидает, что сохранят свою популярность решения, защищающие от утечки конфиденциальной информации, мошенничества, направленных атак на информационные системы. «Обычно подобные риски возрастают в кризисное время, когда увеличивается конкуренция, происходят слияния и поглощения,— объясняет господин Башлыков.— Также на популярность средств информационной безопасности большое влияние оказывают новостные поводы, появляющиеся периодически в СМИ. Стоит в информационном поле появиться новости о DDoS-атаке или новом вирусе, как заказчики начинают интересоваться техническими средствами, которые уменьшают негативные последствия от действий злоумышленников». На фоне публикаций об отказах в обслуживании сайтов госструктур и телеканалов можно ожидать, что в этом году на соответствующие средства защиты будет ажиотажный спрос. В Национальной ассоциации инноваций и развития информационных технологий (НАИРИТ) подсчитали, что за прошлый год количество DDoS-атак на государственные и коммерческие инфраструктурные институты выросло на 178%, тогда как в предыдущие годы эта цифра сохранялась на уровне 20–30%.

Датчик движения

На фоне общей стагнации экономики РФ и прогнозов по падению объемов рынка информационных технологий в целом рынок информационной безопасности все еще выглядит перспективным.

Михаил Башлыков говорит, что сегмент ИБ традиционно растет примерно в 1,5–2 раза быстрее, чем другие ИТ-услуги «Поэтому снижение темпов для нас не столь драматично. По итогам 2013 года мы ожидаем, что данное направление в КРОК увеличится примерно на 10%. И тенденция к росту сохранится. Конечно, сложно давать четкие прогнозы, но рост, по нашим предположениям, в ближайшей перспективе составит 15–20%»,— заключает он.

Сергей Земков объясняет, что сегмент ИБ продолжает расти, так как защитные решения по-прежнему входят в базовые ИТ-системы для работы любого предприятия. «Вместе с тем мы наблюдаем влияние кризисных тенденций — в частности, они спровоцировали снижение темпа роста на рынке ИБ во второй половине прошлого года. В целом, по нашим оценкам, в итоге за 2013 год рынок вырос не более чем на 10–12%»,— говорит господин Земков.

Несмотря на замедление экономики, связанное с кризисными тенденциями, крупный бизнес и государство продолжат реализацию проектов в области ИБ в нынешнем году.

«Традиционно основными потребителями услуг информационной безопасности являются финансовые организации, операторы связи, крупные торговые сети, развивающие онлайн-торговлю. Эти компании сильно зависят в целом от ИТ, потому простой систем, вызванный, например, DDoS-атакой, может негативно отразиться на всем бизнесе. Для государственных структур вопрос защиты ресурсов также стоит достаточно остро. Жесткие требования регуляторов обязывают их хранить, обрабатывать и передавать информацию должным образом»,— объясняет господин Башлыков.

Дмитрий Титков напоминает также, что компании телекоммуникационной отрасли в погоне за новыми скоростями передачи данных (3G, LTE и т. д.) требуют от поставщиков ИБ все более и более производительных решений. Кроме того, ведущие предприятия нефтегазового сектора традиционно являются активными потребителями решений по информационной безопасности. В последнее время также всерьез озаботились вопросами ИБ государственные и общественные организации, которые все чаще подвергаются атакам по политическим мотивам (так называемый хактивизм).

Господин Земков отдельно отмечает решения для защиты критических объектов и инфраструктуры (сектора энергетики, предприятия транспорта и т. п.). Защищать и использовать решения по безопасности такие предприятия будут все активнее, потому что угрозы для них становятся все более реальными.

Введение требований по уведомлению об инцидентах может стать драйвером развития рынка ИБ. Это позволит увидеть реальную картину по инцидентам и мошенническим действиям в масштабах страны. Следующим шагом, по мнению господина Прокудина, должно быть требование по уведомлению о таких инцидентах в режиме реального времени.

Также в последнее время законодатели взялись за сектор промышленности и критически важных объектов. В этой области господин Прокудин видит потенциал для роста.

То есть российский рынок ИБ, как и в прежние годы, весьма зависим от требований регуляторов. Это означает, что компаниям приходится следовать требованиям ФСТЭК, ФСБ и Банка России. Но выполнения этих требований, как правило, недостаточно для обеспечения реальной безопасности, которая необходима для ведения бизнеса сегодня. Количество угроз растет, но компании стремятся обеспечить защиту, не раздувая штат сотрудников. Поэтому все больше российских заказчиков обращаются за соответствующими решениями к мировым лидерам, которые, в свою очередь, уделяют достаточное внимание вопросам локальной сертификации продуктов.

Аркадий Прокудин рассказывает, что, как правило, развертывание современной системы ИБ происходит в два этапа. Для начала внедряются системы управления логами и системы управления событиями/инцидентами. В этом направлении господин Прокудин обозначает следующих лидеров: IBM QRadar, HP ArcSight и McAfee SIEM. Эти приложения позволяют собирать информацию о состоянии всех информационных систем и систем безопасности в едином месте. Такой подход позволяет видеть полную картину организации, не упуская даже мельчайших моментов. Внедрение систем SIEM позволяет руководителю ИБ и ИТ принимать решения при возникающих инцидентах в кратчайшее время, опираясь на полную информацию.

Вторым этапом внедряются решения следующего интеллектуального уровня — системы автоматизации процессов ИБ и построения систем управления информационной безопасностью. Такие комплексы базируются на решениях Security Information and Event Management (управление событиями и информацией о безопасности) и включают в себя управление рисками и активами, а также отчетностью и инцидентами.

Светлана Рагимова

РЕКЛАМА

ГРУППА КОМПАНИЙ
ТендерПро

www.Tender.Pro
www.teclot.com

Россия
+7(495) 215-14-38
client@teclot.com

Украина
+380 (44) 586-41-09
ukr@teclot.com

Казахстан
+7 (727) 350-73-83
kz@teclot.com

Кыргызстан
+996 (312) 96-16-61
kg@teclot.com

Узбекистан
+998 (90) 986-85-80
+7 (495) 215-14-38 доб. 139
yugai@teclot.com

Таджикистан
+992 (37) 221-22-57
td@teclot.com

Китай
+86 (991)-366-49-49
+86 (185) 990-52-494
china@teclot.com

Поддержка ускорения

Проникновение мобильной связи в России уже несколько лет превышает 150%. Трафик данных в сетях растет, абоненты становятся привередливее, конкуренция усиливается. Меняются потребности операторов в ИТ и их роль в бизнесе.

— сектор рынка —

По данным аналитического агентства ACM-Consulting, в четвертом квартале прошлого года проникновение мобильной связи в среднем по России достигло 170% — около 242,79 млн SIM-карт. Цифра эта растет: в декабре 2012 года проникновение составляло 161,3% — 230,5 млн SIM-карт. Рост продолжается даже в Москве, где под конец прошлого года в активном состоянии находилось 40,29 млн SIM-карт, а проникновение составило 216,6%. Показатели прошлого года для столицы — 37,39 млн и 201%. Это означает, что многие жители страны подключают к мобильной сети больше одного устройства. Увеличение числа абонентов и экспоненциальный рост объемов передаваемых по мобильным сетям данных требуют от мобильных операторов инвестиций в инфраструктуру: модернизацию, обслуживание и ее развитие. Но отбивать эти деньги становится все сложнее. Растет конкуренция — абонентов необходимо удерживать, инвестируя в сервисы, а также поддерживая ожидаемое качество услуг.

Айдын Абжанбеков, директор по развитию бизнеса Ericsson в регионе Северная Европа и Центральная Азия, говорит, что 30% российских пользователей смартфонов готовы сменить оператора, если другой обеспечит им более высокое качество работы в сети. Услуга Mobile Number Portability позволяет теперь сменить оператора, сохранив свой номер, что делает жизнь пользователя проще, но усиливает конкуренцию между телеком-компаниями.

По словам господина Абжанбекова, это требует от операторов внедрения новых востребованных и высокоскоростных сервисов, а также вызывает понятное стремление к максимальной монетизации услуг. То есть, главная задача для телеком-компаний сегодня повышение эффективности бизнеса. И это повлияло на то, какую роль сегодня играют ИТ-подразделения мобильных операторов.

Дмитрий Солодовников, руководитель направления по взаимодействию со СМИ компании МТС, комментирует: «За последние годы сфера ИТ трансформировалась — ИТ-подразделения сотовых операторов прошли путь от сервисных структур к отделам, создающим новые конкурентные преимущества, партнерам бизнеса, а сам ИТ-продукт стал товаром массового спроса и генератором прибыли. Изменились роли ИТ-специалистов: от них теперь требуются большая гибкость и нестандартные решения».

В 2014–2016 годах компания МТС нацелена на реализацию стратегических инициатив в области ИТ. Главная из них — формирование ИТ-архитектуры, которая позволит быстро, качественно и с минимальными затратами отвечать на запросы бизнеса, создавать конвергентные продукты, поддерживать инновации. «Также мы намерены уделять внимание ИТ-решениям в рамках группы компаний МТС, которые позволят добиться синергии от взаимодействия различных активов»,— добавляет господин Солодовников.

В компании «Вымпелком» также работают над выстраиванием новой ИТ-архитектуры. Исполняющий обязанности директора по информационным технологиям «Вымпелкома» Владимир Савкин рассказывает: «Помимо традиционных задач по улучшению качества клиентских сервисов как таковых ИТ играет все более важную роль в предоставлении новых услуг, а также упрощении обслуживания. И тут важна трансформация ИТ-архитектуры из voice-centric (которая, как правило, формировалась в течение последних 10–15 лет) в data-centric с последующей консолидацией Self-Service (сервисы самообслуживания), CRM, биллинговых систем для предоставления гибких предложений, тарифных планов, конвергентных услуг и улучшения качества обслуживания клиентов».

В этом году в «Вымпелкоме» будет продолжаться развитие систем самообслуживания, которые коснутся всех точек контакта с клиентом, в том числе «личного кабинета», мобильных приложений, веб-сайтов. Также развернута работа над запуском ряда уникальных для российского рынка предложений, направленных на упрощение сервисов и повышение удобства использования мобильного интернета.

По свежим данным

Чтобы быстро создавать новые релевантные предложения и сервисы, нужна соответствующая инфраструктура. Но это лишь часть задачи. Важно еще знать, что именно и кому предлагать. Для этого требуется проводить глубокий анализ абонентской базы, выявлять сегменты пользователей, определять их потребности, следить за изменениями их предпочтений. Это требует производительных ИТ-систем, позволяющих обрабатывать и анализировать огромные массивы данных о поведении и предпочтениях абонентов из разных источников практически в режиме реального времени, то есть применять инструменты для работы с Big Data.

К примеру, под брендом МТС помимо услуг сотовой связи сегодня оказывают услуги домашнего интернета и платного ТВ, продают смартфоны в 4 тыс. розничных салонов, предоставляют финансовые услуги. Больше 100 млн клиентов МТС круглосуточно потребляют эти услуги, генерируя гигантский объем данных, которые являются источником ценной информации об интересах клиентов. По словам господина Солодовникова, интеграция систем анализа данных абонентов, централизация биллинга и создание единой конвергентной платформы дают возможность использования проактивного подхода к предоставлению услуг. Инструменты бизнес-аналитики, например, позволяют компании определять групповые модели поведения и формулировать индивидуальные предложения. Например, система класса Real-time Marketing анализирует профиль потребления абонентов и позволяет давать им персональные рекомендации по выбору тарифа, подключению услуг и участию в специальных акциях МТС. С помощью другой системы — Social Network Analysis — МТС анализируют социальные связи групп абонентов и влияют на отток клиентов, фиксируя изменения моделей поведения. Представитель компании говорит, что сейчас именно у МТС минимальный уровень оттока абонентской базы среди основных конкурентов — 9% на конец 2013 года.

Мобильные операторы продолжают активный переход на «облака» и виртуализацию. Ольга Мордкович, директор по информационным технологиям Tele2, говорит, что в ее компании помимо проектов, связанных с консолидацией информационных систем и ИТ-инфраструктуры (в результате объединения с «Ростелекомом»), будет происходить дальнейшее развитие программы виртуализации, проектов по внедрению бизнес-систем, направленных на совершенствование управления и контроля в совместном предприятии, а также направления Big Data.

«Облачные» технологии используются для удовлетворения не только внутренних нужд компаний, но и для предоставления новых услуг клиентам. Например, в МТС уже виртуализировано почти 20% ИТ-окружения, в прошлом году начался переход к системе виртуальных рабочих мест Virtual Desktop Infrastructure и вскоре большая часть из 28 тыс. сотрудников МТС получит виртуальные рабочие столы на основе «облачной» инфраструктуры с использованием программного обеспечения Citrix и VMware. Этот проект планируется завершить к 2017 году, на него будет потрачено около $12 млн. Сколько в итоге сэкономит компания, представитель МТС не сказал. Вместе с тем МТС предлагают «облачный» сервис своим корпоративным клиентам, в пакет включены продукты Google, Microsoft, NEC Corporation. «Мы видим активный рост спроса на „облачные“ услуги за счет прямого доступа к крупнейшей базе корпоративных клиентов в России, который ежеквартально увеличивается в среднем на 50%. В нынешнем году мы продолжим развитие „облачных“ сервисов на базе собственной инфраструктуры, сотрудничая с лидерами в области ИТ-решений по схеме разделения доходов», — комментирует господин Солодовников.

Помимо виртуализации телеком-компании применяют и другие способы снижения затрат на ИТ: централизацию ИТ-функций, стандартизацию ПО и пр.

Светлана Рагимова

«ЛОЯЛЬНОСТЬ АБОНЕНТОВ СЕГОДНЯ ОЧЕНЬ НИЗКА — ОНИ С ЛЕГКОСТЬЮ ГОТОВЫ ПОМЕНЯТЬ ПОСТАВЩИКА УСЛУГ»

Мобильные операторы уже несколько лет пытаются отойти от бизнес-модели dump pipe («труба данных») и зарабатывать не только на передаче байтов. СЕРГЕЙ ЖУЧКОВ, директор по работе с операторами связи компании КРОК, рассказывает о том, как технологии оптимизации и монетизации трафика помогают мобильным операторам.

КРОК

— Насколько сегодня операторы нуждаются в оптимизации трафика?

— Ситуация, в которой сегодня оказались мобильные операторы, очень непростая. Абоненты генерируют все большее количество трафика данных, они стали более требовательны к качеству услуг, к скорости доступа в интернет. Видеоконтент становится все более и более популярным. График роста объемов трафика в мобильных сетях практически вертикальный — по прогнозу Cisco, в 2014–2018 годах эта цифра вырастет более чем в десять раз. Чтобы справиться с этим цунами, операторам необходимо вкладывать значительные средства. Для того чтобы управлять как капитальными затратами на строительство сети, так и окупаемостью, многие операторы используют решения по оптимизации трафика.

— Как технически работает данный класс систем?

— В самом простом случае система исполняет роль простого фильтра, сжимающего контент по определенным правилам и отдающего его абоненту. Более сложный вариант — применение различных параметров сжатия в зависимости от условий радиопокрытия, тарифа абонента и т. д. Например, если у абонента ухудшаются условия приема, то для него будет применяться большее сжатие. Использование систем оптимизации трафика позволяет достичь нескольких целей. О первой мы уже сказали: повышается качество сервиса, ведь сжатый контент быстрее загружается. Вторая цель — планирование развития сети с учетом экономии трафика, которая базируется на усредненных параметрах. В результате можно строить сеть с учетом того, какой объем трафика она фактически пропускает. Кроме того, на базе системы операторы могут внедрить различные дополнительные сервисы для монетизации трафика.

— Расскажите о возможностях монетизации с использованием данных технологий.

— Идея заключается в том, что на экране пользователя появляется дополнительное меню, а точнее, tool bar — панель инструментов, предоставленная оператором. Оператор может добавлять на нее практически любые функции, например строку поиска. Для пользователя, который работает с планшета, эта панель инструментов будет очень полезной, ведь у него нет более простой возможности увидеть свой баланс, контролировать потребляемый трафик, менять настройки и пр. Для этого ему необходимо зайти на сайт оператора и авторизоваться в «личном кабинете». Предоставив абоненту панель инструментов с набором полезных функций, оператор может тем самым повысить его лояльность. Важно, что от пользователя не требуется никаких действий, ему не нужно искать специальное ПО и устанавливать его. За пользователя это делает оператор.

— В чем именно заключается возможность дополнительной монетизации?

— Оператор может встраивать в панель инструментов доступ к сервисам своих партнеров. Например, установить поисковую строку «Яндекса», а также разместить иконки своих дополнительных платных сервисов. Абоненты часто попросту не знают, что могут, например, купить дополнительный пакет трафика. А если и знают об этой возможности, то не понимают, как это сделать. Представьте себя на месте пользователя, превысившего свой лимит по трафику. Оператор автоматически снизил скорость его соединения. Если дать пользователю возможность докупить пакет услуг одним кликом через панель инструментов, то он в большинстве случаев это сделает. Фактически для оператора это способ получения дополнительной прибыли.

Кроме того, данный класс систем позволяет оператору встать в центр цифровой экосистемы, в которой существует пользователь. Оператор имеет возможность первым захватить внимание потребителя и направить его по нужному маршруту. Это открывает огромное количество возможностей для дополнительного заработка. Изучая поведение абонента в сети можно делать ему индивидуальные предложения, рекомендовать интересные ему товары, поставляемые партнерами и т. д.

— В России не так много мобильных операторов, которые могли бы стать вашими клиентами. С кем-то уже заключены контракты?

— Да, мы проводим пилотные внедрения в сетях некоторых операторов. Но в качестве клиентов мы рассматриваем не только их, но и интернет-провайдеров, которых в России гораздо больше, чем мобильных операторов.

Интервью взяла Светлана Рагимова

Доверяй, но проверяй

Условия рынка заставляют банки пересматривать свои ИТ-бюджеты и инвестировать только в то, что необходимо и наиболее эффективно решает задачи бизнеса. При этом банки являются одними из ключевых клиентов ИТ-компаний.

— сектор рынка —

Сегодняшнее время участники рынка и аналитики характеризуют как смутное для банковской индустрии. В 2014 году Центробанк продолжит политику оздоровления отрасли. По прогнозу рейтингового агентства «Эксперт РА», кандидатами на отзыв лицензий в текущем году могут оказаться порядка 50 банков. Именно это количество финансовых компаний соответствует хотя бы одному из критериев на вылет. Среди них: достаточность капитала менее 11%, объемы капитала менее 300 млн руб. к 1 января 2015 года, признаки большого количества сомнительных операций.

Обстановка усугубляется тем, что спрос на кредиты начинает уменьшаться, а клиенты стараются перейти в крупные банки, имеются проблемы с ликвидностью, растут объемы проблемных активов.

По прогнозу «Эксперт РА», по итогам нынешнего года активы и кредитный портфель в целом по рынку прибавят не более 11% и 13% соответственно. Для сравнения: в прошлом году эти показатели составляли 15% и 17%. Впервые за последние пять лет снизилась совокупная прибыль банковского сектора с 1011,9 млрд руб. в 2012 году до 993,6 млрд в прошлом году. Наряду с этими тенденциями конкуренция между банками обостряется.

Полное досье

В этих непростых условиях банки стремятся к внедрению и использованию информационно-технических средств, которые позволили бы сократить затраты, при этом поддержать лояльность пользователей и повысить продажи за счет правильно сконфигурированных предложений для клиентов.

Евгений Закрепин, первый заместитель управляющего директора компании «Техносерв», говорит, что стремление к экономии средств, в частности желание снизить стоимость обслуживания каждого клиента, проявилось пару лет назад в том, что банки начали активно внедрять единые CRM-системы. Это снимает необходимость обращения к множеству разных программ во время общения с клиентом: вся информация о нем доступна в одном приложении, причем независимо от того, через какой канал коммуникаций он обратился.

Такие возможности достигаются, только если банк позаботился о создании интегрированной информационной системы всего своего предприятия. По словам господина Закрепина, именно внедрение интеграционных шин — это то, чем продолжает заниматься банковская отрасль в 2014 году.

Интернет-банкинг продолжит активно развиваться потому, что это гораздо менее затратный способ взаимодействия банка с потребителем по сравнению с оффлайновыми отделениями. Так, по планам ВТБ 24 к 2016 году банк будет обслуживать через онлайн-кабинет 4 млн человек, что в три раза больше, чем по показателям второго полугодия 2013 года.

По данным CNews Analytics, сегмент решений для дистанционного банковского обслуживания (ДБО) физических лиц все еще содержит значительный потенциал роста. В 2013 году всего 85% банков, входящих в топ-100, использовали такие системы. Заметно выросла популярность решений для мобильного банкинга: их в 2013 году используют в 64% банков топ-100 против 54,1% годом ранее.

Опасные связи

По данным исследования B2B International, проведенного совместно с «Лабораторией Касперского» в 2013 году, 98% пользователей используют онлайн-финансовые сервисы, при этом почти треть из них не проверяет те сайты, на которых вводит свою конфиденциальную информацию.

«В 2013 году нашими продуктами было заблокировано 1,9 млн атак банковским вредоносным ПО»,— рассказывает Владимир Заполянский, руководитель отдела технологического позиционирования «Лаборатории Касперского».

Согласно тому же исследованию, за предшествующий год с киберугрозами, нацеленными на получение доступа к онлайн-счетам, в мире столкнулись 62% пользователей, а в России — 74%. В 2013 году произошли значительные изменения, связанные с усовершенствованием законодательства, активными действиями правоохранительных органов разных стран, которые вывели из строя некоторые наиболее одиозные преступные группы. Тем не менее, как рассказывает господин Заполянский, место крупных игроков криминального рынка стали занимать мелкие группировки и все большее количество мошенников стало обращать внимание на финансовые организации. В целом мировая тенденция такова, что системы ДБО банков атакуются все чаще.

При этом банковские угрозы быстро эволюционируют не только с точки зрения их количества, главное — они становятся все более сложными. Безусловно, банки осуществляют ряд эффективных мер по борьбе с онлайн-мошенничествами, такие, как CVV2, двухфакторная аутентификация, токены и другие, но, по мнению господина Заполянского, для эффективного противостояния современным угрозам этого не достаточно.

«Финансовым организациям необходим комплексный подход, который бы защищал онлайн-операцию и на конечном устройстве пользователя, и на стороне банка»,— говорит господин Заполянский.

Помимо направлений, связанных с обслуживанием потребителей и обеспечением защиты, банковский сектор, как и раньше, будет продолжать выделять бюджеты на соответствие требованиям регуляторов. В целом игроки ИТ-рынка рассчитывают на то, что бюджеты кредитных организаций на ИТ в 2014 году не уменьшатся.

Светлана Рагимова

«В 2013 ГОДУ ОБЪЕМ КРЕДИТОВ С ПРИЗНАКАМИ МОШЕННИЧЕСТВА ВЫРОС БОЛЕЕ ЧЕМ ВДВОЕ»

АНДРЕЙ ХРУЛЕВ, директор департамента биометрических и комплексных систем безопасности группы компаний «Техносерв», рассказывает корреспонденту «Ъ-ИТ» МАРИИ АНАСТАСЬЕВОЙ о технологии распознавания лиц, которую применяет Сбербанк для выявления мошенников.

«ТЕХНОСЕРВ»

— Зачем Сбербанк решил внедрить систему распознавания лиц?

— Уже несколько лет подряд сегмент потребительского кредитования для банков является как драйвером роста, так и зоной риска. Согласно статистике Национального бюро кредитных историй, в 2013 году объем кредитов с признаками мошенничества вырос более чем вдвое — до 153 млрд руб., а количество потенциальных мошенников может превышать 600 тыс. человек. Это подталкивает банки использовать новые высокотехнологичные инструменты для проверки потенциальных заемщиков. У Сбербанка накоплена большая база по существующим клиентам во всех регионах, которая позволяет проводить качественный анализ. Крупный банк ежедневно рассматривает до нескольких десятков тысяч заявок на выдачу кредитов, а конкуренция диктует жесткие сроки принятия банком решения по выдаче займа. Система распознавания лиц дает целый ряд преимуществ по выявлению мошенничеств, с которыми трудно в таком объеме справиться команде андеррайтеров. Например, система точно отсечет попытку получения кредита по украденному паспорту с переклеенной фотографией или даже той же (мошенник визуально похож на владельца паспорта) или отследит изменение в паспорте одной буквы фамилии. В систему заложено более десятка сценариев проверки, и этот список постоянно пополняется.

— Внедрение реализовано исключительно силами «Техносерва»?

— Проект выполнен полностью силами группы компаний «Техносерв» на основе собственного продукта «Каскад-Поиск». В его разработку компания вложила более 100 млн руб. Над проектом работал «Рексофт» — разработчик ПО, входящий в группу.

— С какими сложностями пришлось столкнуться во время внедрения?

— Это первый подобный проект в России, наложенный на федеральный масштаб Сбербанка. Количество трансакций (десятки тысяч в день) и размер базы, с которыми работает система, колоссальны. Так как система работает параллельно с другими аналитическими системами, перед нами было поставлено очень жесткое условие по скорости ответа по идентификации. Благодаря ряду инновационных решений сравнение по всем базам проходит в течение нескольких секунд (хотя каждая заявка прогоняется почти по десятку баз, некоторые из которых имеют размер, близкий к 1 млн объектов). Для достижения этого результата команде «Техносерва» пришлось погрузиться не только в бизнес-процессы банка, но и в математику процесса распознавания. Ведь силовым структурам, для которых изначально был разработан «Каскад-Поиск», такие скорости были не нужны. В итоге нами был достигнут результат более 1,5 млн сравнений на одном процессоре в секунду. Отмечу, что система работает в полностью автоматическом режиме, то есть ни одна операция не выполняется вручную. Этот проект фактически открывает целый сегмент на отечественном рынке биометрической идентификации, в котором Сбербанк стал первопроходцем.

— Как долго реализовывался проект? Сколько департаментов клиента затронул?

— Проект затронул 17 территориальных подразделений банка и занял почти два года, причем львиная доля времени ушла на аналитику, так как внедрение этой системы предполагает глубокую интеграцию в бизнес-процессы банка и создание тех самых правил и сценариев, по которым банк считает необходимым осуществлять проверку.

— Насколько точны подобные технологии распознавания лиц? Где еще могут применяться?

— Точность распознавания зависит как от качества движка системы, так и в значительной степени от качества входных данных (сканов документов, настройки камер). Если говорить о финансовом секторе, то возможности систем распознавания могут быть востребованы в сегменте депозитов, ведь получать вклад может прийти совершенно другое лицо. Такие системы позволяют эффективно решать не только задачи обеспечения безопасности покупателей, например обнаружение оставленных предметов, распознавание лиц посетителей и выявление среди них лиц, находящихся в розыске. Также они предоставляют уникальную информацию для аналитиков, например подсчет числа посетителей, определение траекторий движения покупателей и соответственно выявление зон наибольшего интереса, контроль работы персонала и т. д. Распознавание лиц используется для обеспечения транспортной безопасности — в частности, «Техносерв» сейчас участвует в проекте по проектированию такой системы в интересах Московского метрополитена. Такие технологии уже давно работают в штатном режиме в Великобритании и других странах. Общемировой объем данного рынка исчисляется $3–4 млрд с ростом 20–25% год.

Борьба с энтропией

— обзор рынка —

с13

«Для IBS одна из главных точек роста — это прежде всего все, что связано с интеграцией и анализом больших объемов бизнес-данных — Big Data,— рассказывает Сергей Мацоцкий.— В этом направлении уже появились и растущий спрос, и понятное продуктовое предложение, и первые проекты. С точки зрения инфраструктурной интеграции мы делаем ставку на строительство частных „облаков“».

По оценкам IDC, среднегодовые темпы роста сегмента «облачных» решений до 2017 года составят 49%, что является самым высоким показателем среди всех направлений отрасли. Точных цифр по развитию «облаков» в России в прошлом году у экспертов пока нет. Однако уже сейчас можно сказать, что отдельные компании показали очень высокий рост в этом сегменте. Так, по данным IDC, доход Microsoft от продаж «облачного» решения Office 365 в прошлом году показал примерно пятикратный рост, для сервиса MS Azure эта цифра еще выше. Такие российские компании, как «Мой склад» («облачные» решения для управления логистикой) или Parking.ru (реализует проекты по построению всех типов «облаков»), в прошлом году увеличили свой бизнес в разы. Говоря о возможностях для компаний в кризисных условиях, Борис Бобровников отмечает, что несомненный рост будут показывать такие направления, как аутсорсинг, решения в области информационной безопасности, услуги в телекоммуникационной отрасли. «Как всегда, в кризис востребованы услуги, повышающие эффективность бизнеса,— считает он.— Еще одна тенденция: российский рынок постепенно переходит на модель мультисорсинга, когда несколько интеграторов решают задачи заказчика, работая в команде».

Другой особенностью российского ИТ-рынка в ближайшем будущем, по мнению председателя правления группы «Астерос» Юрия Бякова, станет его переменчивость как с точки зрения лидеров рынка, так и основных заказчиков. «Прежде всего следует признать отсутствие явного и неоспоримого лидера в том же сегменте системной интеграции. Да, мы можем замерять выручку, оборот или другие финансовые показатели, но стабильные позиции год от года удерживают единицы, а в тройке лидеров постоянно происходят изменения,— рассуждает он.— Также мы наблюдаем медленное нивелирование понятия „якорный заказчик“ и появление новых возможностей для бизнеса в тех клиентах, с которыми раньше в силу различных барьеров это было бы невозможно. Что произошло? На фоне экономических встрясок возрос уровень конкуренции, интеграторы стали в хорошем смысле более голодными, что потребовало от них активных действий в завоевании новых рынков. В результате сложилась ситуация, при которой на коне сегодня вполне может оказаться интегратор, прежде не имевший опыта работ с компанией-заказчиком, но при этом готовый предложить свои компетенции, оптимальную стоимость услуг и качество реализации проекта».

Государство и ИТ

Отдельного внимания заслуживают отношения ИТ-компаний с государством, которое по-прежнему остается крупнейшим заказчиком для российских компаний. Однако и здесь не все безоблачно.

«Мы отмечаем активное появление в последние годы собственных ИТ-структур — „карманных интеграторов“ — у большинства крупнейших корпоративных заказчиков. Все чаще в крупные федеральные проекты назначаются единственные исполнители — государственные институты и специализированные интеграторы. Что это означает для рыночных ИТ-компаний? Конечно, ограничение возможностей работы с крупнейшим ИТ-клиентом, ведь сегодня им является государство в лице органов власти и госкорпораций»,— делится опасениями Тагир Яппаров.

Однако не все участники рынка разделяют эти тревоги. «Про причины неуспешности „карманных“ ИТ-компаний уже много раз говорилось. Я думаю, эта мода постепенно пройдет,— считает Сергей Мацоцкий.— Что касается закупок госведомств, то здесь подавляющее большинство проектов выполняется силами коммерческих поставщиков. К счастью, государство пока не пытается монополизировать сферу ИТ-госпроектов. Новый закон о федеральной контрактной системе №44-ФЗ, я надеюсь, устранит перекосы и злоупотребления, которые были раньше при проведении государственных конкурсов — это дополнительно улучшит положение с конкуренцией в этом секторе. Думаю, государство останется в ближайшие годы крупнейшим заказчиком на российском рынке ИТ».

Подобную точку зрения разделяет и Юрий Бяков из «Астероса»: «Государственные бюджеты независимо от появления сита в виде „карманных“ структур все равно будут занимать значительную долю в структуре выручки крупных интеграторов. На информатизацию запланировано израсходовать в 2014 году около 83 млрд рублей, и я замечу, что тот объем задач, впечатляет не меньше этой цифры… Эти долгосрочные задачи должны и будут решаться в сотрудничестве государства и бизнеса, имеющего опыт реализации подобных задач».

По мнению председателя консультативного совета компании «Техносерв» Сергея Корнеева, именно федеральные программы наряду со сложными интеграционными проектами продолжат оставаться точками роста на ближайшие годы, среди них: программа «Безопасный город», аутсорсинг созданных систем, работа над проектами, гарантирующими доступность и сохранность данных, причем от физического создания ЦОДа до внедрения систем виртуализации и „облачных“ структур».

Появление так называемых карманных интеграторов усугубляет острую кадровую проблему, давая дополнительный импульс нерыночному росту зарплат.

«Сервисный бизнес российских ИТ-игроков в большинстве случаев развивается так, что увеличение объемов бизнеса требует соответствующего роста числа сотрудников. А кадрового резерва у отрасли практически нет. Дефицит персонала на ИТ-рынке становится чуть ли не ключевым сдерживающим фактором развития отрасли и приводит к неоправданному росту издержек за счет постоянного увеличения зарплат и дополнительных расходов на поиск и переподготовку ИТ-специалистов до нужного профессионального уровня,— поясняет Тагир Яппаров.— „Карманные интеграторы“ активно скупают специалистов, предлагая зарплаты в разы больше рыночных».

Все, что не убивает, делает нас сильнее

Прошлый год и первые месяцы текущего уже дали ясно понять, что время стремительного роста доходов ИТ-компаний на фоне восстановления экономики после кризиса пятилетней давности и налаженной схемы работы системных интеграторов безвозвратно ушло. Кроме того, модель бизнеса, при которой системный интегратор выступал фактически в роли перепродавца оборудования, оказывая услуги по установке, разработке ПО и обслуживанию иностранного «железа», также перестает быть эффективной. Однако этот непростой этап в жизни ИТ-компаний по счастливой случайности совпал со стремительным развитием новых технологий и связанными с ними структурными изменениями рынка в целом.

«Ситуация на российском корпоративном ИТ-рынке непростая. В то же время можно предположить, что в результате проходящей трансформации через несколько лет мы получим более сильный и зрелый национальный ИТ-рынок. У российских ИТ-компаний есть достаточно интересные возможности по реализации новых стратегий развития»,— находит повод для оптимизма Тагир Яппаров.

Речь идет о разработке собственных продуктов и технологий, так как будущее за теми компаниями, которые смогут предложить заказчику собственные решения, разработанные на основе глубокой экспертизы. Кроме того, по мнению председателя совета директоров «АйТи», компаниям необходимо расширять географию присутствия, создавая продукцию, ориентированную на экспорт. «По данным РУССОФТ, объем экспорта из России ПО и услуг по его разработке достиг в 2013 году $5 млрд, что вполне сравнимо с потреблением ПО на внутреннем российском рынке»,— напоминает он.

Александра Ромова

Вычислительная инфраструктура — это головоломка. Как сложить, чтобы получить максимальную эффективность? Как добавить элементы, не останавливая бизнес-процессы? Как рассмотреть на практике варианты, не трогая «живую» инфраструктуру?

В Центре решений КРОК на базе технологий EMC собрана полная линейка инфраструктурных решений EMC. На тестовой площадке Вы сможете смоделировать инфраструктуру, используя в том числе такие продукты, как: Vblock, Data Domain, VNX, Avamar, RecoverPoint, и получить демо-доступ к их функционалу. Пусть сложные головоломки станут для Вас простым хобби.

КРОК
EMC² BUSINESS PARTNER

111033, Москва, ул. Волочаевская, д.5, к.1
T: (495) 974 2274 | Ф: (495) 974 2277
E-mail: croc@croc.ru
www.croc/sc

Реклама

«Тематическое приложение к газете «Коммерсантъ» («Информационные технологии»). Учредитель: ЗАО «Коммерсантъ. Издательский дом». Адрес: 127055, г. Москва, Тихвинский пер., д. 11, стр. 2. | **Владимир Желонкин** — президент ИД «Коммерсантъ» | **Павел Филенков** — генеральный директор ИД «Коммерсантъ» | **Азер Мурсалиев** — шеф-редактор ИД «Коммерсантъ» | **Павел Кассин** — директор фотослужбы | **Валерия Любимова** — коммерческий директор ИД «Коммерсантъ». **Рекламная служба:** Тел. (499) 943-9108/10/12, (495) 101-2353 | **Алексей Харнас** — руководитель службы «Издательский синдикат» | **Светлана Рагимова** — выпускающий редактор | **Наталия Дашковская** — редактор | **Сергей Цомык** — главный художник | **Виктор Куликов** — фоторедактор | **Екатерина Бородулина** — корректор | **Адрес редакции:** 125080, г. Москва, ул. Врубеля, д. 4. Тел. (499) 943-9724/9774/9198