ГАЗЕТА ДЛЯ КОРПОРАТИВНЫХ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И РЕШЕНИЙ

PC WEEK RUSSIAN EDITION

СК ПРЕСС

ЕЖЕНЕДЕЛЬНОЕ ИЗДАНИЕ • 27 АПРЕЛЯ — 10 МАЯ • 2010 • № 15-16 (717-718) • МОСКВА

http://www.pcweek.ru

И снова о Сколкове

ДЕНИС ВОЕЙКОВ

Через несколько дней после того, как президент страны 18 марта определил местом строительства будущего инограда подмосковное Сколково, наша редакция решила провести на

ИННОВАЦИИ

эту тему опрос читательской аудитории.

Андрей Шторх: "Не нравится Сколково? А кому-то не нравятся свиные хрящики... Вопрос вкуса"

Примерно тогда же руководителем проекта с российской стороны был назначен глава группы компаний "Ренова" Виктор Вексельберг, и на проведенном по этому случаю тематическом заседании круглого стола в "Росбалте" у общественности появилась возможность ознакомиться с первой реакцией одного из членов правления группы.

Пришло время сопоставить сведения.

Мнения читателей PC Week/RE

Наиболее популярным ответом на вопрос, где имеет смысл строить русскую Кремниевую долину, у наших респондентов оказался такой: "На базе или вблизи существующего регионального научного центра" (59,56%). Примечательно, что на втором месте, хоть и с большим отрывом, следует ответ, формально одобряющий президентский выбор: "В Сколкове или ином месте вблизи или на территории столицы" (15,85%). Последние места достались ответам "нигде; такой проект не нужен" (12,02%) и "в крупном региональном городе" (6,56%). Собственные варианты ответа предложило 13,11% респондентов. Из них более четверти считают, что строить инноград нужно в Зеленограде. Также упоминались новосибирский Академгородок, Долгопрудный, Жуковский, Воронеж и Казань. В качестве аргументов практически во всех случаях выступают уже имеющиеся в том или ином месте ресурсы: инфраструктура, коммуникации, кадры, научный потенциал, дешевое высококачественное жилье, низкий уровень зарплаты потенциальных сотрудников, близость вузов.

В следующих трех вопросах предлагаемые ответы не исключали друг друга, поэтому респонденты могли выбрать сразу несколько из них. Так, из числа условий, необходимых для успешной реализации проекта, жесткий контроль за выделением и использованием финансовых средств отметило 73,22% опрошенных; 66,12% обратило внимание на необходимость четкой программы проекта; 46,45% — на важность бесперебойного финансирования и 38,80% — на наличие политической воли первых лиц государства.

Собственные формулировки ответов выбрало 15,85% респондентов, и их мне-

ПРОДОЛЖЕНИЕ НА С. 5 ▶

C – значит Cloud

ЛЕВ ЛЕВИН

Широкая популярность облачных вычислений привела к появлению нового класса серверов. В обслуживающих облака вычислительных системах резервирование реализовано только на программном

СЕРВЕРЫ

уровне, и если какой-то узел такой системы выйдет из строя, то его нагрузка перераспределяется между другими узлами облака. Отказ от традиционного для стоечных серверов применения жестких дисков с горячей заменой и резервирования блоков питания и вентиляторов позволяет уменьшить как общую стоимость вычислительной системы, так и ее энергопотребление, а также компактнее разместить процессорную мощность.

В недавно представленной системе для облачных вычислений Fujitsu Primergy CX1000 S1 с целью повышения эффективности охлаждения сами вычислительные узлы лишены вентиляторов, зато в верхней части стойки размещены два мощных вентилятора, которые выбрасывают горячий воздух от узлов вверх. Как утверждает Fujitsu, такой подход (компания называет его Cool Central, централизация охлаждения) позволяет отказаться от организации горячих коридоров в ЦОДе и размещать стойки "спина к спине" (заднюю стенку стоек CX1000 закрывает перфорированная металлическая панель), экономя до 40% площади ЦОДа и до 20% снижая затраты на энергопотребление и охлаждение по сравнению с традиционной схемой охлаждения серверов в стойке. Очевидно, что обратной стороной Cool Central является увеличение требований к высоте потолков, поэтому далеко не все существующие ныне ЦОДы подойдут для размещения Primergy CX1000 S1.

В Fujitsu Primergy CX1000 S1 охлаждение вычислительных узлов обеспечивают два мощных вентилятора, установленные в верхней части стойки

В стойке Primergy CX1000 S1 устанавливается 38 вычислительных одноюнитовых узлов Primergy CX120 S1 с двумя процессорами Intel Xeon 5500 или 5600, оперативной памятью 16 либо 64 Гб и одним либо двумя 2,5-дюймовыми жесткими дисками SATA по 500 Гб без поддержки горячей замены, а также с сетевым слотом расширения PCI и гигабитной картой Ethernet. При выходе из строя узел просто заменяется в горячем режиме на запасной. Стойка также оборудуется одноюнитовым 48-портовым гигабитным Ethernet-коммутатором Brocade FCX648S, который реализует обмен данными между вычислительными узлами и внешней локальной сетью.

ПРОДОЛЖЕНИЕ НА С. 23 ▶

В НОМЕРЕ:

ISSN 1560-6929

9 771560 692004 10016

ПОДПИСНОЙ ИНДЕКС 32485 (по каталогу ЦРПА "Роспечать")

Visual Studio 2010 стартует в мире и в России

АНДРЕЙ КОЛЕСОВ

Скорее всего, это просто совпадение, но все же весьма символичное: официальное объявление новой версии платформы разработки Microsoft — Visual Studio 2010 — и ее традиционного спутника .NET Framework

ИНСТРУМЕНТАРИЙ

4.0 пришлось на 12 апреля. Конечно, по уровню общественного внимания данный факт намного уступает выпуску массовых продуктов, таких как Windows или Office. Но по сути, по своему внутреннему влиянию на возможности эффективного использования ИТ, он вполне может претендовать на одно из главных событий в текущем календарном году для Microsoft. Ведь речь идет о продукте, который наряду с настольной и серверной Windows составляет основу технологической программной платформы корпорации.

Visual Studio 2010 имеет рабочий номер версии 10 — юбилейный в последовательности средств разработки Microsoft для Windows. Возможно, именно круглый номер повлиял на то, что анонс продукта на этот раз приобрёл небывалый размах. Центральные события проходили в Лас-Вегасе (США), где состоялась трехдневная конференция Developer Platform &

Брайан Харри: "Главная задача Visual Studio 2010 заключается в том, чтобы объединить усилия разных категорий специалистов в рамках общего процесса создания ПО"

Tools Launch Event, в ходе которой новое ПО представил президент подразделения Servers and Tools Business корпорации Microsoft Боб Муглиа. Подобные мероприятия-представления прошли и по всему миру, в том числе и в России, причем наша страна, кажется, впервые опередила США: когда началась презентация в Москве, в Лас-Вегасе было еще 11 апреля.

Московское событие вызвало интерес, какого, похоже, организаторы и сами не ожидали: зал конференц-центра, рассчитанный на 500 человек, не смог разместить всех пришедших; правда, эта проблема довольно быстро была решена путём оперативной установки больших мониторов и стульев в холлах центра.

Главной фигурой российского запуска стал приехавший из США Брайан Харри, ведущий эксперт (Technical Fellow) компании Microsoft, который уже много лет руководит группой разработчиков одного из ключевых компонентов всей платформы Visual Studio — средства поддержки групповой работы Team Foundation Server (TFS). С его визитом на московскую конференцию тоже произошла накладка: он приехал только к окончанию пленарного заседания (задержался самолет из США), но сотрудники российского офиса Microsoft уверенно продержались до подхода главных сил. По завершении мероприятия московская команда специалистов Microsoft во главе с Брайаном Харри отправилась в презентационное турне: сначала в Санкт-Петербург, оттуда в Екатеринбург.

На протяжении всей истории Visual Studio развитие этого продукта направлено на обеспечение создания все более сложных приложений, что обусловлено необ-

ПРОДОЛЖЕНИЕ НА С. 5 ▶

Доступная замена отслуживших серверов

Вы знали, что замена старых серверов серверами IBM System x3650 M2 Express на базе процессора Intel® Xeon® серии 5500 позволит значительно сократить текущие расходы на ИТ?
И вот как: **1.** Благодаря более высокой вычислительной мощности для работы приложений требуется меньше серверов. **2.** При использовании меньшего количества серверов сокращаются затраты на приобретение лицензионного программного обеспечения. **3.** Расширенные возможности системного администрирования позволяют снизить эксплуатационные расходы. **4.** Новые энергосберегающие серверы способствуют уменьшению затрат на энергопотребление и охлаждение. Делать больше с меньшими ресурсами – сейчас это важно, как никогда. И добиться этого теперь проще, чем когда-либо, – с помощью специалистов и бизнес-партнеров IBM. Хотите узнать, как благодаря IBM System x инвестиции окупаются всего за три месяца?[1] Посетите **roianalyst.alinean.com/stgi**

Мощный.
Интеллектуальный.

IBM System x3650 M2 Express

От 89 403 руб.*

P/N: 7947PGG

До двух процессоров Intel® Xeon® серии 5500

16 разъемов DIMM[2] 1 333 МГц DDR-3 RDIMM[3] (максимум – 128 ГБ)

Энергосберегающий блок питания на 675 Вт с КПД 92%, 6 вентиляторов, альтиметр

IBM ServicePac: выезд инженера и отправка запасных частей в течение 24 часов**; P/N: 65Y0979 – 9 564 руб.*

IBM System x3400 M2 Express

От 55 178 руб.*

P/N: 7837PBP

До двух процессоров Intel® Xeon® серии 5500

12 разъемов DIMM[2] 1 333 МГц DDR-3 RDIMM[3] (максимум – 96 ГБ)

IBM ServicePac: гарантированное время восстановления и отправка запасных частей в течение 24 часов, обслуживание – 24 часа**; P/N: 51J9366 – 17 274 руб.*

IBM System Storage DS3400 Express

От 120 627 руб.*

P/N: 172641X

Внешняя дисковая система хранения с интерфейсом Fibre Channel[4] 4 Гбит/с

Масштабируется до 5,4 ТБ при использовании дисков SAS[5] емкостью 450 ГБ с возможностью «горячей» замены

Или до 12 ТБ при использовании дисков SATA[6] емкостью 1 ТБ с возможностью «горячей» замены

Подробная информация о наших продуктах и бизнес-партнерах – по телефонам:

8 (495) 258 63 48, 8 800 2006 900
(звонок по России бесплатный)
ibm.com/systems/ru/express1

[1] Информация о методике расчета коэффициента окупаемости инвестиций приведена на ibm.com/systems/ru/express/legal. [2] DIMM – модуль памяти с двухсторонним расположением микросхем. [3] RDIMM – регистровый модуль памяти с двухсторонним расположением микросхем. [4] Fibre Channel – волоконно-оптический канал. [5] SAS – последовательный интерфейс. [6] SATA – последовательный интерфейс IDE (IDE – параллельный интерфейс подключения накопителей).
* Все указанные цены – рекомендуемые розничные цены для базовой конфигурации, приведены исключительно для информационных целей и не являются офертой. Цены не включают налоги и таможенные платежи, а также могут меняться, в частности при изменении курса доллара США к российскому рублю. За информацией об актуальных ценах обращайтесь к бизнес-партнерам IBM в вашем регионе: www.ibm.com/ru/partners. IBM не несет гарантийных обязательств по отношению к продуктам или услугам, предоставляемым третьими лицами, включая продукты с пометкой ServerProven или ClusterProven. Прочая информация о гарантийных условиях приведена на странице: www.ibm.com/ru/services/gts/ma/warranty.html, о пакетах расширения гарантийного обслуживания ServicePac – на странице: www.ibm.com/ru/services/gts/ma/servicepac. ** Уточните список городов, в которых данная услуга доступна.

"Университетский кластер": курс на облака

ДЕНИС ВОЕЙКОВ

Учредители программы "Университетский кластер" подвели ее промежуточные итоги на тематическом круглом столе, приуроченном к международной конференции в Москве "Облачные вычисления: образование, исследования, разработки". По убеждению организаторов, именно совместная работа территориально разобщенных специалистов станет основным направлением развития проекта.

КОНФЕРЕНЦИИ

"Университетский кластер" была запущена в сентябре 2008 г. компанией HP, Институтом системного программирования (ИСП) РАН и Межведомственным суперкомпьютерным центром (МСЦ) РАН при участии национального оператора связи "Синтерра". Целью программы было предоставление российским вузам возможности повысить уровень использования параллельных и распределенных вычислений в их образовательной и научно-исследовательской деятельности. На конкурсной основе 12 университетов получили в свое распоряжение кластеры с пиковой производительностью 0,3 Тфлопс, остальные участники — доступ к мощностям суперкомпьютера в ресурсном центре МСЦ РАН.

Виктор Иванников: "Проект будет развиваться в первую очередь в направлении облачных вычислений. Это выгодно для бизнеса. Это новые возможности для образования и науки"

Как отмечают организаторы, основной задачей первого этапа проекта (1,5—2 года), которую к настоящему моменту фактически удалось решить, было создание мощной инфраструктуры, объединяющей университеты и научные организации (их общее число уже перевалило за 60 и продолжает расти) посредством сети передачи данных со скоростью соединения до 10 Гбит/с.

В какой-то момент рамки программы были расширены, и, как уверяет генеральный директор "Синтерры" Виталий Слизень, чтобы сейчас бесплатно подключиться к локальной сети "Университетского кластера", вузу достаточно просто оформить заявку.

Этот факт послужил поводом для дискуссии, которую г-н Слизень условно назвал "курица или яйцо" (что кого подстегивает — ресурсы появление разработок или задачи появление ресурсов; нужно ли предоставлять вузам вычислительные мощности, если они не в состоянии обосновать необходимость в них). Рассуждая на эту тему, он склонен был утверждать, что сегодняшний телеком уже дорос до того состояния, когда простое предоставление каналов связи себя исчерпало, и речь должна уже вестись о создании на ее базе информационных систем и развития инноваций. Соответственно каналы связи пора сравнивать с электросетью: розетка на 220 В должна быть в каждом доме. Формула "купи чайник, тогда установим розетку" неверна. И человек должен платить не за проведенную фазу, а за вскипяченную чайником воду.

В соответствии с этой философией в рамках "Университетского кластера" "Синтерра" стала на равных условиях (вне зависимости от географии) подключать к своей сети все заинтересованные вузы. И, как уверяет г-н Слизень, эта стратегия себя оправдывает. В первый год университеты смотрели на появившиеся ресурсы с удивлением или даже страхом, а сейчас начинают ими пользоваться.

По его словам, в 2009 г. в сеть было интегрировано 30 университетов. За первые три месяца текущего года — еще 12. К июню их общее число должно удвоиться, и дальнейшее удвоение состава участников проекта, по оценкам г-на Слизеня, будет происходить каждый год.

Виталий Слизень: "Телеком пора сравнивать с электросетью — розетка 220 В должна быть в любом помещении. Формула "купи чайник, установим розетку" неверна"

Более того, к настоящему моменту проект перестает быть сугубо российским — в ближайшее время к нему примкнут организации из Белоруссии и Польши, а в обозримом будущем — из Украины и Казахстана.

С основной мыслью г-на Слизеня полностью согласен генеральный директор HP в России (компания предоставила проекту свои кластеры) Александр Микоян. По его мнению, именно ресурсы порождают задачи, и только получая технику, люди начинают действительно чувствовать вкус к вычислениям.

Кстати, расширение состава участников может произойти и в стане организаторов — по уверению директора по технологической политике Microsoft в России Олега Сютина, "Университетский кластер" можно было бы объединить с научными сообществами корпорации. По его словам, разработчики Microsoft весьма заинтересованы в создаваемой среде, в которой они могли бы размещать исследовательские задачи, и уже в конце мая в компании на высоком уровне будет обсуждаться возможность интеграции ресурсов в том или ином виде.

За все время существования "Университетский кластер" финансируется исключительно на средства бизнеса — при старте проекта на реализацию его первого этапа HP выделила более 12 млн. руб., а "Синтерра" — порядка 7 млн. Государство же, хотя, по всей видимости, и лояльно относится к данной инициативе, вопрос о своем финансовом участии в проекте пока не рассматривает.

По уверению представителя Минкомсвязи Игоря Химченко, задача государства заключается в том, чтобы создавать условия для успешных проектов, но они не исчерпываются деньгами. Как утверждает чиновник, например, речь может идти о стимулировании частно-государственного партнерства, где крайне важно непредвзятое отношение власти к участникам процесса.

Говоря о результатах программы, которых Минкомсвязи склонно от нее ожидать, г-н Химченко помимо создания новых продуктов и услуг заострил внимание на воспитании профессиональных кадров: специалистов, преподавателей и даже госслужащих, так или иначе вовлеченных в процесс.

Что же касается организаторов, то они в этой связи рассуждали о синергетическом эффекте, об устранении цифрового неравенства между центром и регионами и о важности среды "Университетского кластера" для развития дистанционного образования.

Говоря о будущем, директор ИПС РАН Виктор Иванников отметил, что проект в первую очередь будет развиваться в направлении так называемых облачных вычислений. При этом, по его мнению, нужно двигаться в сторону создания таких сервисов, на базе которых можно было бы предоставлять принципиально новые услуги — тогда сообщество сможет жить интересно и активно и сумеет обеспечить трансферт технологий в индустрию.

В этой связи интересно отметить мнение генерального директора Российской венчурной компании Игоря Агамирзяна, который считает, что в данном случае в нашей стране впервые удалось вовремя присоединиться в рамках столь масштабного проекта к явно определившемуся серьезному технологическому тренду. Он считает, что облачные вычисления будут крайне актуальны как минимум ближайшие 10 лет и уже обладают очевидными бизнес-перспективами.

От адаптивности к конвергенции

ЛЕВ ЛЕВИН

Компания Hewlett-Packard в начале апреля представила своим российским партнерам и заказчикам новую концепцию подхода к применению ИТ в современном бизнесе, который называется "конвергентной инфраструктурой".

СЕРВЕРЫ

Как нам пояснил менеджер по развитию бизнеса европейского отделения компании Джеймс Генри, ключевым элементом конвергентной инфраструктуры является HP BladeSystem Matrix — объявленный примерно год назад на конференции Technology@Work 2009 в Берлине полностью настроенным программно-аппаратным комплексом на базе лезвий для быстрого развертывания различных корпоративных приложений. Единственное технологическое усовершенствование в этой системе, которое HP реализовала за прошедший год, — это новая версия управляющего ПО, которая улучшила масштабируемость матрицы. До сих пор HP BladeSystem Matrix в Россию не поставлялся, но, как обещают представители московского офиса компании, уже в мае матрица будет доставлена первому российскому заказчику. По словам г-на Генри, с этого года продажами и обслуживанием матрицы будет заниматься не только HP Services, но и партнеры компании.

Первая HP BladeSystem Matrix будет поставлена в Россию через год после официального анонса матрицы

Видимо, чтобы ускорить продвижение матрицы, маркетологи HP решили использовать представленную осенью прошлого года концепцию конвергентной архитектуры. У любого, кто последние годы следил за развитием отделения серверов и систем хранения HP, появление этой концепции не может не вызвать вопрос о том, чем она отличается от прежней концепции адаптивной инфраструктуры (адаптивного предприятия), которая зародилась еще в корпорации Compaq, а затем активно продвигалась HP, особенно в те времена, когда компанию возглавляла инициатор покупки Compaq Карли Фиорина.

По словам Джеймса Генри, конвергентная инфраструктура представляет собой воплощение на практике идей адаптивной инфраструктуры (правда, в таком случае неизбежно возникает вопрос о том, какую отдачу получила HP от многолетних усилий по продвижению прежней концепции). Руководитель направления HP BladeSystem московского офиса компании Сергей Члек определяет конвергентную инфраструктуру как адаптивную с новыми возможностями, которые открывает конвергенция современных технологий, прежде всего сетевых (например, применение протоколов iSCSI, FCoE, Converged Enhanced Ethernet). Хотя такое объяснение эволюции генеральной линии HP вполне логично, в него плохо вписывается HP BladeSystem Matrix как необходимый компонент для реализации конвергентной инфраструктуры — если конвергенция реализуется на сетевом уровне, то ее преимущества будут доступны для любого сервера, снабженного сетевым интерфейсом с поддержкой соответствующего протокола, независимо от того, установлен он в матрице или же в стандартной стойке.

ВКРАТЦЕ

БИЗНЕС

Juniper бросает вызов Cisco

Компания Juniper Networks приобретает частную фирму Ankeena Networks, производителя новаторских технологий для мультимедийных инфраструктур. Точная сумма сделки не объявляется, известно лишь, что она не превышает 100 млн. долл. Благодаря этому поглощению Juniper собирается укрепить положение в области передачи мультимедийного интернет-трафика, в которой прочные позиции занимает Cisco.

Фирма Ankeena, основанная в 2008 г., занимается разработкой программных решений для передачи медиаконтента, которые позволяют передавать большие объемы данных с качеством, сравнимым с телевизионным, при этом существенно сокращая расходы на доставку информации.

Juniper собирается интегрировать программный продукт Media Flow Director компании Ankeena со своими решениями, чтобы удовлетворить высокий спрос на передачу видео при существенной оптимизации расходов. В последнее время объем видеоданных в сетях мобильной и фиксированной связи стремительно растет, что увеличивает нагрузку на инфраструктуру провайдеров услуг. Так, по оценке аналитической компании Nielsen, за последний год в США число любителей интернет-видео выросло на 16% и достигло 138 млн. человек. При этом объем видеотрафика повысился на 26%. Особенно быстро растет объем видео в мобильных сетях.

Кроме того, Juniper собирается воспользоваться растущим рыночным спросом на сети доставки контента (Content Delivery Networks, CDN) и на технологию передачи видео на устройства трех типов — ПК, мобильное оборудование и телевизионные приставки (3 Screen). По данным консалтинговой компании CIMI, сейчас 22 из 23 ведущих мировых провайдеров услуг либо строят собственные сети доставки контента, либо интегрируют свою инфраструктуру с имеющимися CDN-сетями других игроков. При этом большинство поставщиков услуг передачи видео (по кабельным, спутниковым сетям и через Интернет) разрабатывают решения для поддержки технологии 3 Screen.

По мнению наблюдателей, эта сделка не только расширит возможности Juniper в области доставки видео, но и позволит более успешно конкурировать с Cisco, которая в последнее время активно наращивает портфель решений для данной области. Достаточно вспомнить недавние сделки с компаниями Starent и Tandberg.

После слияния шестьдесят сотрудников Ankeena войдут в состав подразделения Junos Ready Software. ***Е. Г.***

СОДЕРЖАНИЕ

№ 15-16 (717-718) • 27 АПРЕЛЯ, 2010 • СТРАНИЦА 4

НОВОСТИ

ИТ-БИЗНЕС

ПЕРСОНАЛЬНЫЕ СИСТЕМЫ

ИНФРАСТРУКТУРА

PC WEEK REVIEW: ИТ-БЕЗОПАСНОСТЬ

КОРПОРАТИВНЫЕ СИСТЕМЫ

ЭКСПЕРТИЗА

ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ

УПОМИНАНИЕ ФИРМ В НОМЕРЕ

"1С-Битрикс" предлагает корпоративные видеопереговорные комнаты

ВЛАДИМИР МИТИН

Наикратчайшим образом основные ступени развития информационных технологий можно обозначить так: цифры — тексты — неподвижные картинки — аудио — видео. В этом направлении развиваются не только аппаратные средства, но и программные решения, в том числе корпоративные. Вот лишь один из примеров.

ВКС

В апреле компания "1С-Битрикс" объявила о начале продаж версии 9.0 решения "Корпоративный портал", предназначенного для организации совместной работы сотрудников и автоматизации бизнес-процессов на предприятиях среднего и малого бизнеса. Эта версия пришла на смену предыдущей, 8.5, объявленной прошлой осенью во время выставки SofTool'2009. Новинка, как и её предшественница, выпускается в трех вариантах ("Интранет", "Экстранет", "Бизнес-процессы"), различающихся функциональными возможностями.

Вячеслав Борилин: "У рынка видеоконференцсвязи очень светлое будущее. По некоторым оценкам, уже сейчас в нашей стране на каждые 100 проданных ПК приходится 25 проданных Web-камер"

По словам генерального директора "1С-Битрикс" Сергея Рыжикова, стоимость различных вариантов "Корпоративного портала" не изменилась. Более того, компании, у которых срок технической поддержки этого решения ещё не истек, могут обновить его до новейшей версии бесплатно.

Главная особенность новинки — возможность организации на корпоративном сайте до двух виртуальных "переговорных комнат". Максимальная вместимость каждой — шесть человек. При этом все участники видеоконференции могут видеть друг друга на экране компьютера, разделенном на шесть зон (в два горизонтальных ряда по три "окна").

Данное нововведение стало возможным благодаря сотрудничеству "1С-Битрикса" с компанией "ВидеоПорт", ведущей свою историю с 2004 г. и имеющей большой опыт работы как с корпоративными, так и с частными клиентами. Директор по продажам "ВидеоПорта" Дмитрий Одинцов отметил, что количество зарегистрированных пользователей бесплатного онлайн-сервиса его фирмы (он в чем-то аналогичен онлайн-сервису Skype, но отличается от него рядом интересных возможностей) в настоящее время превышает 1,2 млн. человек. При этом ежедневно им пользуется, по сведениям компании, около 10 тыс. абонентов.

Кроме того, около пяти сотен предприятий и учреждений приобрели корпоративные серверные пакеты VideoPort SBS (решение для малого бизнеса), VideoPort SBS Plus (решение для среднего бизнеса) или VideoPort Enterprise (решение для крупных корпораций). С точки зрения функциональности "шестиместная" переговорная комната, предлагаемая владельцам "Корпоративного портала 9.0", является примерно вдвое урезанным вариантом решения VideoPort SBS. Предполагается, что уже в апреле "ВидеоПорт" начнет продажи универсального продукта VideoPort VCS 3.0, который будет обладать новыми функциональными возможностями и заменит выпускавшиеся прежде корпоративные решения.

Как сообщил Сергей Рыжиков, годовая аренда каждой "шестиместной" переговорной комнаты, использующей технологии "ВидеоПорта", обойдется владельцу версии 9.0 "Корпоративного портала" примерно в 6000 руб. при условии оформления заказа в апреле — мае. В дальнейшем стоимость такой аренды планируется поднять до 8000 руб. Для сравнения: годовая подписка на серверный продукт VideoPort SBS стоит 35 тыс. руб.

Сергей Рыжиков: "Решения для среднего и малого бизнеса должны быть комплексными, быстрыми в развертывании и простыми в использовании"

Ещё одним технологическим партнером "1С-Битрикса" в области организации систем корпоративной видеоконференцсвязи является компания "ВидеоМост", созданная в конце 2009 г. Среди известных проектов "ВидеоМоста" — организация видеоконференций с участием первого вице-премьера РФ Игоря Шувалова, главы ФАС Игоря Артемьева и главы Сбербанка Германа Грефа, а также госпроект по обучению детей с ограниченными возможностями. Кроме того, как утверждает генеральный директор "ВидеоМоста" Вячеслав Борилин, у компании есть и другие клиенты, но они пока не пожелали афишировать свои имена.

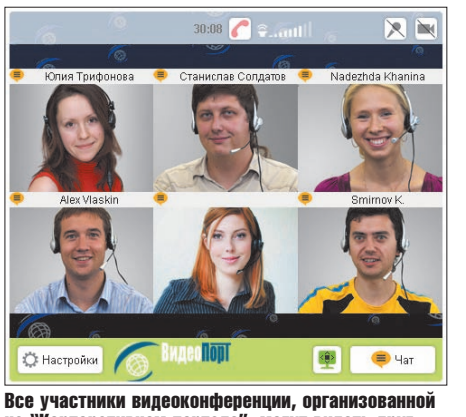
Дмитрий Одинцов: "Мы предлагаем ПО, способное осуществлять видеоконференцсвязь без покупки и использования специального дорогостоящего оборудования"

Предполагается, что виртуальные "переговорные комнаты", использующие технологии "ВидеоМоста", будут доступны владельцам версии 9.0 "Корпоративного портала" уже в мае примерно по той же цене, что и "переговорные комнаты", построенные на технологиях конкурентов.

Представители "ВидеоПорта" и "ВидеоМоста" утверждают, что для организации виртуальных переговоров годятся настольные и блокнотные компьютеры, оснащенные практически любыми Web-камерами. При этом каждый участник видеоконференции создает трафик приблизительной интенсивностью 128 кбит/с. Возможна запись многоточечного сеанса видеоконференцсвязи (с целью его последующего просмотра и более глубокого осмысления). По мнению Дмитрия Одинцова, объем видеозаписи часового виртуального совещания шести человек составит около 300 Мб. Аналогичные цифры называют и специалисты "ВидеоМоста". Однако в настоящее время возможность записи совещаний, круглых столов и прочих мероприятий, проводимых посредством "Корпоративного портала 9.0", не предусмотрена. Прежде всего потому, что разработчики не уверены в востребованности данного сервиса. "Если спрос на эту услугу будет, то будет и соответствующее предложение", — говорит Сергей Рыжиков.

Среди других новшеств версии 9.0 "Корпоративного портала" его разработчики отмечают технологию Send&Save, суть которой состоит в том, что переписка сотрудников по электронной почте дублируется на портале, архивируется по темам и индексируется внутренней системой поиска. "Электронная почта в большинстве компаний традиционно остается единственным инструментом внутреннего общения, а это нередко приводит к тому, что знания сотрудников разбросаны по почтовым ящикам и их невозможно собрать в одном месте, — говорит Сергей Рыжиков. — При таком подходе с уходом того или иного сотрудника многие ценные данные теряются навсегда. Технология Send&Save позволяет не только сохранить важные контакты, данные, обсуждения и защитить компанию от потери информации, но и предоставить доступ к архиву переписки другим сотрудникам в соответствии с их правами доступа".

Кроме того, в версии 9.0 появился визуальный редактор универсальных списков. Теперь в "Корпоративном портале", используя визуальные компоненты с поддержкой drag&drop, можно легко создавать списки частых вопросов, справочники, базы знаний, перечни контрагентов, структурированные архивы, библиотеки, файловые хранилища и прочие объекты.



Все участники видеоконференции, организованной на "Корпоративном портале", могут видеть друг друга на экране компьютера, разделенном на шесть зон

Среди других новшеств "девятки" можно упомянуть возможность подключения к корпоративному порталу обычной папки на сервере в качестве библиотеки документов, расширенные функции фотогалереи, полнотекстовый поиск информации в рамках рабочей группы, упрощение поиска и выбора сотрудника, персонализацию личной страницы пользователя, учет статистики запросов внутренней системы поиска и множество других усовершенствований.

И снова о Сколкове

◀ ПРОДОЛЖЕНИЕ СО С. 1

ния в изрядной степени разделились. Одна часть опрошенных ратует за крупные госзаказы и даже непосредственное участие ВПК, другая настаивает на необходимости свести роль государства (и приближенных к нему олигархов) в Сколкове к минимуму и настаивает на скорейшей коммерциализации проекта — создании спроса на его результаты со стороны крупного бизнеса. Также упоминались: грамотная стратегия привлечения инвестиций и венчурного капитала; наличие готовых переехать в Сколково научных коллективов и профессиональных кадров (с инновационными разработками). Кроме того, высказывались мнения о том, что успех ожидает иноград лишь в случае создания института конфискации имущества (видимо, чиновников) с последующей ссылкой в Китай. А самые пессимистично настроенные предлагали развивать Сколково в рамках другой (свободной) экономики, а еще лучше — на территории другого государства.

Следующий вопрос для редакции был очевиден в контексте старой перманентной дискуссии о жизнеспособности идеи технопарков в России: при каких условиях ИТ-компании захотят стать резидентами нового центра?

Лидером оказался ответ "отсутствие коррупционного давления", обративший на себя внимание 68,31% читателей. Далее следуют налоговые льготы (57,92%), развитая бизнес-инфраструктура (56,28%), арендные льготы (42,62%) и комфортные условия для жизни и отдыха (40,98%).

Собственные варианты стимулирования резидентов предложило 8,74% ответивших. Из них каждый пятый просто акцентировал внимание на том, что необходим полный комплекс вышеупомянутых условий (разве можно что-то исключить?). Остальные считают важным близость крупных городов, доступ к идеям технических вузов, развитость транспорта, обеспечение безопасности (как бизнеса, так и личной), наличие научной и технологической базы для инноваций, а также главного конструктора-идеолога.

На вопрос, какие ИТ-направления имеет смысл развивать в Сколкове, большинство респондентов выбрало ответ "все" (42,62%). Из конкретных точек приложения усилий наиболее популярной стала разработка ПО (31,69%), за ней следуют элементная база (26,78%) и телекоммуникации (19,67%).

В персональных ответах (15,3%) прозвучали идеи развивать робототехнику, сложные информационные системы на базе программно-технических комплексов, био-ИТ, фундаментальные исследования (математику и физику), разработку конечного оборудования, ИТ-обслуживание отраслей, приносящих деньги (нефть, газ и другое сырье, а также, возможно, вооружение).

Среди опрошенных нашлись как сторонники адаптивного развития проекта с учетом постоянных исследований рынка, так и приверженцы стратегии концентрации на приоритетных прорывных направлениях ("распыляться нельзя"). Более того, отдельные респонденты выразили уверенность в том, что развивать можно всё что угодно, лишь бы развивалось хоть что-то, а другие пессимистично заметили, что заданный вопрос не имеет никакого практического смысла, поскольку, где именно в очередной раз будут распилены деньги, не принципиально.

В нашем последнем вопросе мы попытались узнать мнение читателей относительно того, когда проект иннограда сможет начать приносить результаты. Треть (34,97%) предположила, что это произойдет через 5—7 лет; 22,4% назвали срок в 3—5 лет; 18,58% думают, что через 7—10 лет; 13,11% — только через 10—15 лет; 2,73% — еще позже и 6,56% — вообще никогда.

Итак, какие выводы можно сделать из полученных данных? За исключением небольшого количества абсолютных пессимистов, большинство респондентов идею создания мощного научно-исследовательского центра одобряет: у наших читателей есть вполне четкое представление о том, что там нужно развивать и что нужно сделать, чтобы в проекте появились люди и он не превратился в очередную черную дыру госбюджета. Вот только строительство иннограда в чистом поле респонденты явно не приветствуют — конкретное место, выбранное президентом, не нравится практически никому.

Первые вести от исполнителей

Вопрос, почему вся страна сейчас должна возделывать сколковский пустырь, когда уже есть Дубна, Зеленоград, Новосибирск и т. д., горячо обсуждался и за вышеупомянутым круглом столом. Присутствовавший на заседании член правления группы компаний "Ренова" Андрей Шторх в ответ на все выпады высказался в том смысле, что если решение уже принято, то разбираться в его мотивах сейчас нет никакого смысла. В текущей ситуации критиканская дискуссия — просто потеря времени; надо делать дело.

Андрей Шторх признал, что в отношении проекта уже формируется негативное общественное мнение, и ответственность за это возложил, разумеется, на СМИ. По убеждению бизнесмена, критиковать что-либо проще всего, а вот вы пойдите и найдите светлое зерно и вырастите из него нечто доброе. В общем, цель отечественных СМИ, как наставляет их г-н Шторх, должна быть позитивной. (Обязательно при случае передам эти мудрые слова преподавателям журфака.)

Так или иначе, но почему именно Сколково, г-ну Шторху неизвестно (все вопросы к Медведеву). Зато, по его мнению, важно, что группа компаний, которую он представляет, знает, как поднять проект, потому что у нее есть опыт подъема множества других проектов.

По выражению г-на Шторха, главная идея — уйти в Сколкове от "совка". Причем этот проект он со ссылкой на слова Виктора Вексельберга призвал считать своеобразным "пилотом", который в перспективе должен самовоспроизводиться — тиражироваться. (Что характерно, присутствовавший на заседании управляющий партнер Strategy Partners Александр Идрисов, не конкретизируя источник информации, также заверил участников круглого стола, что технологических центров будет несколько и с рядом регионов уже идут некие переговоры на этот счет.)

Из речи г-на Шторха можно было заключить, что он не склонен сравнивать Сколково с американской Кремниевой долиной. В мире проекты так называемых технополисов уже успели пройти три стадии развития. Сначала появились образования вокруг университетов (г-н Шторх считает это не лучшим вариантом для России: наши университеты — центры тусовки; самые способные студенты уехали в Стэнфорд и пр.), затем были бизнес-инкубаторы, потом так называемые сетевые парки. Сейчас мир стоит на пороге четвертой стадии, и именно технополисом нового поколения российский проект и призван стать. Если это удастся, то, как теоретизирует г-н Шторх, последующие энтузиасты-инноваторы в разных странах станут строить у себя "Сколково", а не Кремниевую долину.

Впрочем, по состоянию на конец марта конкретной модели проекта в голове г-на Шторха еще не было. По его словам, г-н Вексельберг оказался в роли руководителя, что называется, наскоком и ему еще только предстояло начать консультации с рабочей группой, занимавшейся проектом уже три месяца.

Отвечая на вопрос, зачем лично г-ну Вексельбергу все это нужно, г-н Шторх высказался в том смысле, что "Ренова" развивает разные направления бизнеса и уже давно взяла курс на диверсификацию. При этом он заверил оппонентов, что возможность отказаться у миллиардера была (вообще его шеф не первым получил предложение на должность), однако он прикинул риски, сопоставил их со своими амбициями и согласился, посчитав поставленную задачу для себя интересной.

Объем бюджетного финансирования Сколкова пока не ясен. Как уверяет г-н Шторх, сначала нужен четко разработанный проект, а уже потом — финансирование под него. В противном случае начнется распил.

Успех участия группы "Ренова" в проекте г-ну Шторху видится в том, что это именно частная компания, заточенная на результат, а не на процесс.

Что же касается ближайших планов, то одним из важнейших первых шагов член правления "Реновы" назвал поиски сопредседателя проекта с иностранной стороны (фигуры, сопоставимой с г-ном Вексельбергом, с другой части планеты), которые должны завершиться до конца мая.

Visual Studio 2010...

◀ ПРОДОЛЖЕНИЕ СО С. 1

ходимостью решения трех основных взаимосвязанных задач: повышение производительности труда разработчиков; управление всем циклом создания приложений; поддержка коллективной работы. Внешне же это проявляется в постоянном расширении состава системы, в том числе за счет средств высокоуровневого программирования с использованием моделей, разнообразных инструментов тестирования, а также такого ключевого компонента, как TFS. Одновременно растет число вариантов продукта, предназначенных для использования разными категориями разработчиков; фактически Visual Studio — это целое семейство инструментальных средств.

Одна из ключевых стратегических линий Microsoft в области разработки ПО — постоянный курс на максимальное сближение методов и технологий создания различных видов приложений (Windows, Web, серверные и клиентские программы, мобильное и встроенное ПО, высокоуровневые бизнес-приложения, приложения на базе Office, игры). В Visual Studio 2010 это направление получило развитие в результате появления средств программирования для облаков.

Разумеется, реализовать все это в рамках одного пакета нельзя, да и не нужно. Именно поэтому подход Microsoft к построению своей платформы разработки подразумевает использование универсального пакета Visiual Studio в качестве базового инструмента создания широкого спектра ПО, а также ключевого компонента, объединяющего весь спектр своих инструментов (в том числе узкоспециализированных) в единую интегрированную систему.

Необходимо добавить также, что составной частью платформы разработки Microsoft можно считать огромное количество различного рода средств и решений независимых поставщиков, которые представляют собой очень важный пласт общей партнерской экосистемы корпорации. В значительной мере данные продукты дополняют и расширяют Visiual Studio. При этом нужно напомнить, что Visual Studio сам по себе является не только собственно средством разработки ПО, но и технологической платформой для создания инструментов третьими фирмами.

Состав семейства Visual Studio 2010

Издания для начинающих и любителей (Express):
- Visual C++
- Visual C#
- Visual Basic .NET
- Visual Web Developer

Для профессиональных разработчиков:

основные издания
- Professional
- Premium (плюс тестирование, анализ кода, управление изменениями)
- Ultimate (плюс расширенное тестирование, моделирование, развертывание)

дополнительные продукты
- Team Foundation Server
- Team Foundation Server Basic
- Team Lab Management
- Test Elements
- Team Egents
- Team Explorer
- Remote Debugger
- Продукты Teamprise (на базе Eclipse)

Средства для разработчиков инструментов на базе IDE Visual Studio:
- Visual Studio 2010 Shell
- Visual Studio 2010 SDK
- Microsoft Visual Studio 2010 DSL SDK

Источник: *Microsoft*.

Новая версия Visual Studio 2010 содержит немало новшеств, среди которых сейчас отметим только некоторые наиболее интересные.

• Visual Studio 2010 стал первым инструментом, интегрированная среда которого реализована на базе технологии Windows Presentation Foundation, что заметно повысило гибкость работы в ней. Интерфейсная оболочка всех предыдущих выпусков инструмента имела своей архитектурной основой продукт версии 6.0.

• Изменилась компоновка продуктов для профессиональных разработчиков (см. рисунок). Основным, базовым изданием по-прежнему остается Professional Edition, а наращивание возможностей возможно как за счет перехода к более полным изданиям, так и применением отдельных специализированных компонентов. Появился "облегченный" вариант TFS.

• В продукте впервые реализована поддержка многоплатформенной разработки. Это достигается на уровне обеспечения коллективной работы через TFS, а также с помощью технологий Teamprise Client Suite, приобретенных в ноябре 2009 г. у компании SourceGear.

• Реализованы новые возможности параллельных вычислений на уровне языков программирования и .NET Framework.

• В составе пакета появился новый язык F# (вариант языка OCaml, реализованный поверх .NET Framework).

• Имеется возможность использовать Windows Azure Tools — набор средств для создания приложений для облачной ОС Microsoft Windows Azure.

Хотя в целом Visual Studio позиционируется как инструмент для профессиональных разработчиков, Microsoft не забывает и многочисленную категорию программистов, которую принято называть начинающими и любителями. Именно для них предназначены бесплатные выпуски продукта серии Express.

Полтора года назад произошло очень важное для российского программистского сообщества событие: в нашей стране появился первый полностью локализованный инструмент разработки зарубежного поставщика; им стал Visual Studio 2008, русский вариант которого вышел спустя год с лишним после выпуска английской версии. На этот раз всё должно произойти намного быстрее: представители Microsoft обещают, что русская версия Visual Studio 2010 появится уже в текущем квартале.

СК ПРЕСС PCWEEK RUSSIAN EDITION

Учредитель и издатель
ЗАО «СК ПРЕСС»

Издательский директор
Е. АДЛЕРОВ
Издатель группы ИТ
Н. ФЕДУЛОВ
Издатель
С. ДОЛЬНИКОВ
Директор по продажам
М. СИНИЛЬЩИКОВА
Генеральный директор
Л. ТЕПЛИЦКИЙ
Редакционный директор группы ИТ
Э. ПРОЙДАКОВ
Шеф-редактор группы ИТ
Р. ГЕРР

Редакция

Главный редактор
А. МАКСИМОВ
Заместители главного редактора:
И. ЛАПИНСКИЙ — 1-й заместитель главного редактора,
И. КОНДРАТЬЕВ — шеф-редактор
Научные редакторы:
М. БУКИН, В. ВАСИЛЬЕВ, Е. ГОРЕТКИНА, Л. ЛЕВИН, О. ПАВЛОВА, С. СВИНАРЕВ, П. ЧАЧИН
Обозреватели:
О. БЛИНКОВА, Д. ВОЕЙКОВ, С. ГОЛУБЕВ, С. БОБРОВСКИЙ, А. КОЛЕСОВ, М. ФУЗЕЕВА
Специальный корреспондент:
В. МИТИН
Корреспондент:
М. ФАТЕЕВА
PC Week Online:
А. ЛИВЕРОВСКИЙ
Тестовая лаборатория: А. БАТЫРЬ
Ответственный секретарь:
Е. КАЧАЛОВА
Литературные редакторы:
Н. БОГОЯВЛЕНСКАЯ, Т. НИКИТИНА, Т. ТОДЕР
Фотограф:
О. ЛЫСЕНКО
Художественный редактор:
Л. НИКОЛАЕВА
Компьютерная графика:
Н. ГУЩИНА
Группа компьютерной верстки:
С. АМОСОВ, А. МАНУЙЛОВ
Техническая поддержка:
К. ГУЩИН, С. РОГОНОВ
Корректор: Л. МОРГУНОВСКАЯ
Оператор: Н. КОРНЕЙЧУК
Тел./факс: (495) 974-2260
E-mail: editorial@pcweek.ru

Отдел рекламы

Руководитель отдела рекламы
С. ВАЙСЕРМАН
Тел./факс:
(495) 974-2260, 974-2263
E-mail: adv@pcweek.ru

Распространение

ЗАО "СК Пресс"
Отдел распространения, подписка
Тел.: +7(495) 974-2260
Факс: +7(495) 974-2263
E-mail: distribution@skpress.ru
Адрес: 109147, Москва, ул. Марксистская, д. 34, к. 10, 3-й этаж, оф. 328

Газета зарегистрирована Комитетом РФ по печати 29 марта 1995 г.
Свидетельство о регистрации № 013458.
Отпечатано в ОАО "АСТ-Московский полиграфический дом", тел.: 748-6720.
Тираж 35 000.
Цена свободная.

Использованы гарнитуры шрифтов "Темза", "Гелиос" фирмы TypeMarket.

"Аскон" в ожидании роста

ЕЛЕНА ГОРЕТКИНА

В прошлом году валовая выручка "Аскона" сократилась на 30% — до 544,2 млн. руб. Компания объясняет это спадом российской промышленности, который привел к сокращению спроса на САПР. Как подчеркнул генеральный директор "Аскона" Максим Богданов, такое падение произошло впервые за десятилетие с лишним (см. диаграмму). Однако благодаря ряду мер фирме удалось сохранить рентабельность. Глядя в будущее, "Аскон" не теряет оптимизма и надеется в этом году возобновить рост и заработать 548 млн. руб.

БИЗНЕС

Максим Богданов: "Всё зависит от состояния промышленности: если она будет расти, то же самое будет происходить и с рынком САПР"

Такие надежды построены не на пустом месте, а основаны на анализе тенденций развития российской экономики. Как считают в "Асконе", у нас рынок САПР будет развиваться в строгом соответствии с трансформацией существующей структуры промышленности. По словам директора по стратегическому развитию Евгения Бахина, если раньше в нашей стране был сильный перекос в сторону оборонки, то теперь наблюдается постепенный рост гражданской промышленности, направленной на разработку и выпуск массовой продукции потребительского и производственного назначения. В связи с этим расширяется основа для массовых САПР, которые быстро внедряются и позволяют решать текущие задачи предприятий.

Однако из-за сложной экономической ситуации требования заказчиков меняются. Так, на первый план выходит экономическое обоснование инвестиций в ИТ, рост производительности труда как обязательный результат ИТ-проектов, а также переход отношений от системы "покупатель — поставщик" к кооперационному партнерству. "Клиенты больше не смотрят на инвестиции в САПР как на престижное капиталовложение. Главную роль теперь играет окупаемость, — объяснил Евгений Бахин. — К тому же покупка САПР зачастую рассматривается не как одноразовая сделка, а является основой долговременных отношений с поставщиком, поскольку крупные проекты быстро не делаются".

Судя по опыту "Аскона", таких проектов становится все больше. Ведь прошлогодний спад коснулся главным образом коробочных продуктов, не требующих внедрения, а доля комплексных решений вместе с услугами выросла. "Все запущенные в прошлом году проекты были реализованы. И хотя сейчас новых проектов стало меньше, они тем не менее запускаются", — сказал Максим Богданов.

Рассматривая перспективы рынка САПР в России, "Аскон" отмечает, что все зависит от состояния промышленности. Если она будет расти, то же самое будет происходить и на рынке САПР, причем его рост составит примерно 3—4% на каждый процент роста промышленности.

Что касается объема продаж САПР в 2009-м, то исходя из опыта "Аскона" г-н Бахин предположил, что падение составило 30—40%. Если взять за основу данные IDC, которая оценила российский рынок САПР (CAD/CAE/CAM/PDM) в 2008 г. в 116,64 млн. долл., то получится, что в 2009-м его объем сократился до 70—80 млн. долл. Правда, по прогнозу IDC, в 2009-м рынок САПР должен был уменьшиться втрое, но в "Асконе" придерживаются другого мнения. "Судя по нашим результатам, столь резкого провала не случилось, — сказал Евгений Бахин. — Кроме того, мы считаем, что в 2009 г. рыночные доли ведущей пятерки поставщиков остались на уровне предыдущих лет".

С точки зрения технологий доминировать будет 3D, хотя 2D-функционал тоже будет востребован, возрастет роль "бесшовной" интеграции средств проектирования и инженерного анализа, а также распределенной коллективной работы над проектом. "Заказчики требуют ускорить проектирование и сократить затраты. Если, не выходя из САПР, конструктор сможет выполнить хотя бы проверочный расчет, что-

ПРОДОЛЖЕНИЕ НА С. 18 ▶

Oracle Primavera — знакомый новый бренд

СЕРГЕЙ СВИНАРЕВ

Впервые после покупки корпорацией Oracle компании Primavera российская конференция пользователей одноименного средства управления проектами прошла под флагом нового хозяина. Что же изменилось? Прежде всего название. Теперь клиентам предлагается пакет Oracle Primavera, на основе которого, как утверждают представители Oracle, ей первой в отрасли удалось реализовать концепцию управления портфелями проектов Enterprise Project Portfolio Management (EPPM), объединив средства проектного управления со своими системами ERP и EPM (Enterprise Performance Management).

КОНФЕРЕНЦИИ

В пакет Oracle Primavera, нашедший широкое применение в нефтегазовой отрасли, энергетике, ЖКХ и строительстве, сегодня входят четыре основных функциональных блока: P6 Enterprise Project Portfolio Management — базовый модуль для планирования, определения приоритетов и управления проектами, Portfolio Management — средство для оптимального управления портфелями проектов, Contract Management — решение для управления работами, выполняемыми подрядчиками и контрагентами, Risk Analysis — инструмент, применяемый для анализа и оценки вероятностей рисков, а также выработки резервных планов на случай реализации тех или иных неблагоприятных сценариев.

Джефф Робертс: "Oracle Primavera и ERP-системы не конкурируют, а взаимно дополняют друг друга"

Одной из центральных тем конференции стало обсуждение вопросов взаимодействия системы проектного управления с контуром ERP. Ведущий консультант департамента Oracle Primavera по региону EMEA Джефф Робертс даже дал своему докладу подчеркнуто полемическое название "Oracle Primavera и ERP-системы — конкуренция или синергия?". И хотя выбор, как и ожидалось, был сделан в пользу синергии, определенные вопросы к позиционированию нового продукта в линейке бизнес-приложений Oracle остались. Трудно не согласиться с тем, что наряду с управлением проектом (и особенно их портфелем) целый ряд процессов компании, связанных с финансовым учетом, закупками, цепочками поставок, бизнес-аналитикой, стратегическим управлением и работой персонала, должен осуществляться вне рамок конкретного проекта, имея целью повышение эффективности организации в целом. Джефф Робертс привел детальную диаграмму процесса управления типичным проектом, практически каждый этап которого требовал взаимодействия с тем или иным контуром ERP.

За время, прошедшее с момента покупки Primavera, корпорация Oracle выпустила специальные интеграционные пакеты Process Integration Pack (PIP) для двух своих ERP-систем — Oracle E-Business Suite и Oracle JD Edwards EnterpriseOne. И хотя подобные интеграционные решения есть и для других ERP-систем, в частности для SAP ERP (Primavera Inspire for SAP) и "1С" (создано российской компанией PMSoft), утверждается, что пакеты PIP от Oracle обеспечивают более тесную связку с ее собственными бизнес-приложениями и позволяют ускорить окупаемость инвестиций и снизить совокупную стоимость владения (TCO). Совершенно очевидно, что подобные заявления плохо согласуются с позиционированием продуктов Primavera как универсальных, лучших в своем классе решений, равноудаленных от систем корпоративного управления отдельных вендоров. О такой равноудаленности недвусмысленно говорил и сам Джефф Робертс. О ней же лишний раз напомнил доклад бизнес-аналитика службы информации южноафриканской нефтяной компании Petro SA Рубина Бера: в Petro SA эксплуатируются как SAP ERP, так и Primavera. Более того, в управлении проектами здесь задействован еще и специализированный модуль Project System, входящий в состав SAP ERP. Аналогичный модуль Oracle Projects, выпущенный задолго до слияния с Primavera, имеется и в линейке Oracle. Но о том, будут ли оба решения Oracle для управления проектами развиваться параллельно или со временем объединятся, на данном форуме ничего сказано не было.

С переходом компании Primavera под крыло Oracle партнерская сеть по продуктам Primavera в нашей стране заметно расширилась: наряду с PMSoft и "Системами управления", продвигавшими указанные решения еще тогда, когда Primavera была самостоятельной компанией, в эту сеть вошли такие известные системные интеграторы и партнеры Oracle, как IBS Borlas, КРОК, ЛАНИТ и "Форс". Как известно, некоторые из них являются также и партнерами SAP.

Dassault ищет направления роста

ЕЛЕНА ГОРЕТКИНА

Кризис негативно отразился на рынке САПР/PLM из-за спада в производственном секторе. Но поставщики ПО продолжают инвестировать в разработку и запускать новые бизнес-инициативы, чтобы переломить ситуацию и возродить былой подъем. Так, Dassault Systemes (DS) завершила сделку по покупке PLM-подразделения IBM, объявленную в прошлом году, и надеется, что этот шаг подстегнет рост продаж. Компания также возлагает надежды на свою новую платформу PLM V6, которая уже внедряется в автомобильной и других отраслях.

САПР

Лоран Вальрофф: "Сейчас предприятия гораздо больше готовы к новым проектам, чем год назад"

В результате приобретения PLM-бизнеса IBM все контракты Голубого гиганта достаются DS. А ведь речь идет о крупных проектах, поскольку клиентами IBM являются ведущие международные корпорации, такие как Airbus, Daimler и др. Дело в том, что с момента создания компании DS в 1981 г. продажами ее САПР CATIA эксклюзивно занималась IBM. Это было выгодно обеим сторонам. Правда, IBM передала DS свой партнерский PLM-бизнес еще три-четыре года назад, но продолжала работать с прямыми клиентами.

Теперь более 700 специалистов IBM, занимавшихся продажами, внедрением и маркетингом в области PLM, перешли в DS, в основном в подразделение по работе с ключевыми заказчиками, что также планируется и в России.

По словам главы российского офиса DS Лорана Вальроффа, главная деятельность DS — не внедрение, а разработка ПО. Ведь более 80% дохода компания получает от продажи лицензий. Но в 2009-м оборот сократился на 6%, до 1,25 млрд. евро, а прибыль упала на 15%, до 150 млн. евро. Руководство DS надеется, что сделка с IBM позволит вернуть рост. Как рассказал Лоран Вальрофф, в последнее время продажи продуктов DS приносили порядка 1 млрд. долл. в год, которые примерно поровну делились между DS и IBM. Теперь все достанется DS. Но IBM тоже не останется внакладе. Корпорация не только получила 600 млн. долл. от этой сделки, но и сохранила сервисные PLM-контракты, так как продолжает оставаться партнером DS.

Более того, DS и IBM анонсировали некоторые шаги в своих партнерских отношениях, в частности, DS становится IBM Global Alliance Partner. Это существенно расширяет партнерские отношения между DS и IBM по сравнению с уже имеющимися договоренностями. Обе компании намерены укреплять и расширять свое сотрудничество в шести ключевых областях: бизнес-услуги, облачные вычисления, промежуточное программное обеспечение, гибкие системы финансирования, аппаратные средства, продажи и дистрибуция. Продажей и поддержкой решений будет заниматься DS.

В России, как и во всем мире, финансовые результаты DS в 2009-м оказались хуже, чем годом ранее. "Спад был связан с тем, что лишь немногие организации смогли утвердить запланированный бюджет на проекты", — сказал Лоран Вальрофф и добавил, что в этом году планируется вернуться примерно на уровень 2008-го (самого успешного года для российского подразделения DS). По его словам, сейчас появились реальные перспективы, так как предприятия проявляют больше готовности к новым проектам, чем год назад. Одной из таких перспективных отраслей является отечественное автомобилестроение.

Так, "АвтоВАЗ" разрабатывает план модернизации ПО для повышения конкурентоспособности, рассказал Лоран Вальрофф. Предприятие — давний клиент DS. Конструкторский отдел использует САПР CATIA с начала 1990-х, а несколько лет назад перешел на версию V5, увеличив число лицензий более чем на 50%. Сегодня CATIA применяется для дизайна новых моделей и разработки цифрового макета автомобиля, включая кузов, силовой агрегат, интерьер, электрооборудование и другие системы.

Нынешняя задача состоит в создании унифицированной PLM-системы, которой смогут пользоваться конструкторский, производственный, маркетинговый и другие отделы. "Мы предлагаем единую платформу нашим автомобильным заказчикам для создания общей среды, в которой можно будет проектировать модели и производственные процессы, передавать их технологам, осуществлять взаимодействие между разными отделами", — рассказал г-н Вальрофф.

Возможно, для "АвтоВАЗа" катализатором к такой масштабной модернизации станет сотрудничество с французской компанией Renault, которой принадлежит 25% российского автомобильного гиганта. Предполагается, что "АвтоВАЗ" будет производить автомобили по моделям Renault, доработанным в соответствии с отечественными техническими параметрами. Для такого обмена данными потребуется единая информационная среда. Но сейчас Renault активно внедряет новую PLM-платформу V6. "Это — первый клиент DS, который переходит на V6. Проект начался в прошлом году, а в этом июне уже начнется эксплуатация системы и появится первая модель автомобиля, полностью разработанная в V6", — сказал Лоран Вальрофф. Так что не исключено, что задача взаимодействия с Renault подстегнет "АвтоВАЗ" к переходу на V6.

Но продукты DS используют не только гиганты автопрома. Например, системы CATIA и SolidWorks применяет российская компания Marussia Motors, которая разрабатывает первый отечественный спортивный автомобиль и первый внедорожник. По словам представителя компании, благодаря проектированию с помощью 3D-технологии удалось ускорить создание автомобиля и удешевить процесс производства за счет почти полного отказа от бумажных технологий. Так, проект автомобиля был представлен в конце 2008-го, а скоро на выставке в Монако будут показаны две модели Marussia с новыми моторами, пройдет их тест-драйв для первых клиентов, а в мае начнется прием заказов.

Правда, у автопроизводителей случаются и проблемы. Достаточно вспомнить, какой широкий резонанс недавно вызвали неполадки с педалью газа в некоторых автомобилях компании Toyota. Но Лоран Вальрофф считает, что сбой вызван организационными проблемами: "Toyota сейчас разбирается со своими процессами производства и проектирования. Компания использует много разных программных продуктов, но не обвиняет в неполадках ни нас, ни других поставщиков ПО".

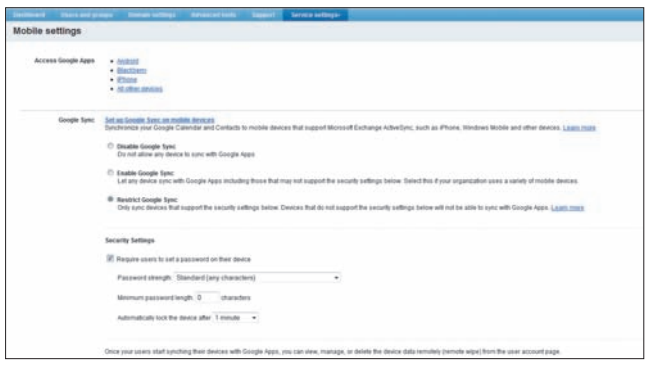
Несмотря на кризис, автомобильная отрасль продолжает инвестировать в проектирование. Это — важно для DS, так как 30% дохода компания получает от этой отрасли. И хотя в прошлом году убытки Renault достигли 3 млрд. евро, компания все равно переходит на V6. "Это характерно для западных компаний — несмотря на спад, они продолжают инвестировать в будущее, — сказал г-н Вальрофф. — Такой подход сильно отличает Запад от России. Здесь заказчики считают, что раз прибыли нет, то нельзя и инвестировать".

Google Apps Premier обеспечивает базовое администрирование мобильных устройств

ЭНДРЮ ГАРСИА

Пакеты онлайн-приложений Google Apps Premier и Education содержат теперь ограниченные средства управления безопасностью и политиками для некоторых мобильных устройств, позволяя компаниям, использующим почтовые услуги Google, контролировать

СЕРВИСЫ



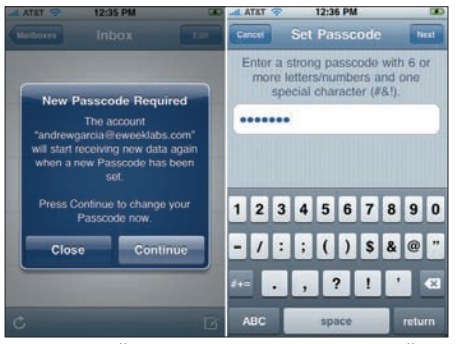
Администраторы могут ограничить доступ лишь устройствам, которые поддерживают политики ActiveSync, и тем самым обеспечить использование паролей

устройства за пределами корпоративной сети. Объем такого контроля чрезвычайно ограничен и, конечно, не сравним с полнофункциональными решениями, но то, что есть, работает нормально и цена адекватна.

В 2009 г. появился инструмент Google Apps Connector для BlackBerry Enterprise Server (BES), что позволило смартфонам BlackBerry синхронизировать контент между приложениями Google Apps и реализацией BES, но фактически администрирование мобильных устройств все равно осуществлялось через BES. И теперь Google поставил протокол Exchange ActiveSync с ног на голову, используя технологию Microsoft не только для синхронизации Android-устройства с сервером Exchange, но также для того, чтобы другие модели, использующие ActiveSync, синхронизировались с Gmail для доставки почты, содержимого ежедневника и контактов и выполняли ограниченные функции администрирования устройств.

Эти функции доступны бесплатно в составе доменов Google Apps Premier и Education. Для тестирования я сделал апгрейд с домена Google Apps Standard на Premier, который стоит 50 долл. за каждый аккаунт (правда, я воспользовался бесплатной 30-дневной пробной версией) и включает другие функции, в частности увеличенный размер почтового ящика и гарантию доступности.

При апгрейде домена разблокировались новые опции конфигурации для сервисов GoogleSync. В домене Standard я мог только разрешить либо запретить GoogleSync для мобильных устройств, но в Premier я смог ограничить доступ к GoogleSync, разрешив этот сервис только для устройств, поддерживающих настройки политики Exchange



При введенной политике использования паролей пользователи обязаны создать пароль на своем устройстве, прежде чем им будет разрешено синхронизировать данные

ActiveSync в дополнение к стандартной доставке почты, контактов и содержимого ежедневника.

Администратор домена может видеть синхронизированные устройства на странице администрирования каждого пользователя. Система Google неважно идентифицирует устройства

Я тестировал функции администрирования Google с разными устройствами, использующими ActiveSync, включая iPhone 3GS и оригинальный iPod Touch, HTC Fuze с Windows Mobile 6.1 и HTC Pure с Mobile 6.5, а также Nokia N97 с установленным модулем Mail for Exchange.

Функции администрирования Google довольно ограниченны. Я обнаружил, что могу (как администратор Google Apps) задать несколько параметров безопасности и они будут одинаково применяться к каждому мобильному устройству, которое синхронизируется с доменом (при условии, что я ограничил услуги синхронизации лишь моделями, поддерживающими политики ActiveSync). В частности, я мог задать политику, которая требует, чтобы пользователи создали пароль блокировки своего устройства, и устанавливает также минимальную длину пароля и время бездействия, прежде чем экран автоматически заблокируется. Другое требование, какое я мог задать, это надежность пароля, выбор состоял лишь из двух опций: стандартная (любые символы) или высокая (как минимум одна буква, одна цифра и один знак препинания).

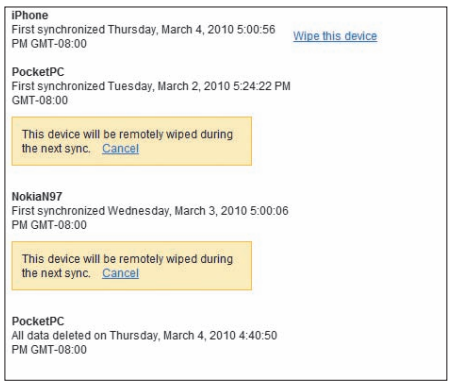
Эти настройки будут одинаковы для всех пользователей, так что я не мог задать разные политики, установив более строгие требования для определенных групп пользователей.

С таким набором параметров при каждой попытке синхронизировать устройство с учетной записью пользователя я видел диалоговое окно на экране устройства, предлагающее создать пароль. Устройство не смогло синхронизироваться с первого раза, пока на нем не был создан пароль, отвечающий заданному уровню сложности.

Устройства, зарегистрированные на домене Google до апгрейда на Premier, при следующей попытке синхронизации также предлагали пользователю создать пароль.

Чего не хватает в администрировании Google

Я обнаружил, что администратор не может диктовать через политику максимальное число неверных логинов до того, как устройство будет отключено, так что в зависимости от конкретной платформы потенциальный взломщик мог продолжать свою атаку прямым подбором без всяких последствий. К примеру, оба устройства с Windows Mobile по умолчанию допускали миллионы попыток перебора паролей, а N97 заблокировал пароль на 5 мин после пяти неудачных попыток.



Консоль Google часто не сообщает об успешном уничтожении данных на устройстве. Если после очистки от данных устройство вновь подключается к домену, то процедура очистки будет повторена вновь, пока администратор не отменит это действие

После того как устройство успешно синхронизировалось с Google Apps Premier, оно появляется на странице настроек соответствующего пользователя в консоли администрирования домена Google. Здесь нет видов и отчетов для всех устройств, подключенных к домену, так что администратор не может получить общее представление об устройствах или их использовании по всему домену в целом. Чтобы найти устройство, администратору нужно сначала знать, какой пользовательский аккаунт с ним синхронизирован.

ПРОДОЛЖЕНИЕ НА С. 23 ▶

Смартфоны Microsoft

МАКСИМ БУКИН

Судя по всему, компания Microsoft берет пример... с Google, которая с помощью сторонних вендоров, но под своим творческим руководством разрабатывает смартфоны, "заточенные" под веб-сервисы собственного производства. В качестве поставщика вместо HTC, как у Google, в Microsoft выбрали Sharp, которая и реализовала творческие задумки специалистов из Редмонда. Без сомнения, самое деятельное участие в разработке новых устройств принимали бывшие сотрудники компании Danger, поглощенной Microsoft еще в 2008 г. Ведь именно они выпускали на рынок вполне интересную серию мобильных устройств Sidekick.

СОТОВАЯ СВЯЗЬ

Kin One — устройство начального уровня с 4 Гб встроенной памяти

Чтобы не перебивать рынок вендорам, которые предлагают свои смартфоны под управлением Windows Mobile для корпоративных пользователей, в Microsoft решили сосредоточиться на потребителях, дотоле предпочитавших модели под управлением Symbian или Android. Таким образом, основная целевая аудитория новых устройств Kin — частные пользователи, которым интересны различные социальные сервисы. В настоящий момент на рынке представлено всего два устройства под незатейливыми названиями Kin One и Kin Two (ранее — Pink Turtle и Pure соответственно), в которых изначально функция голосового общения между пользователями — далеко не самая важная. В принципе, имя устройства в данном случае не так уж и важно — все равно они будут продаваться по операторской модели через Verizon и Vodafone и на их лицевой стороне будет логотип оператора.

Устройства Microsoft — это именно смартфоны, не телефоны. Они нацелены на масштабное потребление интернет-трафика, поэтому для них, как и для устройств Apple и Google, операторы будут предлагать ТП, построенные либо по принципу тарифного калькулятора (когда за определенную абонентскую плату пользователь выбирает любой тип услуг), либо по сборному принципу (голосовые минуты, пакет SMS и интернет-трафика и т. д.).

Следуя новомодной традиции сочетания различных сервисов на одном рабочем экране, в моделях Kin реализовано несколько вполне функциональных настроек поверх Windows Phone 7. К примеру, Kin Loop позволяет агрегировать информацию из социальных сетей Facebook, MySpace, Twitter и, кто бы сомневался, различных сервисов Microsoft Live. A Kin Spot, чем-то серьезно смахивающая на HTC Sense (но о копировании речи не идет — это просто различные реализации одной идеи), реализована как центр управления всеми типами контактов: сюда собраны все записи: от телефонов и IM-идентификаторов до SIP-номеров и адресов электронной почты. Достаточно только указать, с кем вы хотите связаться и по какому идентификатору его искать, и система сама запустит необходимое приложение. Kin Studio отвечает за синхронизацию пользовательских данных, куда разработчики относят контакты, сообщения, списки звонков и все мультимедийные файлы. В данном случае все подобные данные копируются через беспроводную сеть в удаленное веб-хранилище, где их можно администрировать и загружать на устройство в случае их потери. Разумеется, браузером для устройств Kin является Internet Explorer, поисковым сервисом — Bing, а для просмотра мультимедиа используется Windows Media Player. А вот стороннее ПО, пусть даже приобретенное в Windows Marketplace, устанавливать в эти устройства нельзя — во всяком случае пока у Microsoft именно такая позиция. Как долго она продержится — вопрос открытый.

Смартфон Kin Two с QWERTY-клавиатурой и сенсорным дисплеем

Для упрощения ввода информации обе модели оснащены QWERTY-клавиатурами, причем и One, и Two по форм-фактору — слайдеры, позволяющие прятать клавиатуру в корпус, когда она не нужна. Кроме того, дисплеи терминалов — сенсорные с возможность управления пальцем. Объем встроенной памяти невелик, но вполне достаточен для среднего абонента — 4 и 8 Гб соответственно, камеры — разрешением 5 и 8 мегапикселов. Дисплеи — с диагональю 2,6 дюйма (QVGA, 320×240 точек) для One и 3,4 дюйма (HVGA, 480×320 точек) для Two. Оба устройства имеют встроенный модуль A-GPS и FM-радио.

Для США выпущены версии с поддержкой CDMA2000, правда, в диапазоне 800 МГц, для Европы — устройства, работающие в UMTS-сетях на частоте 2,1 ГГц. Bluetooth и Wi-Fi есть в обеих моделях — это коммуникационные сервисы по умолчанию для любой портативной техники.

Три новинки OKI

ВЛАДИМИР МИТИН

ПЕРИФЕРИЯ

Начало нового финансового года — 1 апреля — компания OKI Printing Solutions ознаменовала выпуском трех новых устройств формата A4 для нужд малого и среднего бизнеса: высокоскоростного принтера C610, монохромного МФУ MB400 и цветного МФУ MC160. Все новинки имеют трехлетнюю гарантию, а входящие в их состав светодиодные головки (для принтеров формата A4 они насчитывают свыше 14 тыс. отдельных светодиодов) — пожизненную гарантию.

Семейство C610 появилось как замена выпускавшемуся ранее высокоскоростному принтеру C5950. В настоящее время в это семейство входят три модели: C610n (традиционное "одностороннее" сетевое печатающее устройство с двумя лотками — основным и многофункциональным), C610dn (сетевое печатающее устройство, допускающее работу в автодуплексном режиме для бумаги плотностью от 64 до 120 г/м²) и C610dtn (устройство с двумя дополнительными входными лотками емкостью 530 листов каждый). Быстродействие данных устройств — до 34 стр./мин при цветной печати и до 36 стр./мин при монохромной. Разрешение — 1200×600 точек на дюйм. При наличии дополнительных входных лотков в устройство можно загрузить 1460 листов бумаги плотностью 80 г/м².

Принтер OKI C610

По словам директора по маркетингу и работе с партнерами московского офиса OKI Олега Бондарева, в принтерах семейства C610 используется принципиально новый печатающий механизм, отличающийся весьма низким потреблением электроэнергии: 1,2 Вт в режиме сна и 600 Вт в режиме типовой печати. Отличительная особенность принтеров данного семейства — возможность работы с бумагой плотностью до 250 г/м². То есть данные устройства могут печатать документы практически на картоне. Что иногда бывает немаловажно.

В принтеры семейства C610 можно установить четыре картриджа: один (с черным тонером) для монохромной печати и три — Cyan/Magenta/Yellow (голубой/малиновый/ желтый) — для цветной. По информации производителя, монохромные картриджи обеспечивают распечатку 8000 стр., а цветные рассчитаны на печать 6000 стр. Декларируемый срок службы фотобарабана составляет 20 тыс. стр., а транспортной ленты и блока термического закрепления — 60 тыс. стр.

В комплект поставки этих принтеров входят три программных продукта: Print Control, Colour Access Policy Manager и PrintSuperVision. С их помощью можно контролировать расходы на печать.

Монохромное МФУ MB400 разработано на основе популярной серии монохромных принтеров B400, позволившей OKI, согласно данным IDC, по итогам минувшего года втрое (в штучном выражении) увеличить свою долю на российском рынке монохромных печатающих устройств. "Монохромные МФУ представляют собой самый быстрорастущий сегмент рынка печатающих устройств, — утверждает Олег Бондарев. — Монохромная продукция по-прежнему доминирует в сегменте офисной печати, охватывая порядка 80% от общего объема выпускаемых печатающих устройств".

МФУ OKI семейства MB400

Серия MB400 включает три модели: MB460 выполняет функции печати, сканирования, копирования, MB470 предоставляет также возможности факса, а MB480 снабжена дополнительным лотком подачи бумаги для более крупных рабочих групп.

Все три модели обеспечивают печать и копирование со скоростью до 28 стр./мин (при этом время выхода первой страницы составляет всего 5 с, что, по мнению представителей OKI, является абсолютным рекордом для устройств данного класса) и имеют повышенный ресурс тонера (12 тыс. стр. для модели MB480). При этом предназначенные для них расходные материалы совместимы с серией принтеров B400, что позволяет свести к минимуму соответствующие затраты. Декларируемый срок службы фотобарабана для данных принтеров составляет 25 тыс. стр.

Полноцветное МФУ OKI MC160

Разрешение этих устройств — 600×600 точек на дюйм. Во входные лотки МФУ MB460, MB470 и MB480 можно загрузить до 780, 830 и 1110 листов соответственно. Допустимый диапазон плотности используемой бумаги лежит в пределах 60—120 г/м². В режиме сна данные устройства потребляют 10 Вт, а в режиме типовой печати 500 Вт.

Полноцветное МФУ MC160n адресовано небольшим рабочим группам (для использования в качестве сетевого устройства) и предназначено для сканирования, копирования и печати документов (в том числе в двустороннем режиме), а также отправки и приёма факсимильных сообщений. Оно разработано на базе принтеров серии C110/C130 и совместимо с ними по расходным материалам.

Новинка обеспечивает печать с разрешением 1200×600 точек на дюйм. При этом скорость монохромной печати составляет 20 стр./мин, а цветной — до 5 стр./мин. Отсканированные документы можно отправить на электронную почту, FTP-сервер, общую папку на компьютере или записать на USB-носитель. Емкость входных лотков можно довести до 700 листов бумаги.

В МФУ MC160n используются тонер-картриджи четырех видов: черный, голубой, пурпурный и желтый. В режиме монохромной печати цветные картриджи "отдыхают". Каждый из картриджей имеет два варианта исполнения: на 1500 и на 2500 стр. Декларируемый срок службы фотобарабана МФУ MC160n зависит от режима использования устройства и составляет 45 тыс. стр при монохромной печати и 11 250 стр. — при цветной. В режиме сна данное устройство потребляет 14 Вт электроэнергии, а в режиме типовой печати 560 Вт.

Почему стоит применять "зеленые" технологии в вашем ЦОДе

МЭТЬЮ САРРЕЛ

Сейчас уделяется большое внимание использованию экологически чистых технологий. Нас призывают спасти планету, применять композитные материалы, перерабатывать отходы, уходя гасить свет, не расходовать зря бумагу и т. д. Всё это поможет уберечь окружающую среду, но давайте скажем прямо: для бизнеса "зеленые" технологии имеют смысл только тогда, когда позволяют сберечь капитал и ресурсы. Обеспечить тепло и комфорт в вашей квартире — недостаточно веская для компании причина, чтобы переходить на "зеленые" технологии, а вот сэкономить миллионы долларов на электроэнергии, отоплении, вентиляции и кондиционировании воздуха — это уже совсем другое дело.

ЭНЕРГОСБЕРЕЖЕНИЕ

Действительно, многие предприятия добились значительной экономии благодаря использованию экологически чистых технологий и тщательному регулированию энергопотребления.

В 2009 г. такие организации, как IBM, Sun, агентство национальной безопасности, Microsoft и Google, объявили, что они создают "зеленые" ЦОДы.

IBM совсем недавно сообщила о создании ЦОДа, самого экологичного в мире. Этот проект совместно финансировали IBM, штат Нью-Йорк и университет г. Сиракузы. Анонс прозвучал в мае 2009-го, а уже через шесть месяцев работы были закончены. Это сооружение потребовало инвестиций в 12,4 млн. долл. и заняло площадь 1115 кв. м (одну половину занимает инфраструктура, другую — сам ЦОД, для которого настелен фальшпол). В нем используются собственная энергетическая установка, обеспечивающая электропитание, отопление и охлаждение, а также созданные в IBM новейшие энергосберегающие серверы, технологии охлаждения компьютеров и ПО системного управления.

Пресс-релиз пестрит цветистыми выражениями о том, что планета спасена и налицо пример для других. Но прочитав три четверти документа, мы натыкаемся на итоговую для всех этих рассуждений фразу: "Это разумное вложение средств... обеспечивающее столь необходимую экономию ресурсов тем компа-

Сотрудники ЦОДов о своих основных целях общего характера на 2010 г.

Исследование корпорации Symantec "Состояние датацентров в 2010 г." основано на результатах опроса 1780 менеджеров ЦОДов в 26 странах, проведенного в ноябре 2009-го. В результате исследования оказалось, что 37% респондентов считают совершенно необходимым сокращение энергопотребления, 30% — использование экологически чистых ИТ-технологий, 54% — снижение затрат.

Источник: *Symantec*.

Защита с помощью hi-tech

МАКСИМ БУКИН

Все участники 15-го форума "Технологии безопасности" компактно уместились в восьмом зале "Крокус Экспо". Если верить официальному релизу, то здесь было представлено "всё, чем располагает современная индустрия для обеспечения безопасности бизнеса, государства и личной безопасности". На самом деле, конечно, показана была только небольшая часть громадного рынка безопасности. Да и количество интересных экспонентов, если отсеять производителей бронежилетов, холодного оружия, систем защиты периметра и т. д., не превышало нескольких десятков компаний. Хотя определенные тенденции развития информационных технологий на рынке систем защиты мы все-таки отследили.

БЕЗОПАСНОСТЬ

Безопасность без проводов

Одно из наиболее интересных направлений, которое получило второе рождение с внедрением сетей 3G операторами "большой тройки", — передача крупных объемов данных через беспроводную сеть. Это может быть как информация о местоположении подвижного объекта (к примеру, милицейской машины или автобуса), так и видеоинформация с камеры наблюдения в квартире или офисе.

В частности, можно отметить миниатюрные решения "Трал-5" и "Кадр-5", похожие по своему функционалу: по сути это малогабаритные беспроводные системы видеонаблюдения для частных пользователей и рынка SoHo. У них достаточно простая задача — обеспечивать подключение одного-двух аналоговых или цифровых камер, внешних охранных датчиков и передачу информации через Интернет на удаленный компьютер или веб-сервер. Причем если у того же "Трала" мобильный модем может быть любым (включая UMTS-сети или мобильный WiMAX), то у "Кадра" устройство для передачи информации встроено непосредственно в блок управления (и пока что там поддерживается только GPRS).

Очень удобно, что просматривать такое видео можно с помощью самого обычного веб-браузера, а устройства поддерживают форматы сжатия видео (H.263 или H.264 или MPEG-4), могут подключаться к внешнему жесткому диску по USB-интерфейсу и работать даже на открытом воздухе: "Кадр" при температуре от –30 до 50 °C, а "Трал" — от 0 до 55°C. Как и у подавляющего большинства камер видеонаблюдения, напряжение питания таких миниатюрных видеосерверов составляет всего 12 В, что позволяет поместить их в термокожухе вместе с видеокамерой.

Уже сейчас в качестве монорешения такие системы активно используются на бензоколонках, в небольших офисах (просматривать картинку можно через обычный нетбук), а также как резервный канал информации при наличии проводных каналов связи, например в офисных зданиях.

Кроме того, по "беспроводке" (обычно по GSM-сетям) все чаще подключают охранно-пожарные сигнализации, а также мониторинговые станции в зданиях (в частности, серии "Контакт"), которые могут взаимодействовать с охранными панелями различных производителей (ISECO, Paradox, Ademco, C-Nord, Visonic). Обычно для на-

Все участники форума разместились в одном зале второго павильона "Крокус Экспо"

дежности работы в них предусмотрена установка как минимум двух SIM-карт от разных операторов связи, встроенная память событий, шифрованная передача информации на пульт централизованного наблюдения охранного предприятия.

Постепенно трансформируются решения слежения за автотранспортом — "самосборные" комплекты не пользуются популярностью, поскольку рынок предлагает широкий спектр типовых решений ("железо" + ПО) для различных типов эксплуатации транспортных средств: для транспортных компаний (ключевые параметры — автоматический контроль отклонений техники от маршрута, контроль количества разгрузок, расхода/слива топлива), автопредприятий, работающих со спецтехникой (выезды за пределы строительной площадки, время работы двигателя "в рабочем режиме" и т. д.), для автобусных парков (контроль маршрута, количество пассажиров), таксопарков (маршруты следования, срабатывание тревожной кнопки). Правда, производители этих решений на выставке очень неохотно говорили о специфике их внедрения — пока что руководство большинства крупных компаний приходится убеждать в том, что это им действительно необходимо.

Отметим, что в подобных проектах используются решения трех основных типов: модули начального уровня с GPS-приемником, более продвинутые решения, где кроме GPS используется и ГЛОНАСС (к примеру, Voyager 2), а также трекеры, способные передавать данные не только о местоположении автомобиля, но и параметры опционно поставляемых датчиков. Возможно, что в скором времени число таких решений увеличится за счет появления на рынке приемников с чипами NV08C-MCM от компании Navis, которые смогут работать не только с GPS/ГЛОНАСС, но и с потенциально интересными Galileo и Compass. Кстати, для отображения информации, полученной с помощью спутниковых навигаторов, обычно используются карты "Яндекса", Google, OziExplorer, векторные карты в формате MP и OpenStreetMap.

Интересно, что на форуме "Технологии безопасности" в категории систем наблюдения за транспортом было представлено определенное количество как отечественных (к примеру, "Ритм"), так и иностранных (GeoVision и т. д.) решений. Общим у них является не только учет информации о передвижениях автотранспорта, но и возможность работы с этой информацией в АСУ, "привязка" видео в салоне и из транспортного средства к его положению на карте, а в перспективе учет дорожной ситуации с помощью информационных сервисов. Стоит отметить и локальные решения. Так, компания "Российские космические системы" представила малогабаритный аппаратно-программный комплекс подвижного пункта мониторинга перевозок опасных и ценных грузов железнодорожным транспортом. Это решение позволяет определять местоположение груза с помощью GPS/ГЛОНАСС, передавать информацию с датчиков (целостность упаковки, влажность, температура и т. д.) в отраслевой центр системного мониторинга через GRPS/EDGE или систему "Гонец" (в разработке), а также организовывать передачу сигнала "Тревога" с использованием международной системы спасения "Коспас-Сарсат".

Интересным нам показалось и решение для патрульных машин ГИБДД от крошечной китайской компании Shanni. В отличие от существующих решений, кроме двух камер, которые устанавливаются на крыше патрульного автомобиля и наблюдают за дорожной ситуацией (информация выводится на монитор в салоне машины и записывается на жесткий диск — своеобразный опломбированный "черный ящик"), еще две, размерами поменьше, находятся в салоне автомобиля и ведут запись происходящего в салоне в постоянном режиме. Возможно, использование именно таких решений сможет нивелировать "человеческий фактор" при общении водителей с сотрудниками ГИБДД.

Перспективное видеонаблюдение

Самые большие стенды кроме системных интеграторов представили производители камер видеонаблюдения: что и говорить, этот сегмент рынка даже в финансовый кризис переживает бурный рост. Разгадка достаточно очевидна —

Просматривать картинку с камер видеонаблюдения, полученную по беспроводной сети, можно и с нетбука

использование технических средств всегда дешевле команды охранников, которые не могут быть в десятке мест одновременно.

Наиболее перспективные разработки в данной области были продемонстрированы Axis Communications, LG, Panasonic и т. д.: фиксированные и купольные поворотные камеры с мощными объективами, системами дистанционного управления и питанием по Ethernet-каналу. Основные тенденции этого рынка — падение цены на сетевые камеры из-за возросшей конкуренции различных производителей, развитие идеи о хранении данных в камерах с помощью карт памяти SD (что позволяет сэкономить на системах хранения), активное развитие систем видеоаналитики за счет улучшения поиска происшествий в цифровых видеоархивах (сами системы видеонаблюдения будут "подписывать" каждый кадр различными тегами, с помощью которых и будет вестись поиск). Интересно, что рынок подобного "железа" все больше зависит от крупных национальных проектов — олимпиад, чемпионатов мира по футболу или различных экономических форумов. Именно такие события являются основным двигателем даже во время финансового кризиса.

Аналогичные изменения происходят и с видеорегистраторами (производители — QNAP, GeoVision и т. д.) для рынка So-

ПРОДОЛЖЕНИЕ НА С. 12 ▶

ниям и организациям, которые стремятся сократить как затраты на ИТ, так и их зависимость от сжигания угля".

Как отделить зерна от плевел при проектировании "зеленого" ЦОДа? Где проходит граница между заботой об окружающей среде и потребностями бизнеса?

Прежде всего необходимо усвоить несколько важнейших принципов проектирования ЦОДов. Они позволят вам сконцентрировать усилия на строительстве здания, которое удовлетворит нынешние и завтрашние нужды вашей организации.

Стройте с расчетом на сегодняшний день и на будущее. Конечно, вы не можете в точности знать, какое оборудование и ПО будут использоваться в вашем ЦОДе через пять лет. Поэтому вам необходим гибкий, модульный и предусматривающий наращивание мощностей проект. Сейчас уже никого не устроит просто большое помещение, заставленное стойками в ожидании нового оборудования.

Однотипные устройства (например, серверы хранения или серверы приложений) следует сгруппировать, чтобы упростить управление ими. Кроме того, вместо охлаждения одного большого объема, заполненного лишь на 25%, разделите помещение на изолированные зоны, где будет последовательно устанавливаться нуждающаяся в охлаждении техника.

В большинстве ЦОДов создаются чередующиеся воздуховоды для горячего и холодного воздуха. Стойки с оборудованием размещаются между ними, в результате чего холодный воздух обтекает машины, поступает в горячий воздуховод и откачивается из ЦОДа с помощью вытяжной вентиляции.

Важно замерить потребление энергии и расходы на отопление, вентиляцию и кондиционирование. Это не только поможет понять, насколько эффективно работает ваш ЦОД (и укажет способы повышения этой эффективности), но и позволит управлять затратами в условиях постоянного роста цен на электричество, а кроме того, облегчит вам соблюдение возросших требований к отчетности о выбросах углекислого газа.

При проектировании современных ЦОДов очень важное значение имеет плотность размещения стоек. Сократить их количество, увеличив плотность, позволят консолидация серверов и виртуализация. Сегодня норма — лезвия и серверы высотой 1-3U. Чем выше плотность оборудования в ЦОДе, тем потенциально эффективнее его работа, особенно если взять такой критерий, как стоимость строительства одного квадратного метра.

Однако более плотное размещение стоек означает и более высокие требования к энергоснабжению, и рост тепловыделения.

В прошлом расход энергии на одну стойку мог достигать 5 кВт, тогда как при нынешнем, более плотном размещении она потребляет 20 кВт и более. Для охлаждения 5-киловаттной стойки было достаточно обычных способов отопления, вентиляции и кондиционирования. Но 20-киловаттная (и тем более потребляющая 30 и даже 40 кВт) требует гораздо более интенсивного охлаждения.

Старайтесь охлаждать каждую стойку в отдельности с использованием либо воды, либо принудительной вентиляции. Совместный проект IBM и Сиракузского университета предусматривает отведение избыточного тепла с помощью охлажденной воды, которая затем прогоняется через охлаждающие каналы в каждой стойке. Такое интенсивное охлаждение гораздо эффективнее отводит тепло, чем обычные системы. В исследовании, проведенном в 2009 г. компанией Emerson, приводятся расчеты, согласно которым использование подобных решений позволяет снизить стоимость охлаждения ЦОДа примерно на 35%.

Никакого фальшпола

Хотите верьте, хотите нет, но в 2010 г. для фальшпола пробьет последний час. Если горячий воздух поднимается вверх, то холодный заканчивает свой путь под фальшполом, где от него мало пользы. Кроме того, приподнятый пол просто не способен выдержать вес плотно размещенных стоек. Стойка высотой 42U с установленными в ней четырнадцатью серверами высотой 3U каждый может весить до полутонны.

Фальшпол просто невозможно эффективно использовать. Много лет назад мне довелось в одном крупном городе возводить ЦОД площадью около 1000 кв. м. Через семь месяцев после завершения строительства наша сеть стала периодически выходить из строя. Потребовалось много человеко-часов, чтобы установить причину неполадок. Оказалось, что крысы перегрызли изоляцию проводов, проложенных под фальшполом. Но и без крыс прокладывать новые провода, вносить изменения в кабельное хозяйство и устранять в нем неисправности будет гораздо проще в отсутствие фальшпола.

Многие организации пришли к выводу, что если в серверной комнате поддерживать температуру на уровне 20 или даже 22 °C, это может обеспечить немедленное и довольно значительное снижение затрат. Мне, например, не нравится работать в помещении, где не выше 17°. Да и само оборудование, выпускаемое в последние годы, предназначено для работы при более высокой температуре. Но прежде чем поднять температуру, сверьтесь со спецификациями оборудования, а в дальнейшем следите за его производительностью.

Поскольку некоторые ЦОДы стали предпочитать постоянный ток, многие производители, в том числе HP, IBM, Dell и Sun, снабжают все или некоторые линейки своих серверов источниками питания, работающими от постоянного тока, что позволяет компьютерам использовать напряжение 48 В. Чтобы облегчить переход с переменного тока на постоянный, поищите серверные шасси с модульными источниками питания.

Первый самарский суперкомпьютер

В День космонавтики в Самарском государственном аэрокосмическом университете им. академика С. П. Королева (СГАУ) запущен в эксплуатацию новый суперкомпьютерный центр (СКЦ) "Сергей Королев" с пиковой производительностью 10 Тфлопс. Этот, первый в Самарской области, высокопроизводительный суперкомпьютер предназначен для решения научно-исследовательских задач, проводимых СГАУ в новом статусе — национального исследовательского университета. Проектирование центра, поставку, монтаж и пусконаладку оборудования выполнил региональный системный интегратор — самарская группа компаний "Парус". Суперкомпьютерный центр построен на базе вычислительного кластера IBM и инженерной инфраструктуры APC. Об особенностях данного проекта проректор по информатизации СГАУ ***Венедикт Кузьмичев и*** *директор ООО "Парус"* ***Виктор Ломакин*** *рассказали нашему обозревателю* ***Владимиру Митину****.*

ИНТЕРВЬЮ


Венедикт Кузьмичев


Виктор Ломакин

PC Week: Чем была вызвана необходимость реализации данного проекта?

ВЕНЕДИКТ КУЗЬМИЧЕВ: В прошлом году СГАУ получил статус национального исследовательского университета и стал одним из ведущих вузов страны, осуществляющих подготовку кадров, а также научные исследования и разработки в интересах авиационно-космической, геоинформационной, оборонной и других высокотехнологичных отраслей экономики страны. Для этих работ требуются высокопроизводительные вычисления. Данный проект реализован как часть инновационной образовательной программы "Развитие центра компетенции и подготовки специалистов мирового уровня в области аэрокосмических и геоинформационных технологий" национального проекта "Образование". Кроме того, нам была оказана поддержка правительством Самарской области в рамках региональной программы "Развитие среды генерации знаний на базе межвузовского медиацентра путем создания суперкомпьютерного центра, ориентированного в том числе на исследования в сфере нанотехнологий и наращивания телекоммуникационной инфраструктуры".

PC Week: Почему для реализации данного проекта СГАУ выбрал компанию "Парус"?

В. К.: Эта компания давно работает с нами в части реализации комплексных проектов по компьютерным сетям, корпоративной сети передачи данных, оснащения серверных помещений, поставки и сопровождения вычислительной техники и серверного оборудования. Так, в 2005—2008 гг. ею были выполнены работы по оснащению компьютерной и телекоммуникационной инфраструктурой Межвузовского медиацентра СГАУ. В середине 2009 г. "Парус" поставил нам кластер HP BladeSystem c3000 производительностью 1,5 Тфлопс, который в настоящее время успешно эксплуатируется сотрудниками университета. Одним словом, "Парус" зарекомендовал себя надежным партнером. Поэтому мы и доверили этой компании оснащение нашего нового суперкомпьютерного центра.

PC Week: Почему за основу были взяты решения IBM и APC?

ВИКТОР ЛОМАКИН: Разработанная APC инфраструктура для ЦОДов, сопровождаемая специальной системой качества по созданию и внедрению проектов, не имеет аналогов, а соотношение качество/цена у данной инфраструктуры, на наш взгляд, наиболее приемлемое. Среди прочего это подтверждается успешным практическим опытом реализации более 10 проектов на данном оборудовании, выполненных нами с 2006 г. Что касается оборудования вычислителя, то здесь наш совместный со СГАУ выбор объясняется тем, что IBM является признанным лидером в области построения высокопроизводительных кластерных решений.

PC Week: Что дал университету этот проект и как скоро он окупится?

В. К.: СГАУ получил современный вычислительный комплекс, который сможет обеспечить решение текущих и перспективных научно-исследовательских задач, расширит горизонты научных исследований, позволит решать совместные задачи с предприятиями авиационно-космического профиля и, самое главное, не только учить студентов, но и повышать квалификацию специалистов со стажем с использованием самых передовых информационных технологий. Говорить о конкретных сроках окупаемости вложений в подготовку специалистов достаточно трудно. Да и едва ли есть методика точного подсчета этих сроков.

PC Week: Что сейчас представляет собой СКЦ "Сергей Королев"?

В. Л.: На первом этапе данного проекта выполнены проектирование и установка универсальной инженерной инфраструктуры СКЦ на базе комплексного решения APC InfraStruXure, включающего шесть напольных 19-дюймовых шкафов высотой 42U. При этом применяется HACS-технология APC (Hot Aisle Containment System) для изоляции так называемого "горячего коридора" — модульных панелей и перегородок, объединяющих шкафы в единую конструкцию и обеспечивающих высокую эффективность системы охлаждения.

Затем были осуществлены поставка и ввод в эксплуатацию ИБП Symmetra PX и кластера IBM Cluster e1350 (восемь шасси IBM BladeCenter H, сервер управления кластером IBM x3650 M2, коммутаторы сети InfiniBand производства QLogic и другое оборудование) с пиковой производительностью 10 Тфлопс (на тесте Linpack — 8,542 Тфлопс). Сейчас мощность потребления установленного вычислительного оборудования IBM составляет около 40 кВт. Кроме того, от ИБП Symmetra PX питается система кондиционирования.

PC Week: С какими трудностями пришлось столкнуться при реализации данного проекта?

В. Л.: Проект выполнялся в условиях отложенного финансирования и при весьма сжатых сроках поставки и монтажа оборудования. Это потребовало привлечения собственных инвестиций для начала проекта. Работы проводились в весьма интенсивном режиме, при постоянном контроле менеджеров нашей компании, дистрибьюторов и производителей. По нашему опыту, такие проекты реализуются не менее чем за шесть месяцев, мы уложились практически в четыре. В процессе настройки кластера были трудности, связанные с запуском новых моделей оборудования. Так, для пусконаладки коммутатора InfiniBand QLogic 12800-180 потребовалось участие производителя в написании новых прошивок микрокодов оборудования. Тесное сотрудничество со службой поддержки производителя позволило быстро решить эти проблемы.


Внешний вид СКЦ "Сергей Королев"

PC Week: Какое системное и прикладное ПО используется в СКЦ "Сергей Королев" сейчас и какое предполагается использовать в будущем?

В. К.: В данном проекте поставлялось только системное ПО. В настоящее время на всех узлах кластера установлено лицензионное программное обеспечение Red Hat Enterprise Linux Release 5, включающее ПО управления кластером xCAT (Extreme Cluster Administration Toolkit). Для управления инфраструктурой используется комплекс программно-аппаратного обеспечения APC InfraStruXure Central. В качестве прикладного ПО суперкомпьютера предполагается использовать программную систему конечно-элементного анализа ANSYS для моделирования задач газодинамики, аэродинамики, механики и т. д., системы инженерного анализа и проектирования Unigraphics, Star — CD, FlowVision и т. п.

PC Week: Как примерно в данном проекте выглядит соотношение стоимость оборудования/стоимость лицензионного ПО/стоимость услуг по установке оборудования?

В. К.: Данное соотношение выглядит примерно так: 85:3:12.

PC Week: В каком направлении будет развиваться данный проект?

В. К.: В перспективе в рамках уже смонтированной и запущенной инженерной инфраструктуры запланировано увеличение мощности кластера IBM до 25 Тфлопс. Соответствующий задел для этого имеется. Проект по данному кластеру разрабатывался для размещения оборудования IBM в шести стойках. В настоящее время из этих шести стоек используются только три. Есть резерв мощности и у ИБП Symmetra PX. Сейчас его полная выходная мощность составляет 112 кВ·А (96 кВ·А с резервированием N+1), но путем добавления модулей её без труда можно увеличить до 160 кВ·А.

PC Week: Спасибо за беседу.

Защита с помощью...

◀ ПРОДОЛЖЕНИЕ СО С. 10

Но — это уже неттопы с мощными жесткими дисками. Основная задача подобных устройств — фиксация информации с камер наблюдения, ее хранение и возможность доступа к ней в удаленном режиме по TCP/IP. Наиболее типичная конфигурация подобных систем для массового рынка небольших компаний-потребителей — до восьми записываемых каналов, один-два закрываемых отсека для жестких дисков с возможностью горячей замены, процессор Intel Atom 1,6 ГГц, 1 Гб ОЗУ, причем ОС чаще всего — Linux для встраиваемых систем.

Кстати, весьма активно продвигаются на рынок не только системы контроля, использующие для авторизации пользователей карты с чипами, но и системы выделения и распознавания лиц. К счастью, эйфория, наблюдавшаяся на заре их становления, сошла на нет, и разработчики, трезво оценивают возможности своих аппаратно-программных комплексов. Сейчас представители компаний-производителей говорят о вероятности распознавания на уровне 80%. Поэтому, несмотря на гипотетическое желание применять их в местах массового пребывания людей (стадионы, кинотеатры, торговые центры, аэропорты, вокзалы, автостанции), а также на пограничных паспортно-визовых контрольных пунктах для выявления преступных элементов, эффективность таких проектов пока под большим вопросом. А вот в работе деловых центров они вполне приемлемы и в сочетании с камерами высокого разрешения и интеграцией с исполнительными устройствами (к примеру, турникетами, лифтами и т. д.) позволяют достаточно точно идентифицировать сотрудников при наличии хотя бы двух ракурсов лица человека (такие возможности есть в Vocord FaceControl, "Face-Инспектор" и т. д.).

Учитывая рост числа небольших предприятий, вполне перспективными являются профессиональные системы видеонаблюдения. Их основа — компактные аппаратно-программные комплексы, позволяющие не только получать информацию от камер, но и оснащать их дополнительным функционалом. Они служат, к примеру, в качестве сегмента безопасности в торговых точках самых разнообразных форматов и размеров, где кроме автоматизации торговли требуются решения, защищающие от краж со стороны как посетителей, так и персонала. Для этого среди прочих элементов безопасности (сигнальные наклейки на товары вкупе с электронными воротами, камеры наблюдения по торговому залу и около стоек с дорогими товарами, упаковка товара в специальные пластиковые поддоны с метками безопасности и т. д.) все чаще внедряют системы видеонаблюдения, контролирующие кассовые операции.

В самом простом варианте текстовые отчеты о покупках поступают в АСУ торговой сети, где на их основе создается выборка по наиболее ходовым товарам, учитываются складские запасы и т. д. Но если добавить к этому специальное ПО ("POS-Инспектор", SET Prisma, решения от EasService и т. д.) и по одной камере на каждую кассу, то можно кроме статистики продаж получить видеозапись процесса расчета кассира с покупателем с возможностью поиска видеофрагмента по всем операциям кассира. На каждое действие сотрудника магазина устанавливается цифровая метка, по которой можно отследить получение денег за товар без его регистрации, махинации с кредитными картами, изменение содержания кассового чека, фиктивный возврат товара и т. д.

PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
АПРЕЛЬ • 2010 • МОСКВА
http://www.pcweek.ru

Защита конечных точек сегодня

ВАЛЕРИЙ ВАСИЛЬЕВ

Согласно результатам исследования компании Webroot, 80% от участвовавших в опросе восьмисот ИТ-служащих США, Великобритании и Австралии считают, что в текущем году основным источником информационных угроз, серьезно осложняющих работу предприятий, являются технологии Web 2.0. Этот вывод подтверждают также специалисты ряда ведущих мировых ИБ-поставщиков и аналитических компаний. Например, аналитики Gartner пишут, что киберпреступники активно используют веб как среду распространения вредоносных программ и канал управления ими.

ОБЗОРЫ

Казалось бы, коль скоро основные угрозы вновь переместились вовне, компаниям опять нужно сосредоточиться на защите периметра. Однако установка новых шлюзовых решений для борьбы с угрозами Web 2.0 вовсе не означает, что можно ослабить внимание к средствам прямой защиты конечных точек, как правило, располагающихся позади этих шлюзов, внутри периметровой защиты. Так, посвященный именно этой проблеме опрос, проведенный компанией Check Point Software среди двухсот с лишним специалистов по ИТ и компьютерной безопасности из разных стран и секторов экономики, привел экспертов к выводу о том, что количество незащищенных конечных точек в корпоративном сегменте растет. Похоже, сами предприятия относятся к этой ситуации с пониманием, поскольку около 47% респондентов указали, что в течение года планируют купить новые продукты для защиты конечных точек, при том что у 90% из них уже используются антивирусные пакеты, а примерно у половины установлены также персональные шлюзы безопасности и средства VPN.

Валерий Ледовской: "Преимущества антивируса, как услуги, очевидны — низкая стоимость, надёжность защиты, удобство оплаты, более точное планирование расходов, снижение затрат на оплату работы администраторов сети"

Функциональный состав решения для защиты конечных точек

Говоря о функциональном составе решения для защиты конечных точек и о его основных характеристиках, эксперты единодушно указывают на комплексность, что означает способность защищать и мобильные, и стационарные конечные точки как от внешних, так и от внутренних атак. Именно поэтому устанавливаемые практически на всех рабочих станциях антивирусы давно переросли рамки средства противодействия только вирусным заражениям, превратившись, по выражению аналитика компании "Доктор Веб" Валерия Ледовского, в комбайны, вобравшие в себя кроме антивирусного также и функционал персонального межсетевого экрана, способность защищать рабочие станции от широкого класса вредоносных программ, спама и внешних атак, используя для этого не только сигнатурный анализ, но и проактивные технологии обнаружения злонамеренных активностей в вычислительной среде точки подключения к сети (HIPS). Важным компонентом антивируса, как отмечает г-н Ледовской, являются средства защиты самого антивируса от используемых современными вредоносными программами изощренных механизмов блокирования его работы.

На основании проведенных исследований эксперты из компании Webroot пришли к удручающему выводу о состоянии интернет-безопасности в компаниях, несмотря на то что в 88% опрошенных организаций введены жесткие политики пользования Интернетом, в 69% предприятий регулярно доводят до каждого сотрудника информацию об интернет- опасностях, у 56% респондентов есть строгие запреты на посещение сайтов социальных сетей, а в 44% не реже чем раз в год рассылают соответствующие оповещения. Из этого следует, что одними организационными мерами не обойтись и параллельно по-прежнему нужно совершенствовать технические средства контроля информационной безопасности рабочих мест.

Возрастающая роль мониторинга и принудительного выполнения политик в области ИБ определяет потребность в функционале контроля доступа к сети (NAC). Опрос Check Point показывает, что 22% компаний уже готовы купить NAC-продукты для того, чтобы в соответствии с установленными политиками контролировать состояние пользовательских компьютеров.

Оправданная статистикой ИБ-инцидентов и диктуемая регуляторами озабоченность компаний сохранением конфиденциальности определенного вида корпоративной информации обуславливает рост спроса на средства борьбы с утечками данных (DLP). Системы DLP обеспечивают контроль обращения пользователей с информацией, помогают бороться с кражами и непреднамеренными утечками данных, представляющих ценность для бизнеса или относящихся к разряду критически важных в силу действующих регулятивных требований.

Практически неотъемлемым для систем защиты конечных точек становится единый для всего комплекса средств такой защиты интерфейс. Причем к объединению под общим "зонтиком" администрирования и эксплуатации выпускаются не только моновендорные решения. К примеру, компании BigFix и Trend Micro объединились в рамках OEM-партнерства для того, чтобы обеспечить пользователям решений безопасности, построенных на продуктах Trend Micro, доступ к разработанным BigFix функциям управления жизненным циклом компьютеров (PCLCM), таким как управление патчами и электропотреблением.

Алексей Мурзин: "Для успешных продаж необходимо многоуровневое конкурентное сравнение по всем характеристикам EPP-решения, начиная с параметров защищенности и заканчивая показателями ROI и TCO"

Важное значение, особенно для мобильных средств подключения к корпоративной сети, приобретает функция шифрования данных на жестких дисках и сменных носителях информации. Чтобы подчеркнуть актуальность этого средства защиты, можно сослаться на весьма показательные данные из США: в 2008 г. только в аэропортах этой страны еженедельно терялось в среднем 12 тыс. ноутбуков. По мере неуклонного роста количества мобильных коммуникационно-вычислительных устройств будет возрастать и роль шифрования, ведь уже сегодня ноутбуков покупается больше, чем настольных систем. Правда, технический консультант Trend Micro в России и СНГ Николай Романов обращает внимание на то, что распространение средств шифрования данных иностранного производства в России пока имеет законодательные ограничения и их использование в ряде случаев не представляется возможным. "Однако не исключаю, что под давлением объективных факторов ситуация со временем изменится", — полагает он.

Состояние рынка средств защиты конечных точек

Начиная с 2007 г. компания Gartner выделила такие средства в отдельный класс продуктов, который назвала платформами защиты конечных точек (Endpoint Protection Platform, EPP). Это обособление аналитики обосновывают тем, что специализированные рынки традиционных антивирусов, средств защиты от шпионских программ и персональных межсетевых экранов вытесняются более широкими комплексами взаимосвязанных технологий безопасности.

Николай Романов: "Следует четко разделять рабочие места сотрудников, не обрабатывающих персональные данные, и тех специалистов, компьютеры которых надлежит защищать особенно тщательно"

Зафиксировав в 2008 г. объем мирового рынка EPP в 2,5 млрд. долл., Gartner на 2009-й предсказывала его рост на 8% (данных о точности прогноза пока нет). Лидерами, разделяющими между собой 85% этого рынка, в прошлом году оставались McAfee, Symantec и Trend Micro. Вместе с тем компания ожидает в нынешнем году усиления позиций в области EPP от Microsoft, отмечая, что в основном это касается сегмента среднего и малого бизнеса. В 2009-м в магическом квадранте EPP появились новички: фирмы Eset, Prevx и SkyRecon Sytems. Активное поведение этих молодых в технологиях EPP игроков — провидцев и претендентов — стимулирует лидеров к наращиванию функционала и вместе с тем к тому, чтобы держать разумные цены.

Gartner обращает внимание на то, что поставщики средств контроля операционных ресурсов, среди которых присутствуют BigFix и LANDesk, активно дополняют свои инструменты средствами сигнатурной и проактивной защиты информации, поглощая производителей таких продуктов или заключая с ними партнерские соглашения, и тем самым упрочивают свои позиции в магическом квадранте вендоров EPP. Со своей стороны традиционные ИБ-вендоры наступают там, где сильны BigFix и LANDesk. Например, Trend Micro и IBM некоторое время назад лицензировали технологию управления жизненным циклом рабочих станций PCLCM компании BigFix, а Symantec купила фирму Altiris и интегрировала ее средства с аналогичным функционалом в управление своей платформой Symantec Endpoint Protection.

Отмечается, что только четыре вендора, присутствующие в магическом квадранте EPP, — Check Point, McAfee, Sophos и Symantec — имеют функционал NAC, достаточно развитый для того, чтобы одновременно находиться и в магическом квадранте поставщиков NAC. Продукты остальных EPP-вендоров либо имеют только основу функционала NAC, либо вообще игнорируют эту технологию, склоняясь к другим способам контроля доступа компьютеров в сеть, основанным на технологиях сетевого управления.

Факторы влияния на рынок средств защиты конечных точек

Экономическая обстановка. Согласно исследованию состояния ИБ в 2009 г. в России, которое недавно завершила компания PricewaterhouseCoopers, почти половина респондентов считают, что финансовый кризис не оказал значительного влияния на обеспечение информационной безопасности в российских компаниях.

Регулирование. По мнению руководителя отдела компании "Айдеко" Алексея Мурзина, регуляторы, долгое время даже по ключевым вопросам ИБ занимавшие позицию: "Делайте, что хотите, только чтобы это не противоречило руководящим документам", — теперь активно включились в процессы выработки конкретных рекомендаций по всем основным аспектам защиты конечных точек. Как следствие, отмечает он, стремительно растет спрос на сертифицированные решения, а доверие заказчиков смещается в пользу российских ИБ-производителей, тогда как еще два-три года назад во многих сегментах ИБ-рынка первые позиции уверенно держали западные компании. Вместе с тем выбор сертифицированных продуктов делается не всегда осознанно, поскольку еще не все операторы детально погрузились в особенности национального закона о защите персональных данных и зачастую выбирают "самое сертифицированное" решение, тогда как в конкретных условиях своей ИТ-инфраструктуры могли бы обходиться и менее дорогими средствами. "Однако правовые знания ИТ-менеджеров стремительно растут, и такое

ПРОДОЛЖЕНИЕ НА С. 15 ▶

Важный рубеж корпоративной ИБ

ИНТЕРВЬЮ

Используя компьютерные сети, злоумышленники нацелены в конечном счете на места хранения и обработки данных, к которым относятся и конечные точки корпоративных сетей. О состоянии российского рынка средств защиты конечных точек, об отношении российских компаний к этому рубежу информационной безопасности (ИБ) ***Константин Монахов,*** *руководитель отдела по работе с поставщиками дистрибьюторской компании MONT, рассказал научному редактору еженедельника PC Week/RE* ***Валерию Васильеву****. В продуктовом портфеле MONT есть решения ИБ-вендора Trend Micro, который одним из самых первых начал предлагать для защиты конечных точек новые технологии — облачные вычисления и репутационный подход.*

Константин Монахов

PC Week: Кто в России покупает продукты для защиты конечных точек?

КОНСТАНТИН МОНАХОВ: Покупают все — компаниям и организациям разных размеров, из разных отраслей и регионов уже понятно, что за ИБ следить нужно, а тот минимальный объем корпоративной ИБ, с которого следует стартовать, как раз и представляет собой антивирусную защиту конечных точек. Понятно, что защита конечных точек не спасает от всех проблем, связанных с ИБ, но именно на этом уровне наиболее эффективно решается их существенная часть, а предотвращение некоторых угроз возможно только на данном уровне

PC Week: Какова ваша оценка подходов российских корпоративных пользователей к организации защиты конечных точек?

К. М.: Я бы оценил подход российских компаний к задачам защиты конечных точек как зрелый. Они эшелонируют эту защиту, используют в ней средства, не только устанавливаемые на самих рабочих станциях, но и сетевые ресурсы этого назначения, а также и организационные меры в виде соответствующих политик. Можно отметить, что крупные компании подходят к защите конечных точек более системно, как и к обеспечению ИБ в целом, и чем крупнее заказчик, тем полнее функционал для защиты конечных точек он использует. Растет спрос на "тяжелые" масштабные решения, в том числе и в регионах.

PC Week: Какова в России емкость рынка продуктов для защиты конечных точек?

К. М.: По моим оценкам, российский ИБ-рынок можно оценить примерно в 250 млн. долл. Продукты для защиты конечных точек активно покупаются по всей стране, и в общем объеме их доля составляет около 150 млн. долл. При этом нужно учитывать, что отдельно продукты для защиты конечных точек покупаются редко. Как правило, они поставляются в рамках некоторых комплексных ИТ-проектов. Например, антивирусную защиту серверов и рабочих станций заказчики гораздо чаще покупают в составе программного пакета Trend Micro NeatSuite, нежели в виде отдельных антивирусных продуктов этого вендора.

PC Week: Что происходит со спросом на продукты защиты конечных точек в России ?

К. М.: Экономический кризис в прошлом году не отразился на рынке ИБ так жестко, как, например, на рынке программных приложений. В среднем за 2009 г. российский ИБ-рынок подрос на 8%. Характерно, что некоторые отечественные ИБ-вендоры даже сумели заметно превзойти этот показатель. Не думаю, что в текущем году ситуация будет резко отличаться от прошлогодней, — кризис продолжается, компании поиздержались. Однако падать рынок по-прежнему не будет, хотя и удвоения объемов продаж, как это было накануне кризиса, ожидать не приходится. Скорее всего, он подрастет на 10—15%.

Существенно, что в спросе корпоративных заказчиков четко обозначился комплексный подход к ИБ в целом и к защите конечных точек в частности. Чаще внедряются многовендорные ИБ-решения. Что касается влияния регуляторов, то, разумеется, прежде всего нужно иметь в виду закон "О персональных данных". Перенос сроков контроля соответствия требованиям этого закона систем защиты персональных данных (СЗПДн) на 1 января 2011 г. привел к тому, что компании всерьез занялись аудитом своих информационных систем. Наши партнеры, участвующие в этих работах, отмечают озабоченность заказчиков задачами четкого выделения ПД из общей массы, оптимизации их структуры и размещения в ИТ-инфраструктуре, назначения ответственных за обработку, определения способов и средств защиты. Спрос на продукты защиты ПД, куда входят и средства защиты конечных точек, начнется во второй половине года, когда заказчики более четко поймут, какие ИБ-продукты для соответствия закону им нужны. Да и вендоры к этому сроку подтянутся с сертификацией своих продуктов — сегодня еще не все, особенно иностранные производители, успели завершить то, что наметили с этими процедурами в связи с законом "О персональных данных".

PC Week: Насколько типизированы по функционалу продукты для защиты конечных точек?

К. М.: Практически у всех лидирующих ИБ-вендоров для защиты конечных точек есть продуктовые комплекты, куда входят антивирусы, средства проактивной защиты, межсетевые экраны, шифрование, средства предотвращения атак, репутационный контроль ресурсов. К ключевым средствам защиты, перечисленным выше, также можно добавить ряд вспомогательных средств, решающих задачи защиты информации в несколько ином срезе. Уже давно Trend Micro предлагает механизм Network Admission Control (NAC), позволяющий решить вопросы соответствия подключающихся к корпоративным ресурсам конечных точек. В рамках современных проблем с утечками данных компания также предложила свою концепцию защиты, реализованную с помощью как классических средств (на основе регулярных выражений и ключевых слов/фраз), так и с помощью технологии цифровых отпечатков (Fingerprinting).

На мой взгляд, важной частью защиты конечных точек являются средства защиты от утечек данных (DLP), хотя пока их у нас в стране продавать трудно. Как утверждают наши партнеры, сегодня обосновать актуальность такой защиты нелегко, и хотя в пилотных проектах внедрения DLP часто развертывается самый полный функционал таких систем, в последующих внедрениях в масштабах всей компании заказчики реализуют только малую часть функционала DLP. Видимо, наши компании еще не пришли к пониманию ценности своих корпоративных данных. Особенно это заметно на фоне растущего стремления выполнять требования по защите персональных данных, которые составляют только малую часть корпоративных информационных ресурсов и зачастую не самую ценную.

PC Week: Среди других вы продвигаете средства защиты конечных точек разработки компании Trend Micro. Чем руководствовался дистрибьютор MONT, когда включал в свой продуктовый портфель продукты этого вендора?

К. М.: На самом деле Trend Micro интересна нам как компания, входящая в тройку сильнейших мировых вендоров рынка ИБ. Она является также одним из лидеров средств защиты конечных точек, реализуя в этой области новые подходы.

PC Week: Резкое увеличение количества вредоносов снизило эффективность сигнатурного детектирования заражений. Какие проактивные средства для защиты конечных точек предлагает Trend Micro?

К. М.: Долгое время антивирусные средства защиты являлись основой защиты конечной точки и их возможности были слишком переоценены. В последние два-три года ситуация сильно изменилась в связи с резким увеличением числа инцидентов, связанных с многовекторностью угроз и разнообразием сценариев. В связи с этим в значительной степени возрос интерес к дополнительным механизмам защиты конечных точек, к которым можно отнести HIPS, поведенческий анализ, средства шифрования в рамках работы мобильных пользователей и ряд вспомогательных средств (например, решения для блокировки использования уязвимостей, встроенные в средства защиты конечных точек).

Trend Micro обеспечивает максимальный охват существующих угроз, которые есть сейчас, и старается опережать события, предлагая новые подходы. К ним можно отнести систему проверки конечных точек как локальными средствами (HIPS, брандмауэр, поведенческие средства анализа, контроль периферийных устройств), так и средствами распределенной архитектуры Smart Protection Network, которая включает проверку подозрительных данных (файловая репутация) и запросов к веб-ресурсам (проверка их легитимности — веб-репутация).

Что наиболее важно, Trend Micro предлагает свои технологические возможности для клиентов любых масштабов.

PC Week: Как реагируют российские заказчики на вынос сигнатурных проверок в облака?

К. М.: В первую очередь эти возможности, фактически представляющие собой аутсорсинг ИБ-услуг, интересны для СМБ. Крупные заказчики пока предпочитают здесь обходиться своими силами. Хотя, на мой взгляд, за этим будущее. Сегодня уже есть спрос на услуги по проверке корпоративной электронной почты, фильтрации интернет-трафика. Замечу, что российские компании категорически предпочитают работать по схеме аутсорсинга не с иностранными вендорами (выступающим в роли провайдера услуг), а с отечественными провайдерами. При этом последние обслуживают российских же клиентов, используя в своих ЦОДах решения иностранных вендоров. Такие схемы у отечественных заказчиков вызывают доверия больше, нежели перенаправление своего трафика в зарубежные ЦОДы.

PC Week: Как влияет перемещение ИТ в облака на продуктовый портфель средств защиты конечных точек и на их дистрибуцию?

К. М.: Такие продукты только начали появляться, отражая зарождение спроса. В абсолютном исчислении их доля пока очень мала — доли процентов. Что касается структуры канала, то она остается прежней.

PC Week: Одним из основных требований к ИБ-продуктам, тем более композитным, к которым относятся решения по защите конечных точек, является централизованное управление. Какие средства для этого есть у Trend Micro? Насколько они подходят для сегмента среднего и малого бизнеса (СМБ)?

К. М.: Trend Micro дружественно настроен к СМБ и создал целую линейку продуктов под названием Worry-Free. В ней учтено все, что нужно СМБ с точки зрения защиты и централизованного управления (с учетом дефицита квалифицированного ИТ-персонала в небольших компаниях). В решениях, ориентированных на крупных клиентов сегмента Enterprise, есть полнофункциональный продукт централизованного управления Control Manager, который концентрирует в рамках единой консоли все необходимые для управления ИБ функции. Вместе с тем нужно отметить, что сложные решения Trend Micro масштабируются и под заказчиков с несколькими десятками рабочих мест. Все дело в целесообразности использования заложенного в Enterprise-решениях функционала в масштабах небольшой компании.

PC Week: Функционал управления жизненным циклом компьютеров (PCLCM) Trend Micro поставляет при условии 10 тыс. конечных точек у заказчика. Не считаете ли вы, что это много даже для крупных заказчиков, особенно в России?

К. М.: Для начала замечу, что функционал PCLCM, который Trend Micro заимствует на партнерских условиях у компании BigFix, как показывает опыт, небольшим компаниям не нужен — его используют только очень крупные заказчики. Ну и потом, чтобы купить средства PCLCM у Trend Micro, у заказчика по ныне действующим условиям должно быть 5 тыс. точек подключения, а не 10 тыс.

PC Week: Сейчас у Trend Micro из функций PCLCM только управление патчами и электропотреблением. Предполагает ли вендор этот функционал в рамках своего решения для защиты конечных точек?

К. М.: Если говорить о решениях для защиты конечных точек, то на сегодняшний день нет информации о планах Trend Micro расширять функционал PCLCM. У партнера Trend Micro, компании BigFix, есть продукты с полным набором таких функций, они интегрируемы в платформы защиты конечных точек, однако заказчикам Trend Micro эти продукты пока поставляются по каналам BigFix.

PC Week: В качестве обязательной технологии защиты конечных точек эксперты называют шифрование данных. Есть ли этот функционал в решениях Trend Micro для защиты конечных точек? Не испытываете ли вы трудностей с их продвижением в среде отечественных заказчиков из-за специфики сертификации средств шифрования в России?

К. М.: У Trend Micro в продуктах защиты конечных точек есть средства шифрования. Но из-за сложности процедуры их сертификации в России преимущества в этой области имеют отечественные вендоры, а потому этот функционал продуктов Trend Micro у нас в стране не востребован, как, впрочем, и аналогичных продуктов других зарубежных ИБ-поставщиков.

PC Week: Благодарю за беседу.

Защита...

◀ ПРОДОЛЖЕНИЕ СО С. 13

положение дел долго не продержится", — полагает г-н Мурзин.

Положительное влияние продиктованной законом "О персональных данных" необходимости использования сертифицированных средств, и прежде всего такого массового продукта, как антивирус, Валерий Ледовской усматривает в снижении показателя использования нелицензионных программных продуктов в корпоративной среде.

Николай Романов обращает внимание на то, что, организуя выполнение требований к обработке персональных данных, компании должны четко разделять рабочие места сотрудников, которые обрабатывают данные, не являющиеся персональными (к ним закон гораздо менее требователен, и потому их защита обходится гораздое дешевле), и специалистов, чьи компьютеры надлежит защищать особенно тщательно (например, бухгалтеров и работников кадровой службы).

Изменение ландшафта угроз. Аналитики Gartner отмечают, что сигнатурные антивирусные движки быстро утрачивают эффективность из-за роста количества вредоносных программ в геометрической пропорции и слабого противодействия целевым атакам. Они не способны противостоять неизвестным угрозам и угрозам "нулевого дня". Поэтому, считают в Gartner, сегодня эффективнее несигнатурные проактивные технологии, такие как HIPS, а также контроль работы конечных точек, направленный на обнаружение ресурсов, управление конфигурациями, оценку угроз, управление ПО, использование белых списков.

Такие компании, как F-Secure, McAfee, Trend Micro, Prevx, активно внедряют в свои продукты поддержку прямых клиентских обращений к облачным сигнатурным базам данных и репутационным характеристикам для определения статуса безопасности подозреваемых ресурсов. Gartner отмечает, что в 2009 г. ИБ-вендоры существенно усовершенствовали свои технологии обнаружения руткитов. Согласно данным этой аналитической компании, вендоры платформ EPP по-прежнему направляют свои усилия на повышение защищенности информации, реализуя для этого полное шифрование данных жестких дисков и съемных носителей, функционал DLP, контроль портов и устройств. При этом, наращивая возможности своих EPP, вендоры из-за жесткой конкуренции ограничены в возможности поднимать цены.

Тенденции развития

Оценивая динамику российского рынка средств защиты конечных точек, Алексей Мурзин полагает, что его объем будет расти, опережая показатели, связанные только с увеличением количества вновь создаваемых рабочих мест. Что касается технологических тенденций, то, по его мнению, хитом продаж в этом сегменте стало бы решение по фильтрации и контролю исходящего голосового трафика. "Однако в ближайшей перспективе таких средств контроля, к сожалению, ждать не приходится", — заключает он.

Консолидация технологий и централизация управления. Эксперты отмечают, что ИБ-угрозы становятся комплексными, утрачивают признаки только внешних или внутренних. Аналогичные процессы происходят и со средствами защиты: размываются технологические и продуктовые границы в пользу построения комплексных систем ИБ с централизованным управлением средствами защиты, мониторингом и корреляцией ИБ-событий, автоматизацией принятия решений; возрастает актуальность создания центров управления информационной безопасностью (Security Operations Center, SOC). По мнению Алексея Мурзина, сегмент EPP тоже развивается в этом направлении — компании разрабатывают решения, централизованно контролирующие поведение конечных точек, продукты, в которых реализован комплексный подход с поддержкой технологий защиты от интернет-угроз и утечек данных, с возможностью блокирования несанкционированной активности устройств и отдельных портов, с шифрованием данных, аутентификацией пользователей, управлением правами доступа и политиками использования приложений. "Такие решения должны иметь единые средства администрирования и мониторинга, учитывать особенности национального регулирования и способность постоянно актуализироваться, чтобы работать на опережение киберпреступников", — считает он.

Как отмечалось выше со ссылкой на сведения Gartner, развитие платформ EPP идет в условиях жесткой конкуренции, не позволяющей поставщикам поднимать цены. Вместе с этим наблюдается повышение зрелости и у заказчиков EPP. Говоря о российских компаниях, Алексей Мурзин отмечает их возросшую прагматичность в выборе средств защиты. "Сегодня вендору недостаточно показать весь функционал своего решения и сослаться на примеры удачного внедрения. Для успешных продаж стало необходимо многоуровневое конкурентное сравнение по всем характеристикам EPP-решения, начиная с параметров защищенности и заканчивая показателями ROI и TCO", — сказал он.

Защита конечных точек как услуга. Как полагает Николай Романов, вариант аутсорсинга в защите конечных точек интересен компаниям, не желающим тратить собственные ресурсы на обслуживание подобных систем, но прежде всего он важен небольшим компаниям, у которых таких ресурсов попросту недостаточно. Он считает также, что классические клиент-серверные решения в режиме аутсорсинга для большинства небольших компаний остаются дорогими и сложными в эксплуатации. Зато решения типа Hosted (решение как услуга), по его мнению, гораздо привлекательнее: никакого оборудования на стороне заказчика, никаких затрат на администрирование, и можно все внимание переключить на вопросы основного бизнеса. "Такие решения уже есть, и они хорошо зарекомендовали себя", — говорит он, ссылаясь на опыт продвижения hosted-версии продукта Trend Micro Worry-Free Business Security.

Валерий Ледовской напоминает, что с середины февраля, с выходом интернет-сервиса Dr.Web AV-Desk 5.0.1 компании "Доктор Веб", корпоративным пользователям стала доступна по модели "программное обеспечение как сервис" услуга "Антивирус Dr.Web". "Преимущества использования антивируса, как услуги, очевидны: низкая стоимость, надёжность защиты, удобство оплаты и более точное планирование расходов, снижение затрат на оплату работы администраторов локальной сети", — пояснил Валерий Ледовской.

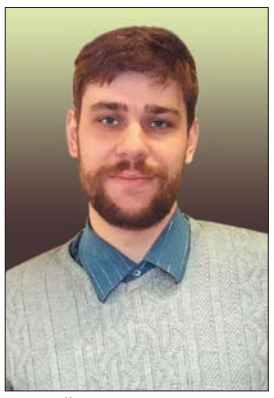
Аутсорсинг позволяет за счет провайдера оперативно реагировать на изменение ландшафта угроз: если провайдер не успевает перестроить свою защиту, можно перейти к другому, более расторопному. Вместе с тем, по мнению Алексея Мурзина, сегмент "безопасность как услуга" в общей картине рынка пока заметно себя не проявляет, спрос здесь невысокий. "Российские заказчики ещё не доверяют безопасности «в облаках»", — утверждает он.

Защита конечных точек в "Сибстройнефтегазе"

ВАЛЕРИЙ ВАСИЛЬЕВ

Компания "Сибстройнефтегаз" специализируется на производстве работ, связанных с повышенной опасностью. Это строительство нефте- и газодобывающих производств и объектов, магистральных трубопроводов, объектов газового хозяйства. Регион ее деятельности — Томская, Кемеровская, Новосибирская и Омская области.

ПРОЕКТЫ



Николай Иванов

Проект по внедрению решения для защиты конечных точек от интернет-угроз был связан с расширением бизнеса компании и строительством нового офиса с новой сетевой инфраструктурой, а также тем, что ранее используемый для защиты продукт перестал устраивать компанию из-за низкой устойчивости к атакам и большого числа уязвимостей в программном коде. При выборе замены, как сообщил главный ИТ-специалист "Сибстройнефтегаза" Дмитрий Пшеничников, на первом месте для компании стояли показатели эффективности защиты и отказоустойчивости нового решения.

Изначально заказчик склонялся к решениям, построенным на технологии NAT, с возможностями контроля активности конечных точек и блокирования различных типов паразитного трафика. Из предложений подобного класса специалисты "Сибстройнефтегаза" остановили свой выбор на интернет-шлюзе Ideco Internet Control Server (ICS) — программном решении, базовым компонентом защиты в котором является межсетевой экран с возможностью фильтрации трафика по любому из полей заголовка IP-пакета.

Как сообщил ведущий специалист томской компании-интегратора ТПК "Галактика" Николай Иванов, настройки системного межсетевого экрана шлюза по умолчанию запрещают все явно не разрешенные действия пользователей. Такой подход обязывает администратора системы изменить фабричные установки в соответствии с корпоративными правилами ИБ. Все исполняемые файлы решения хранятся в области read-only, статус которой, как утверждает компания-разработчик "Айдеко", не может изменить даже администратор — таким образом исключается модификация или подмена файлов.

Дмитрий Пшеничников

Шлюз автоматически обнаруживает подключенные к сети конечные точки, позволяя для каждой из них (или для каждого отдельного пользователя) назначать набор правил работы в Интернете, в том числе запрет определенных типов трафика и контентную фильтрацию интернет-запросов по 18 категориям. Предусмотрены также групповые настройки контроля электронной почты.

Как показали тестовые испытания, Ideco ICS обеспечивал требуемый заказчику уровень защиты от внешних атак (как самого сервера, так и конечных точек), обладал хорошей функциональностью (в шлюзе реализовано около 20 встроенных сетевых служб) и удобным веб-интерфейсом, позволяющим администратору устройства большинство рутинных операций выполнять в один-два клика мышкой.

Кроме того, как подчеркнул Николай Иванов, сервер Ideco ICS в сравнении с конкурирующими вариантами (в том числе с продуктами Microsoft) отличался меньшими стоимостью лицензирования и совокупной стоимостью владения, а также, как со своей стороны отметил заказчик, более оперативной технической поддержкой. Заказчику также понравилось то, что база данных пользователей сети может быть синхронизирована со штатным расписанием, что позволяет контролировать интернет-безопасность в соответствии с правилами использования Интернета, разными для разных подразделений. Так, для бухгалтерии была организована поддержка защищенных соединений интернет-банкинга, а для проектировщиков настроили высокоскоростное соединение со службами заказчика.

Выбору шлюза Ideco ICS поспособствовало также и то, что этот продукт позволял завершить проект в отводимые на все работы две недели. Со стороны интегратора в проекте участвовали два специалиста. В качестве куратора от "Сибстройнефтегаза" в проекте участвовал Дмитрий Пшеничников. Как он утверждает, после завершения монтажа и первичной настройки программного обеспечения сервера, на которые ушло три дня, "всё заработало сразу". Для встраивания Ideco ICS в существующую сетевую инфраструктуру, по свидетельству компании "Галактика", не потребовалось вводить какие-либо инфраструктурные изменения, поменялись только настройки VPN-шлюза. Развертывание и окончательную настройку шлюза в соответствии в ИБ-политиками заказчика (кстати, в удаленном режиме) выполнил один специалист "Галактики", на что у него ушла примерно неделя. Общий бюджет проекта не превысил 2,5 тыс. долл.

Как показали тестовые испытания, Ideco ICS обеспечивал требуемый заказчику уровень защиты от внешних атак, обладал хорошей функциональностью и удобным веб-интерфейсом.

По словам Дмитрия Пшеничникова, с завершением проекта заказчик решил изначально поставленную задачу защиты конечных точек от внешних угроз. Выполненные собственными силами с помощью сетевых сканеров XSpider и Nessus тесты на проникновение и сканирование сети подтвердили ожидаемый результат: безопасность конечных точек обеспечена.

Согласно планам заказчик намеревается использовать обещаемый разработчиком в следующих версиях продукта функционал защиты от утечек данных — средства анализа содержимого и логирования потоков исходящего трафика. В настоящее время из возможностей контроля утечек данных, реализованных в шлюзе Ideco ICS, заказчик применяет блокировку отправки вложений электронной почты, перенаправление трафика на рабочие места сотрудников службы ИБ, блокировку использования публичных почтовый систем и интернет-форумов.

Внесите поправки в свои ИБ-политики

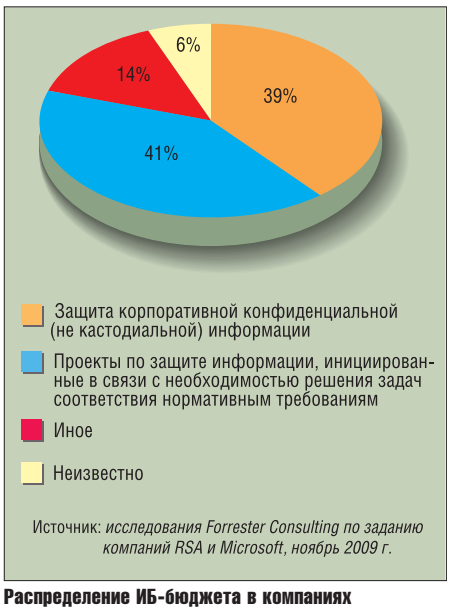
ВАЛЕРИЙ ВАСИЛЬЕВ

Год 2010-й знаменателен для российских компаний и организаций двумя рубежными событиями в области информационной безопасности (ИБ), подойти к которым они должны, как того хотелось бы установившим эти рубежи регуляторам, со стопроцентной готовностью.

БЕЗОПАСНОСТЬ

Начиная с октября 2010-го совет PCI Security Standards Council обещает начать штрафовать российских участников платежных систем American Express, Discover Card, JCB, MasterCard и Visa за невыполнение требований стандарта PCI DSS. Это касается в основном российских компаний из финансового и торгового секторов (точнее, всех тех, кто передает, обрабатывает и хранит данные держателей платежных карт упомянутых систем). Ну а в декабре закончатся все отсрочки, на которые согласилось государство в начале текущего года ввиду фатальной неготовности операторов персональных данных, и санкции за несоответствие закону "О персональных данных" будут введены в полном объеме. А это уже касается всех структур, занимающихся как коммерческой, так и иной деятельностью, связанной с обработкой персональных данных, т. е. практически всех организаций, предприятий, фирм, действующих на территории России.

Учитывая серьезные изменения, которые российские организации должны будут внести в свои системы обеспечения ИБ (и неизбежно пойти при этом на немалые ресурсные затраты) для выполнения требований регуляторов, можно с уверенностью сказать, что им будут интересны результаты завершенных в конце прошлого года компанией Forrester Consulting исследований, в которых приняли участие руководители информационных отделов из 305 компаний по всему миру. Эти результаты могут помочь эффективнее распределять корпоративные ИБ-бюджеты между затратами на выполнение требований внешних регуляторов и затратами на защиту информации, критически важной для бизнеса.



Распределение ИБ-бюджета в компаниях

Исследователи из Forrester Consulting ставили перед собой цель определить количество конфиденциальной информации в компаниях, уровень контроля за нею, побудительные мотивы разработки и выполнения корпоративных программ защиты информации, стоимость последствий инцидентов, связанных с утратой конфиденциальной информации. Защищаемые данные они разделили на конфиденциальные, обеспечивающие долговременные конкурентные преимущества компании (такие, как планы разработки продуктов, прогнозы прибыли, профессиональные секреты), и кастодиальные (custodial) данные, утрата которых связана с наказанием в соответствии с законом, регулирующим обращение с такими данными (к ним принадлежат данные о клиентах, медицинские сведения, пользовательская информация о платежных картах и т. п.).

Было установлено, что в среднем около 60% корпоративной информации относится к конфиденциальной (хотя в соотношении между конфиденциальной и кастодиальной информацией была выявлена существенная разница у предприятий и организаций разного вида деятельности). Проприетарные секреты компаний, согласно выводам исследователей, вдове ценнее, чем кастодиальные данные, к тому же их у компаний более чем в полтора раза больше по объему и именно на них в основном нацелены похитители. В то же время, как показали опросы, затраты на защиту и тех и других делятся примерно поровну.

Компаниям также следует обратить внимание на то, что инцидент, связанный с кражей информации, "стоит" в десять раз дороже, чем инцидент, произошедший из-за случайной утраты данных, — сотни тысяч долларов против десятков тысяч. Важно учесть, что средние и малые компании злоумышленники атакуют гораздо (в разы) реже, чем крупные, ценность информации которых к тому же эксперты оценивают как примерно в двадцать раз более высокую, чем у небольших.

Аналитики утверждают, что за последние пять лет соответствие всевозможным законодательным требованиям, отраслевым стандартам (таким, как PCI DSS), существующим стандартам политик ИБ превратилось в основной движитель защиты информации. "Соответствие" съедает сегодня в среднем 39% корпоративного ИБ-бюджета (см. рис.). С этим согласны приблизительно 90% респондентов. При этом, как считают исследователи из Forrester Consulting, инвестиции, выделяемые для обеспечения такого соответствия, слишком завышены, а корпоративные секреты остаются в компаниях недооцененными и недозащищенными. Организации тратят большие средства на обеспечение соответствия регулятивным требованиям и защиту от случайных утечек связанной с этим информации, но в то же время недостаточно защищают от утечек другие, более ценные корпоративные данные, в том числе представляющие корпоративные секреты.

Аналитики из Forrester Consulting пришли к выводу, что затраты на обеспечение защиты в принявших участие в исследовании компаниях несоразмерны ценности защищаемой информации. Около 90% респондентов согласились, что главная цель их программ по безопасности — обеспечить соответствие отраслевым требованиям (таким, как PCI DSS), законам о соблюдении конфиденциальности информации и недопустимости ее неправомерного использования, а также стандартным подходам в политиках обеспечения безопасности данных.

"Компании тратят деньги, чтобы защитить информацию о клиентах, их медицинские данные и сведения об их кредитных картах... Так и должно быть. Однако им следует уделять больше внимания защите своей интеллектуальной собственности и информации, которая имеет для них первостепенное значение, потому что утрата интеллектуальной собственности может привести к долговременной потере конкурентных преимуществ", — считает Сэм Карри, техниче-

"Внедрению экономичных ИБ-решений мешает неготовность ИТ-инфраструктуры"

Утечки данных стали приоритетной проблемой в обеспечении информационной безопасности (ИБ). Конечные точки сети — одно из критически важных мест, через которые могут "протекать" данные. О своем видении этой проблемы научному редактору PC Week/RE ***Валерию Васильеву*** *рассказывает менеджер по маркетингу продуктов информационной безопасности российского офиса Microsoft* ***Максим Скида****.*

ИНТЕРВЬЮ

Максим Скида

PC Week: Какое место в иерархии корпоративной ИБ занимает защита конечных точек?

МАКСИМ СКИДА: Прежде чем говорить об иерархии в системе ИБ каждой компании, следует классифицировать обрабатываемую в компании информацию, выделить ту, которая нуждается в защите, и если она обрабатывается или хранится в конечных точках корпоративной сети, то защищать ее нужно и там.

Как показывает опыт, практически на каждом рабочем месте есть данные, которые требуют той или иной степени защиты. Но даже если сотрудник на своем рабочем месте не имеет дела с такими данными, защищать точку его подключения к корпоративной сети все равно нужно, для того чтобы она не оказалась уязвимым звеном, дающим возможности для атак на те информационные ресурсы, в которых есть критически важная информация. Поэтому защита конечных точек — дело необходимое. А вот определять очередность внедрения тех или иных решений при построении системы защиты данных нужно исходя из конкретной модели угроз для каждой компании.

К примеру, если сотрудникам разрешено свободное посещение Интернета, использование съемных носителей, администрирование своих рабочих компьютеров, то точки их подключения к сети будут представлять собой высокую опасность и их защита становится высокоприоритетной задачей. Если же в компании действуют строгие регламенты для использования мобильных устройств связи, внешних накопителей, доступа в Интернет, управления компьютером на рабочем месте, то приоритет защиты конечных точек снижается и фокус смещается на защиту периметра корпоративной сети, хранилищ данных и других ресурсов. Таким образом, если мы хотим понизить приоритет защиты конечных точек, нужно должным образом выстроить бизнес-процессы и отразить это в модели угроз.

PC Week: Каков, по вашему мнению, взвешенный функциональный набор для защиты конечных точек?

M. C.: Прежде всего — управление доступом пользователей к конечным точкам, четкие регламенты, определяющие методы аутентификации, сложности паролей, периоды их изменений, а также управление обновлениями ПО. Это необходимый минимум. Далее в наращивании функционала нужно исходить из модели угроз. Так, персональный антивирус и межсетевой экран нужны в конечной точке лишь тогда, когда информация на нее может попадать по каналам, не контролируемым другими средствами защиты. Если же конечная точка работает в терминальном режиме, взаимодействуя только с внутренними серверами, маршрутизаторами, межсетевыми экранами и т. п., ее не нужно защищать локальным антивирусом.

Эффективны решения, централизованно контролирующие поведение рабочих станций. Они позволяют обнаруживать как несанкционированные действия пользователей, так и проникновение вредоносных программ с конечных точек при соблюдении пользователями жестких рабочих регламентов безопасности, например заражение компьютера, изъятого из корпоративной сети на время сервисного обслуживания в сторонней организации. Для защиты критически важных данных, размещаемых на пользовательских рабочих станциях, следует также использовать шифрование.

PC Week: А можно ли говорить о "типовом портрете" заказчика решения для защиты конечных точек?

M. C.: Для определения такого заказчика можно использовать концепцию развития и оптимизации ИТ-инфраструктуры Core Infrastructure Optimization Model, которая была разработана с участием таких ведущих аналитических компаний, как IDC и Gartner. Эта концепция позволяет оценить состояние и уровень интеграции корпоративных ИТ, определить зрелость ИТ-инфраструктуры компании и отнести ее к одному из предлагаемых моделью уровней, начиная от базового и заканчивая динамическим.

Компании с базовым уровнем состояния ИТ можно отнести к заказчикам с низкой организацией ИТ — у них довольно пестрый состав операционных систем (ОС), прикладных программ, систем хранения данных и нет централизованного управления ИТ-ресурсами. Они нуждаются в защите данных на всех уровнях, и конечные точки должны быть защищены по максимуму, используя персональные антивирусы, межсетевые экраны, шифрование...

PC Week: Есть ли у компаний с базовым уровнем состояния ИТ-инфраструктуры возможность сэкономить на защите конечных точек?

M. C.: Основным препятствием к внедрению экономичных решений является неготовность ИТ-инфраструктуры заказчика. Таким компаниям нужно начинать с ее оптимизации, чтобы перевести ее на более высокий уровень. Нельзя сэкономить на ИБ без повышения структурированности и управляемости ИТ-инфраструктуры.

PC Week: Чем предложения Microsoft для защиты конечных точек отличаются от предложений конкурентов?

M. C.: В защите конечных точек Microsoft реализует комплексный платформенный подход, отличный от того, что предлагает большинство других разработчиков. В ОС и серверы приложений компании Microsoft уже внедрены технологии, позволяющие защищать конечные точки от различного вида угроз. Например, в наших ОС есть технологии шифрования данных, которые являются частью платформы, а не наложенным решением, как у конкурентов. На той же платформенной основе Microsoft предлагает своим клиентам решать задачи идентификации и аутентификации пользователей, управления правами их доступа, политиками использования приложений и т. п.

Чтобы контролировать выполнение корпоративных ИБ-политик при подключении конечных точек, Microsoft реализовала технологию Network Access Protection. Другая технология, Application Locker, позволяет управлять установкой и использованием приложений в конечных точках. В рамках платформы Microsoft работает также технология контроля учетных записей пользователей (UAC), исключающая доступ к ресурсам администрирования системы тем приложениям, которые запущены неуполномоченными пользователями. При защите конечных точек можно использовать технологии корпоративного управления ИТ-инфраструктурой Microsoft System Center Operation Manager и System Center Configuration Manager, позволяющие администраторам централизованно управлять в том числе и антивирусной защитой.

PC Week: Какие перемены в защите конечных точек вы отмечаете сегодня?

M. C.: При разработке продуктов вендорам следует учитывать, что в изменившихся экономических условиях заказчики остро реагируют на стоимость сопровождения решений. Например, Microsoft, развивая семейство Forefront, для снижения затрат на администрирование старается обеспечить максимальную преемственность по базовым технологиям, чтобы не заставлять специалистов переучиваться.

Возросло влияние на защиту конечных точек со стороны отраслевых и государственных регуляторов. Напомню, что Microsoft начиная с 2002 г. следует стратегии соответствия национальным законодательствам тех стран, в которых она развивает свой бизнес. Россия не является исключением: наши продукты, относящиеся к ИБ, проходят запланированную сертификацию во ФСТЭК и ФСБ России.

Разумеется, в защите конечных точек ИБ-вендоры учитывают и современное состояние киберугроз, поэтому в нашем межсетевом экране, выпущенном в декабре 2009 г., реализована новая технология Microsoft Network Inspection System. Она позволяет работать на опережение киберпреступников, защищая ИТ-ресурсы компаний от атак нулевого дня. Если в ИТ-инфраструктуре компании есть ПО с выявленной "дырой", а установить "заплатку" по каким-либо причинам невозможно или нежелательно, то новая технология в точках подключения корпоративной сети к внешним сетям (включая Интернет) позволяет обнаруживать и вырезать из входящих сетевых пакетов коды, атакующие установленную уязвимость. Распространив (планируется сделать это в этом году) данную технологию на уровень защиты конечных точек, в клиентскую часть Forefront, мы обеспечим блокировку угроз, нацеленных на конкретные рабочие станции, а также угроз, исходящих от зараженных компьютеров внутри корпоративной сети.

Перемещая приложения и данные в облака, заказчики хотят быть уверены, что и там с ИБ дела обстоят не хуже, чем внутри корпоративного периметра. Для защиты конечных точек в облачных вычислениях используются известные, проверенные технологии, зато немало организационных проблем. Заказчики требуют, чтобы провайдеры облачных услуг заключали соглашения с четко прописанным уровнем защиты данных, с юридически закрепленными гарантиями его обеспечения. Развитие идет в этом направлении.

Что касается нашей страны, то, как показывает опыт, распространение облачных технологий сильно тормозит психологическая неготовность отечественных заказчиков к тому, чтобы доверять обработку критической информации третьей стороне.

PC Week: Благодарю за беседу.

ский директор и директор по маркетингу компании RSA, подразделения систем безопасности в составе EMC.

Примерно 58% респондентов рассматривают инциденты, связанные с пользовательскими оплошностями (хищения и потери пользовательских устройств, ошибочные отправки информации по почте), как самые многочисленные. В то же время последствия таких инцидентов для компаний существенно менее разрушительны, нежели последствия остальных, которых заметно меньше (такие, например, как злонамеренные действия инсайдеров и внешних вредителей). Так, один акт мошенничества ИТ-администратора стоит компании в среднем 452 тыс. долл., в то время как потеря пользователем ноутбука — "всего лишь" 26 335 долл., хотя последние и случаются чаще.

Forrester предлагает компаниям руководствоваться представленными ею данными и защищаться не только от более частых, но менее разрушительных инцидентов, но и от менее частых, однако более дорогостоящих. В качестве эффективных средств борьбы с инсайдерскими угрозами эксперты предлагают полное шифрование данных на жестких дисках ноутбуков, DLP-системы, политики обнаружения защищаемой информации (например, о состоянии здоровья клиентов и их персональных идентификаторах), программные средства контроля за устройствами.

Подавляющее большинство ИБ-руководителей участвовавших в опросе компаний (95%) заявили, что знают, где хранится, откуда и куда передается важная корпоративная информация. В Forrester считают это явным преувеличением, ссылаясь в том числе и на то, что этого мнения придерживаются "безопасники" как крупных, так и небольших фирм, хотя данные исследования показывают, что в крупных компаниях инциденты случаются в четыре раза чаще, чем в небольших, и обходятся они примерно вдвое дороже.

Для исправления выявленной ситуации эксперты из Forrester, Microsoft и RSA предложили ряд рекомендаций, которые могут помочь организациям сбалансировать программы по обеспечению безопасности. Прежде всего им следует выделить у себя самые ценные информационные активы. Затем нужно создать перечень рисков, разделив их на те, что связаны с потерей: а) конфиденциальной и б) кастодиальной информации; оценить и сбалансировать затраты на обеспечение соответствия регулятивным требованиям и затраты на защиту корпоративной конфиденциальной информации. Эксперты рекомендуют быть более бдительными во внешних информационных обменах, в том числе с партнерами, и обязательно оценивать эффективность своих программ по защите данных. Руководствуясь этими рекомендациями, российские компании могут внести поправки в процесс подготовки своих ИБ-систем, с тем чтобы они соответствовали требованиям регуляторов.

Финальная версия MS Project 2010 появится в мае

ВЛАДИМИР МИТИН

Можно без преувеличения сказать, что система управления проектами (СУП) Microsoft Project (MS Project) — самая массовая в мире*. Генеральный менеджер Microsoft по продуктам семейства MS Project Людовик Хаудук утверждает, что к настоящему времени в разных уголках нашей планеты насчитывается примерно 20 млн. пользователей различных вариантов этой СУП. При этом серверные редакции данного продукта взяли на вооружение свыше 10 тыс. предприятий и учреждений. Аналогичная статистика по отдельным странам (в том числе России) традиционно не разглашается, но, по мнению специалиста по бизнес-решениям департамента по работе с крупными организациями и партнерами московского представительства Microsoft Максима Войцеховского, в нашей стране тот или иной вариант MS Project можно найти практически в каждой компании, насчитывающей свыше 100 автоматизированных рабочих мест.

УПРАВЛЕНИЕ ПРОЕКТАМИ

В нынешнем тысячелетии основных событий в жизни данного продукта три: выход семейств MS Project 2003, 2007 и 2010 соответственно. Общедоступное бета-тестирование MS Project 2010 и ряда других продуктов Microsoft с индексом 2010 идет с ноября 2009-го, а финальная коммерческая версия этого продукта (в том числе его русскоязычный вариант) должна появиться в мае.

Авторы продукта выделяют четыре главные особенности MS Project 2010:

- объединенное управление проектами и портфелями проектов;
- простой и интуитивно понятный пользовательский интерфейс;
- расширенные возможности совместной работы по созданию и ведению проектов;
- масштабируемая 64-разрядная платформа Project Server.

Первая из них основана том, что если раньше существовали два серверных продукта — MS Project Server 2007 (для управления проектами) и MS Project Portfolio Server 2007 (для управления портфелями проектов), то MS Project Server 2010 объединяет оба эти продукта. Предполагается, что стоимость MS Project 2010 будет несколько выше стоимости MS Project 2007, так как новый продукт имеет более широкий функционал, чем его предшественник (повышение универсальности продуктов — общая стратегия Microsoft).

Расширенные возможности совместной работы по созданию и ведению проектов обеспечиваются глубокой интеграцией MS Project Server 2010 с платформой Microsoft SharePoint Server 2010, что позволяет строить решения с поддержкой согласований, касающихся изменений сроков работ и ресурсов, выделенных для них.

Среди других особенностей MS Project 2010 стоит отметить функцию редактирования проектов через Интернет; улучшенный контроль за бизнес-процессами, который можно оптимизировать с помощью гибких настроек; простоту разбивки проекта на подпроекты, улучшенное управление ресурсами, мощные инструменты отчетности и бизнес-аналитики; возможность добавления новых видов графиков для слежения за ходом проекта, средства определения приоритетов в рамках портфеля проектов и т. д.

Новый продукт, как и его предшественник, будет выпускаться в трех редакциях: MS Project Standart 2010 (персональная программа для автономной работы пользователя), MS Project Professional 2010 (решение, допускающее взаимодействие пользователя с серверной частью пакета) и MS Project Server 2010 (реализация различных серверных функций). Целевая аудитория каждой из этих редакций приведена в таблице. Там же перечислены ключевые особенности этих редакций (в сравнении с аналогичными редакциями семейства MS Project 2007) и так называемые главные зависимости, т. е. сведения о программных продуктах, которые могут работать в связке с соответствующей редакцией программы.

Следует также отметить, что существует комплексное решение Microsoft Office Enterprise Project Management Solution (EPM 2007). Оно построено на базе нескольких продуктов Microsoft: MS Office Project Server 2007, MS Office Project Professional 2007, MS Office Project Web Access 2007, MS Office Project Portfolio Server 2007 и Microsoft Office Project Portfolio Web Access 2007.

В нашей стране освоение MS Project 2010 уже идет. "Мы первые в Восточной Европе сделали пилотное внедрение на MS Project Server 2010 и уже получили некоторый опыт работы с этим интересным продуктом, — отметил руководитель отдела развития и управления проектами ЗАО "Национальная спутниковая компания" Дмитрий Соколов. — В нем нас привлекает возможность редактировать проекты через Web-интерфейс вне зависимости от физического местоположения пользователя. В клиентском приложении Project Professional 2010 среди прочих улучшений довольно интересны визуальные средства оптимизации графиков загрузки инженеров".

"Microsoft Project 2010 — это решение принципиально нового уровня и возможностей, — считает генеральный директор компании PM Consulting Services Владимир Иванов. — Важнейшее улучшение — это мощная интеграция с Microsoft SharePoint Server 2010, позволяющая строить решения с поддержкой согласований изменений по срокам и ресурсам. Очень приятно и ценно, что при разработке и тестировании данного продукта Microsoft прислушивалась к мнению экспертов из России. На мой взгляд, совместная работа по обеспечению повышенной надежности этого решения позволит начать его внедрение, не ожидая пакета Service Pack 1".

По оценкам PM Expert, около 76% компаний, использующих системы управления проектами, осваивают их самостоятельно. Остальные обращаются за помощью в консалтингово-интеграторские фирмы. Одна из них — группа "Проектная ПРАКТИКА". По словам директора по маркетингу этой группы Виталия Талдыкина, среди ее клиентов насчитывается свыше 500 компаний, применяющих продукт MS Project: "Большинство из них пришло к нам с целью как можно быстрее освоить все возможности платформы Microsoft EPM для решения стоящих перед ними конкретных задач".

Не подкосит ли улучшение пользовательского интерфейса (читай — облегчение процесса освоения и эксплуатации продукта) бизнес тех партнеров Microsoft, которые заняты обучением и консультированием заказчиков. "Не подкосит, — считает Максим Войцеховский. — Улучшение интерфейса идет параллельно с расширением функциональности продукта. Отсюда — его неизбежное "утяжеление". Поэтому роль консалтинговой составляющей в бизнесе наших партнеров не уменьшится".

Средства повышения эффективности управления проектами (как уникальными, так и типовыми) — это хорошо. Другой вопрос — какова стоимость владения этими средствами (включая расходы на обучение персонала и настройку системы под требования заказчика)? Похоже, многих она отпугивает. Интересно отметить, что на состоявшейся в марте в московском офисе Microsoft конференции по управлению проектами многие выступающие, ссылаясь на итоги различных опросов, неоднократно говорили, что в настоящее время главным конкурентом MS Project является табличный процессор Excel, с помощью которого также можно получать всевозможные красивые графики. Разумеется, при этом речь идет о проектах, руководители которых контролируют не так много работ. Во всяком случае не десятки тысяч. И даже не тысячи.

*О некоторых других СУП и особенностях их практического использования рассказывалось в PC Week/RE, № 23/2008.

Целевая аудитория MS Project 2010

MICROSOFT PROJECT 2010	MS PROJECT STANDARD 2010	MS PROJECT PROFESSIONAL 2010	MICROSOFT PROJECT SERVER 2010
Целевая аудитория	Отдельные пользователи и руководители проектов с частичной занятостью	Профессиональные руководители проектов	Директора по ИТ, руководители проектов, операционные отделы, отделы исследований и разработок, отделы разработки продуктов
Ключевые изменения	Пользовательский интерфейс типа Microsoft Office Fluent Планирование пользователями Представление временной шкалой	Project Standart+ Улучшенные возможности составления расписаний Планировщик работы группы Синхронизация Project с SharePoint	Веб-планирование Объединенное управление проектами и портфелями Улучшенные возможности бизнес-аналитики и отчетности
Клиентские лицензии	Клиентские лицензии не требуются	Клиентская лицензия Project Server включена	Клиентские лицензии требуются
Главные зависимости	Windows XP, Vista или Windows 7	Windows XP, Vista или Windows 7	SharePoint Server 2010 SharePoint Enterprise CAL 64-разрядная ОС Windows Server 2008.

Источник: *Microsoft*

"Аскон"...

◀ ПРОДОЛЖЕНИЕ СО С. 6

бы избежать натурных испытаний, это уже большое дело, — пояснил Евгений Бахин. — В связи с улучшением каналов связи упрощается работа распределенных коллективов. Виртуальные КБ будут развиваться".

Кроме того, для сегмента САПР актуальны общие тенденции ИТ-рынка, такие как мультиплатформенность, веб-ориентированность, облачные вычисления, удобство и простота интерфейса, поддержка сенсорного 3D-экрана, движение в сторону Open Source и Linux.

Важным результатом прошлого года стало увеличение объёма контролируемой государством экономики примерно до 50%. Поэтому возросло влияние госзаказа. Как отметил директор по маркетингу Дмитрий Оснач, в связи с увеличением влияния госзаказа компания переориентировала сбыт на те отрасли, которые получают бюджетное финансирование: "В прошлом году оборонка была нашим основным заказчиком. Раньше эту роль играло обычное машиностроение, однако в 2009-м объем продаж здесь сократился на 35%, а в оборонке на 14% вырос, и благодаря государственным инвестициям в образование поставки ПО в учебные учреждения увеличились на 70%".

Предполагается, что в этом году высокая доля присутствия государства в экономике сохранится, в основных отраслях "Аскона" — машиностроении, строительной промышленности — начнется незначительный рост, а в нефтегазовой, энергетической, металлургической, атомной индустрии и ОПК будет наблюдаться более существенный подъем. Поэтому компания делает упор именно на этих отраслях.

Так, для работы с предприятиями ОПК компания недавно получила сертификаты ФСТЭК для систем КОМПАС-3D и ЛОЦМАН:PLM. "Этот шаг направлен на привлечение новых клиентов, — объяснил Дмитрий Оснач. — Зарубежным компаниям сложно пройти сертификацию, потому что для этого нужно открывать исходные коды, и к тому же многие из них не имеют права поставлять ПО на предприятия, которые производят технику оборонного значения".

Для строительной отрасли создан новый продукт КОМПАС-СПДС. Отчасти его выпуск был вызван ростом конкуренции на рынке САПР, объем которого сократился, а число игроков не изменилось. "Мы ожидали роста спроса на клоны AutoCAD'а и в качестве ответной меры выпустили систему начального уровня КОМПАС-СПДС", — сказал г-н Оснач.

Для удовлетворения спроса на тесное взаимодействие конструкторских и расчетных систем "Аскон" реализует интеграцию КОМПАС-3D с WinMachine компании НТЦ АПМ. "Вскоре выйдет специальная версия WinMachine, которая работает в оболочке КОМПАСа", — пообещал Максим Богданов.

Что касается остальных продуктов, то компания продолжает их развитие и представила план выпуска очередных версий на этот год.

В стратегическом направлении "Аскон" собирается воспользоваться тем, что она одновременно является и разработчиком, и интегратором (внедрением проектов занимаются ее многочисленные подразделения по всей территории России). "В отличие от обычного вендора мы имеем прямой выход на заказчиков, можем узнавать их потребности и работать над удовлетворением этих запросов", — сказал Максим Богданов.

В компании надеются, что такая политика принесет плоды, и планируют вернуть оборот на уровень 2008 г. в 2012-м или даже раньше.

Как BPM может помочь в разработке приложений

ЭНДРЮ ХУЛЛ

Недавно Gartner перечислила основные проблемы, с которыми столкнулись CEO в 2009 г. Первая в списке — сокращение персонала и реструктуризация компании. Вторая связана с необходимостью "ограничить деятельность задачами, решение которых обеспечит выживание компании в краткосрочной перспективе, но при этом не убить ее будущее". Насколько хорошо ваш ИТ-департамент сработает, когда придет время перекраивать бюджет? Это можно предсказать по вашим ответам на два следующих вопроса.

МЕТОДОЛОГИЯ

1. Разрабатывает ли ИТ-департамент решения, которые являются критически важными для достижения стратегических целей компании?

2. Насколько оперативно бизнес-пользователи могут извлечь реальную пользу из этих решений? Способны ли вы достаточно быстро реагировать на ситуацию, чтобы помочь бизнесу в решении тактических задач?

Если, отвечая на эти вопросы, вы понимаете, что у вас здесь есть реальные проблемы, есть смысл прочитать данный материал, в котором мы познакомим вас с методологией их решения с помощью BPM (Business Process Management, управление бизнес-процессами) — технологии, позволяющей, как показывает опыт, уже в первый год ее применения снизить издержки на 20%. Именно эта технология является приоритетом номер один для CEO в 2009 г. BPM дает возможность сконцентрироваться на стратегически важных для компании процессах и помогает бизнес-руководителям найти правильные решения максимально быстро.

Традиционный подход

Традиционно ИТ-проекты начинаются с того, что бизнес-аналитики, отнимая время у бизнес-пользователей, выясняют все детали, необходимые для создания приложения. В итоге спустя несколько месяцев они вырабатывают объемный документ с постановкой задачи для разработчиков. Последние переводят изложенные в документе требования на свой язык и приступают к созданию приложения. К сожалению, представители бизнес-подразделений не участвуют в этом процессе вплоть до окончательного выпуска приложения.

Когда по прошествии месяцев (а порой и лет) оно будет готово к выпуску, вам останется только "скрестить пальцы" в надежде, что процесс, который был подробно описан в наборе требований, все еще поддерживается в компании и сохраняет свою актуальность. Но и до, и после выпуска приложения любые изменения требований к нему со стороны бизнес-пользователей вызывают раздражение у сотрудников ИТ-департамента, поскольку эти изменения всегда выходят за рамки ранее согласованного документа.

BPM-подход

Подход, основанный на BPM, предполагает постоянное сотрудничество ИТ-департамента с бизнес-подразделениями, а также максимально оперативное и эффективное реагирование на их нужды. При таком подходе ИТ-проект начинается не со сбора и согласования требований к новому приложению, а с выяснения и детализации того, что, собственно, бизнес-пользователи, владельцы компании и другие участники бизнес-процессов хотят получить.

Разобравшись в этом, заинтересованные лица могут сформировать предложения по тем процессам, которые непосредственно связаны со стратегическими бизнес-целями компании, утвержденными ее высшим руководством.

После этого аналитики и разработчики совместно начинают работу над наиболее важными процессами из предложенного им списка. При этом разработчики представляют свои наработки бизнес-пользователям каждые 4—6 недель, чтобы быть уверенными в том, что идущий процесс соответствует ожиданиям последних. После того как в приложении реализован минимально необходимый функционал, бизнес-подразделения могут начинать его эксплуатацию, по мере которой возможности приложения наращивают.

Работа в команде

При таком подходе бизнес-пользователи и ИТ-департамент, вместо того чтобы отсылать друг друга к согласованному когда-то документу и тыкать в подписи под техническим заданием, трудятся как одна команда, заинтересованная в том, чтобы разработанное ею приложение было максимально эффективным для компании. Любые изменения ожидаются и приветствуются. По ходу разработки уже написанный код можно проверить с использованием реальных накопленных данных и программ моделирования, а также оптимизировать с помощью предназначенных для этого инструментов.

В рамках такого сотрудничества ИТ-департамент может быстро оказывать эффективную помощью бизнес-подразделениям на постоянной основе. Углубленное изучение того или иного процесса и участие в его совершенствовании на начальной стадии проекта существенно упрощают для бизнес-пользователей этап внедрения готового приложения. Каждая его новая версия несет бизнесу дополнительные возможности.

Преимущества BPM-подхода

Совсем недавно преимущества BPM-подхода к ИТ-проектам в полной мере оценили в одной финансовой компании, за короткое время внедрившей несколько бизнес-процессов. Началось все с того, что в ИТ-департамент был направлен перечень требующих автоматизации бизнес-процессов. Затем аналитики проинтервьюировали руководителей бизнес-подразделений, чтобы понять основные проблемы, с которыми сталкивается компания. Среди таковых был и широкий набор нормативных требований, которым компания удовлетворяла далеко не в полной мере. Удовлетворение этих требований стало первоочередной задачей для ИТ-департамента. Поэтому бизнес-процессам, имеющим к этой задаче непосредственное отношение, был отдан высший приоритет.

После этого сотрудники ИТ-департамента провели несколько встреч с бизнес-пользователями, чтобы разобраться в том, что представляют собой данные бизнес-процессы на текущий момент. В ходе этих встреч аналитики использовали специальные коллективные инструменты для описания модели обсуждаемого процесса. Участники, по-разному понимавшие один и тот же процесс, могли изобразить его так, как они его видят, а потом после ряда обсуждений выработать единую точку зрения.

Из таких встреч бизнес-пользователи выносили идеи относительно того, что нужно сделать для решения имеющихся проблем. И при этом они отчетливо понимали, что ИТ-департамент работает на них и новые процессы будут вскоре внедрены.

Затем аналитики обсудили схемы процессов и перечни предлагаемых доработок с разработчиками, чтобы уточнить масштаб работ по каждому из этих процессов, и совместно составили план выпуска версий приложений с указанием реализуемого в них функционала.

Уже через пять недель после начала работ по проекту бизнес-пользователи смогли опробовать работающий прототип приложения, функционал которого формировался в соответствии с их нуждами. По мере выпуска очередных версий они направляли в ИТ-департамент свои замечания по их функционированию и предложения по внесению изменений в процесс. Поскольку сотрудничество уже было налажено и цели бизнес-подразделений и ИТ-департамента согласованы, у разработчиков это не вызывало негативной реакции.

Заключение

Применив BPM-подход, ИТ-департамент смог за полгода внедрить четыре бизнес-процесса, успешно решив проблему обеспечения соответствия компании нормативным требованиям.

Итак, в свете приведенного примера, как вы думаете, какой подход более целесообразен в нынешние нелегкие времена, когда ресурсы компаний ограниченны?

Как оптимизировать производительность межсетевого экрана

РУВЕН ХАРРИСОН

Не перегружен ли ваш межсетевой экран? Симптомы этого — высокая загрузка ЦП, низкая пропускная способность брандмауэра и медленная работа приложений. Прежде чем модернизировать оборудование, стоит подумать, нельзя ли оптимизировать конфигурацию брандмауэра.

Приведенные рекомендации помогут администраторам максимально оптимизировать работу межсетевых экранов.

Метод № 1. Добейтесь того, чтобы исходящий трафик соответствовал политикам

Устраните несанкционированный или нежелательный трафик в сети. Уведомите администраторов о серверах, перегружающих брандмауэр прямыми исходящими запросами DNS, NTP, SMTP, HTTP и HTTPS, которые были отвергнуты, а также отмененными/отвергнутыми запросами внутренних устройств. Администраторы должны переконфигурировать серверы, чтобы те не генерировали неразрешенный исходящий трафик (что снимет лишнюю нагрузку с брандмауэра).

Метод № 2. Фильтруйте нежелательный трафик на маршрутизаторе(ах), а не брандмауэре

Переместите правила фильтрации нежелательного входящего трафика с брандмауэра на маршрутизатор(ы) периметра, сбалансировав производительность и эффективность политики безопасности. Для этого сначала выявите самые частые входящие запросы, которые были отвергнуты, и переместите их выше по сети, на маршрутизатор, в стандартный список управления доступом (ACL). Это может потребовать времени, но это хороший способ, который снимет часть нагрузки с ЦП брандмауэра и освободит его память.

Затем, если у вас есть внутренний дроссельный маршрутизатор между сетью и межсетевым экраном, можно переместить блоки обычного исходящего трафика на него. Это снимет еще часть нагрузки с брандмауэра.

Метод № 3. Удалите неиспользуемые правила и объекты

Удалите неиспользуемые правила и объекты из громоздких баз правил. Очистка баз правил может показаться опасным занятием, но на рынке есть множество утилит, которые помогут в этом деле. Благодаря им управление политиками брандмауэра становится гораздо менее трудоемким.

Метод № 4. Упростите базы правил

По возможности упростите базы правил и сведите к минимуму взаимное перекрытие правил. Опять-таки, есть автоматические средства, которые могут значительно уменьшить затраты времени и сил на очистку и упрощение баз правил.

Метод № 5. Ограничьте широковещательный трафик

Если интерфейс межсетевого экрана подключен напрямую к сегменту локальной сети, то следует создать правило для широковещательного трафика (bootp, NetBIOS через TCP/IP и т. п.) без занесения в журнал.

Метод № 6. Поместите наиболее часто используемые правила в верхнюю часть перечня правил

Наиболее часто используемые правила лучше разместить в верхней части перечня правил. Но имейте в виду, что производительность некоторых межсетевых экранов (в частности, Cisco Pix, ASA версии 7.0 и выше, FWSM 4.0 и определенных моделей Juniper Networks) не зависит от порядка правил, так как они используют оптимизированные алгоритмы контроля пакетов.

Метод № 7. Избегайте DNS-объектов

Избегайте объектов, требующих просмотра DNS.

Метод № 8. Настройки интерфейса брандмауэра должны соответствовать настройкам коммутатора и маршрутизатора

Интерфейсы вашего брандмауэра должны соответствовать интерфейсам маршрутизатора и/или коммутатора. Если у маршрутизатора или коммутатора 100-Мбит/с полудуплекс, то и у брандмауэра должно быть то же самое. Интерфейсы обязательно должны соответствовать один другому, и скорее всего, это будет 100 Мбит/с-дуплексный интерфейс.

Ваши маршрутизатор/коммутатор и межсетевой экран должны показывать одну и ту же скорость и один и тот же режим связи. Если и коммутатор, и брандмауэр имеют интерфейс Gigabit Ethernet, то они оба должны быть настроены на автосогласование скорости и дуплексного режима. Если Gigabit-интерфейсы брандмауэра и коммутатора не соответствуют друг другу, то следует попробовать заменить кабели и порты коммутационной панели. Если Gigabit-интерфейсы не связываются на скорости 100 Мбит/с в дуплексном режиме, то это почти всегда признак других проблем.

Метод № 9. Отделите брандмауэры от VPN

Отделите брандмауэры от VPN, чтобы им не нужно было обрабатывать VPN-трафик.

Метод № 10. Снимите с брандмауэра лишнюю нагрузку

Выгрузите с брандмауэра функции единой защиты от угроз (UTM), в том числе антивирус, защиту от спама, блокирование вторжений (IPS) и сканирование URL.

Метод № 11. Перейдите на последнюю версию ПО

Как правило, новые версии ПО дорабатываются с целью повышения скорости функционирования. Однако в них могут быть добавлены и новые функции, так что общий рост производительности не гарантирован.

Весна 2010: киберпреступность и киберзащита

ВАЛЕРИЙ ВАСИЛЬЕВ

ОБЗОРЫ

О коммерциализации и организованности действий киберпреступников СМИ говорят на протяжении уже нескольких лет. Ныне даже в ходу термин "рынок киберпреступности". Так, Денис Батранков, консультант корпорации IBM по ИБ в регионе Восточной Европы, Азии и России, ссылаясь на отчеты команды экспертов из X-Force, сообщил, что киберпреступники используют те же технологии ведения своего бизнеса, что и легальные предприниматели. Они, например, тоже переходят на облачные вычисления. Через Интернет сегодня можно заказать киберкриминальные услуги с разными уровнями и стоимостью поддержки, с регулярными дистанционными обновлениями задействованного в услугах ПО. Часто прибегая к целевым атакам, хакеры активно используют средства технической и экономической разведки, внимательно и продолжительно, порой по нескольку месяцев, изучают средства защиты жертвы, выявляют слабые места, планируют возможную выручку.

Киберпреступники активно легализуют свой бизнес, выводя на рынок ботнет-услуг серые схемы. Примером могут служить так называемые "партнерские программы", позволяющие владельцам ботнетов "монетизировать" свою работу, не заставляя "партнеров" непосредственно выполнять услуги явно криминального характера (такие как рассылка спама, DoS-атаки, распространение вирусов...).

Как следует из отчета компании McAfee о киберугрозах, в последнем квартале прошлого года по числу заново подвергшихся зомбированию компьютеров лидировали США (15,7%), за ними следовали Китай (9,3%) и Бразилия (8,2%). Россия на "почетном" четвертом месте — 5,6%. Самыми активными, согласно данным "Лаборатории Касперского", в 2009 г. оказались китайские хакеры: на их долю пришлось почти 53% всех кибератак, и вместе с тем сам Китай стал главной целью международных атак. По-видимому, бурно развивающиеся экономика и ИТ-инфраструктура этой страны представляют для преступников двойной интерес: как место проживания перспективных кибержертв и как площадка для создания бот-сетей для новых атак .

Эксперты говорят, что вредоносные программы, распространяющиеся через социальные сети и приложения Web 2.0, становятся большой проблемой для ИБ.

По словам Бориса Мирошникова, начальника бюро специальных технических мероприятий МВД России, среди зарегистрированных киберпреступлений в нашей стране в прошлом году преобладали неправомерный доступ к компьютерной информации (54%), создание и распространение вредоносных программ (12%) и мошенничество (6%).

Киберпреступность

Технологический рост. Отмечая, что темпы роста количества новых вредоносных программ в 2009 г. заметно снизились, "Лаборатория Касперского" называет одной из главных причин этого возросший уровень конкуренции на рынке киберпреступности. Вступив в конкуренцию, вирусописатели вынуждены серьезное усложнить используемые технологии. В качестве яркого примера таких перемен специалисты "Лаборатории Касперского" упоминают технологию drive-by-download, позволяющую незаметно для пользователя заражать компьютер во время обычной работы в Интернете. Зафиксированное "Лабораторией" количество атак с использованием этой технологии, исчисляемое десятками миллионов, увеличилось за 2009 г. примерно в три раза. Другим заметным технологическим явлением стали удачные атаки со стороны эксплоита Gumblar, которым подверглись десятки тысяч веб-ресурсов, приводящие к созданию автоматизированных систем самостроящихся ботнетов.

Заметно эволюционировали руткиты. Среди них эксперты выделяют такие вредоносы, как Sinowal, TDSS и Clampi. При этом отмечается, что руткит Sinowal представлял собой в 2009 г. самую продвинутую вредоносную программу, которую не обнаруживало большинство антивирусов. Вредоносная программа TDSS использовала сразу две сложные технологии: она заражала системные драйверы Windows и одновременно создавала собственную виртуальную файловую систему, в которой прятала свой основной вредоносный код. В "Лаборатории Касперского" считают, что TDSS стала первой вредоносной программой, способной внедряться в операционную систему на таком уровне.

Один инцидент, связанный с компрометацией данных, наносит банку США ущерб в 6 млн. долл.

Главной эпидемией прошлого года эксперты называют распространение червя Kido (Conficker), поразившего миллионы компьютеров во всем мире. Червь использовал несколько способов проникновения на компьютеры жертв: подбор паролей к сетевым ресурсам, флэш-накопители, уязвимости Windows MS08-067. Каждый зараженный компьютер становился частью зомби-сети. Как отмечают специалисты, в Kido тоже реализованы современные и эффективные технологии вирусописательства: он противодействует обновлению программ защиты, отключает службы безопасности, блокирует доступ к сайтам антивирусных компаний и т. д.

Уязвимости ОС и приложений. Что касается состояния безопасности ПО, то за прошедший год, согласно данным "Лаборатории Касперского", больше всего уязвимостей было обнаружено в продуктах Microsoft, Apple, Adobe и Sun. По числу уязвимостей файлов и приложений, обнаруженных на пользовательских компьютерах, самыми распространенными в 2009 г. стали уязвимости в продукте компании Apple — QuickTime 7.x. Чтобы реально оценивать уровень безопасности ПО упомянутых вендоров, определяемый качеством разработки, следовало бы учитывать распространенность этого ПО. Однако исследователи рынка ИБ такую статистику не приводят.

Согласно данным седьмого выпуска отчета Microsoft Security Intelligence Report, общее количество выявленных уникальных уязвимостей ПО в первом полугодии 2009 г. сократилось на 28% по сравнению со вторым полугодием 2008 г., число уязвимостей ОС Windows осталось приблизительно на том же уровне, а уязвимостей браузеров — немного возросло. Количество зловредов, целью которых является заражение ПО Microsoft, по сравнению с вредоносными программами, ориентированными на ПО других разработчиков, установленное на компьютерах под управлением ОС Windows Vista, составляет 16% (в то время как под ОС Windows XP — 56%).

Уязвимости мобильных платформ. Все больше внимания со стороны вирусописателей привлекают мобильные ОС. В прошлом году "Лабораторией Касперского" было обнаружено 39 новых семейств и 257 новых модификаций вредоносных программ для мобильных устройств. В том же 2009-м выявлены первые вредоносные программы (черви Ike) для iPhone, создана первая шпионская программа для Android, а также зафиксированы первые инциденты, связанные с появлением предназначенных для Symbian-смартфонов вредоносных программ, подписанных разработчиками.

Для платформ iPhone и Android "Лаборатория Касперского" прогнозирует сложный год в части ИБ, отмечая появление в 2009 г. первых угроз и для них. При этом, если для пользователей iPhone потенциальную угрозу представляют только взломанные устройства, открытые таким образом для установки ПО из любых источников, то для Android такого ограничения нет изначально. Растущая популярность телефонов на базе этой ОС в Китае и слабая технология ИБ-контроля публикуемых для них приложений могут привести в этом году к ряду крупных вирусных инцидентов.

Мошенничество в киберсреде. Разнообразными становятся схемы мошенничества в Интернете. "Лаборатория Касперского" отмечает, что российские мошенники поставили на поток создание сайтов с предложением всевозможных "услуг", количество которых исчисляется уже сотнями. Среди них такие, как предложение указать местоположение человека через GSM, предоставить доступ к чужой приватной переписке в социальных сетях, собрать информацию о частном лице или компании. Обеспечением их функционирования занимаются десятки упомянутых выше "партнерских программ". Для вовлечения в них доверчивых пользователей активно используется спам в электронной почте, в социальных сетях и сервисах мгновенного обмена сообщениями. Исследователи отмечают, что вероятность того, что пользователь социальной сети откроет предлагаемый ему "друзьями" файл или пройдет по присланной от их имени ссылке примерно в десять раз выше, чем если бы эти данные пришли к нему по электронной почте.

Псевдоантивирусы. Отмечается, что количество предложений псевдоантивирусов остается высоким. Задача мошенников, действующих по этой схеме, заключается в том, чтобы убедить пользователя в заражении его компьютера (на самом деле не существующем) и заставить человека уплатить деньги за нейтрализацию этого заражения. По оценкам ФБР США, на лжеантивирусах преступники в общей сложности заработали в 2009 г. примерно 150 млн. долл.

Web 2.0 как угроза. Эксперты компании Webroot Software, проводившие опрос ИТ-специалистов организаций США, Великобритании и Австралии, отмечают, что вредоносные программы, распространяющиеся через социальные сети и приложения Web 2.0, становятся большой проблемой для ИБ-бизнеса, особенно среднего и малого. Так, 80% респондентов считают, что вредоносы, имеющие источником Web 2.0, серьезно осложняют работу ИТ-отрасли, а 73% относят эти веб-угрозы к более приоритетным, чем атаки через электронную почту. По мнению экспертов "Лаборатории Касперского", в области веб-сервисов важной ИБ-темой нынешнего года могут стать атаки через Google Wave. Предполагается, что их развитие будет проходить по стандартной схеме: сначала рассылки спама, затем фишинг-атаки, потом использование уязвимостей.

Киберзащищенность

Важной особенностью нынешней ситуации с ИБ, как отмечают эксперты, является падение среднего уровня компьютерной грамотности пользователей вследствие возрастающей доступности компьютеров, устройств связи и Интернета во всем мире. Это в первую очередь относится к индивидуальным пользователям, хотя благоприятствует развитию киберпреступности и ведет к общему повышению уровня ИБ-рисков через развитие тех же бот-сетей.

Доли ИБ-инцидентов, связанных с потерей данных, в зависимости от типа инцидента

Источник: *Open Security Foundation, 2009 г.*

Что же касается общей картины состояния корпоративной ИБ, то, согласно данным исследований компании Webroot Software, в 88% организаций введены жесткие политики пользования Интернетом, в 69% ведут работу с персоналом по информированию об опасностях, подстерегающих пользователей в Сети, в 44% не реже раза в год рассылают соответствующие оповещения, в 56% действуют строгие запреты на посещение сайтов социальных сетей. О том, как эти меры сказываются на общемировой ситуации в 2009 г. с потерями информации, можно судить по результатам исследований ассоциации Open Security Foundation (см. диаграмму). Согласно собранным ассоциацией сведениям, основной причиной потерь данных остается кража оборудования, составляющая 30% от общего количества случаев потери данных, в то время как нарушения в системах безопасности, возникающие в результате взлома ИТ-инфраструктуры или использования вредоносных программ, составляют менее 15%.

ИБ-эксперты считают, что защищенность российских корпоративных пользователей за прошедший год повысилась. В качестве аргументов они отмечают рост внимания разработчиков к безопасному производству ПО и поиску в нем ошибок на этапе эксплуатации, увеличение количества внедрений DLP, IPS/IDS-систем, систем мониторинга и корреляции ИБ-событий, систем веб-безопасности, управления обновлениями ПО и жесткой аутентификации пользователей, переход корпоративных пользователей с антивирусных сканеров и мониторов на ИБ-комбайны, объединяющие несколько технологий многоуровневой ИБ-защиты, и, как следствие, замедление роста количества утечек данных.

Организационные меры в ИБ. Как отмечает компания InfoWatch, специалисты по ИБ сегодня излишне сконцентрированы на защите электронной информации и при этом забывают о традиционных носителях, прежде всего бумажных, а утечки данных в таком виде можно предотвратить лишь организационными мерами.

"Вера во всесилие технологий закончилась, — считает Вениамин Левцов, глава московского представительства компании Trend Micro, — теперь особое значение приобретают не столько технические средства, сколько организационные мероприятия, и существенное место в них занимает задача соответствия внешним и внутренним требованиям к ИБ. Это общемировая тенденция. Во главу угла при организации ИБ ста-

ДЖИМ РАПОЗА: 25 ЛЕТ EWEEK

Сеть изменила всё

Шестнадцать лет назад я стал работать аналитиком в лаборатории издания, которое тогда называлось PC Week. Более старшие и опытные аналитики занимались тестированием самых важных технологий того времени, таких как ПК, офисные пакеты, сети клиент/сервер и принтеры. А мне поручили обзор технологии, которая, хотя и считалась многообещающей, еще не привлекла особого внимания корпоративных ИТ-профессионалов. Что это была за технология? World Wide Web.

Для меня это было большой удачей, так как я начал работать с Сетью в момент ее зарождения. Мне также посчастливилось сотрудничать с аналитиком лаборатории *PC Week* Имонном Салливаном, пионером в области создания веб-сайтов и разработок на языке HTML. Именно он построил веб-сайт для *PC Week*, и этот еженедельник стал одним из первых веб-изданий.

Я могу с уверенностью утверждать, что World Wide Web — это самая важная технология минувшего столетия, не говоря уже о последних 25 годах. Более того, ее можно поставить в один ряд с самыми важными разработками всех времен и народов. Однако и внутри самой Сети имеется множество отдельных технологий, которые заслуживают особого внимания.

Пожалуй, самая выдающаяся из них — это браузер. В первое время Всемирная паутина хотя и вызывала интерес, но мало отличалась по возможностям от того, что обеспечивал, например, сетевой протокол Gopher. Стоило, однако, появиться браузеру Mosaic, который открыл потенциал графических возможностей веба, как поднялась мощная волна веб-разработок. Mosaic живет до сих пор — его код составляет основу не только браузеров на базе технологий Netscape и Mozilla, но и продукта Internet Explorer.

Другой важной технологией, которую также разработала компания Netscape, является протокол SSL. Все понимали, какие возможности Сеть открывает для онлайновых игр, однако корпоративный мир не проявлял к ней особого интереса до тех пор, пока не обнаружил, как с ее помощью можно зарабатывать деньги. Протокол SSL (Secure Socket Layer) позволил создавать безопасные соединения, посредством которых пользователи и предприятия могли покупать и продавать через Сеть. Без SSL были бы невозможны многочисленные виды деятельности, начиная от бизнеса компаний Amazon и eBay и кончая корпоративной электронной почтой.

Одним из самых интересных и удивительных достижений в развитии Интернета стало появление практически из ниоткуда множества новых продуктов и технологий, которые обычно создавали не крупные компании, а небольшие группы разработчиков и энтузиастов, начиная от Google и Yahoo и кончая Facebook и Twitter.

Еще один выдающийся пример последних лет — технология AJAX и графические пользовательские веб-интерфейсы. Эти новинки появились благодаря программистам, которые смогли применить имеющиеся технологии разработки и создания скриптов для построения основанных на браузерах интерфейсов с насыщенной графикой, которые стали достойными соперниками интерфейсов настольных приложений.

Это привело к резкому росту популярности веб-приложений и услуг, которые позволяют с помощью одного браузера решать почти все задачи предприятий или индивидуальных пользователей. Не за горами время, когда веб станет операционной системой, к которой вы сможете обращаться независимо от ОС, используемой в вашем устройстве.

Однако, пожалуй, наиболее важная инновационная особенность Сети остается неизменной: каждый человек может с помощью бесплатных или недорогих инструментов и сервисов создать в ней новое приложение или услугу и изменить мир.

вятся ИБ-политики, регламенты, процедуры...”

Соглашаясь с тем, что ИБ уже невозможно обеспечить одними лишь техническими средствами, Иван Мелехин, начальник отдела консалтинга компании “Информзащита”, обращает внимание на то, что и поддерживать ее только силами подразделения безопасности тоже недостаточно. “Управление информационной безопасностью является частью общей системы менеджмента организации, — говорит он. — Оно основано на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения ИБ и включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, процедуры, процессы и ресурсы. Решить задачи управления ИБ можно путем построения системы управления информационной безопасностью — СУИБ”.

Максим Скиба, менеджер по маркетингу продуктов информационной безопасности российского офиса Microsoft, отмечает, что российские компании стали внимательнее подходить к разработке политик ИБ, внутрикорпоративных регламентов, классификации информации. Вместе с тем он напоминает, что компаниям при организации ИБ также следует учитывать увеличение количества возможных сценариев работы пользователей, связанное с развитием мобильных технологий, технологий передачи голоса и видео по IP-сетям.

С активизацией регулятивной деятельности государства в области ИБ ИБ-специалистам стало, по мнению Дениса Батранкова, полезно приобретать смежную профессию юриста. “Нам приходится внимательно вникать в законы, отслеживать их изменения, на что, честно говоря, не хватает времени”, — сказал он.

ИБ-сервисы в России. Александр Гостев, руководитель центра глобальных исследований и анализа угроз “Лаборатории Касперского”, отмечает, что основным технологическим трендом ИБ-индустрии становятся облачные технологии. “Те антивирусники, что не развивают эту технологию, раньше или позднее умрут”, — полагает он.

Однако, как считает Алексей Лукацкий, менеджер по развитию бизнеса Cisco, распространение в России облаков, а вместе с тем и услуг “Безопасность как сервисы” (Security as a Services) упирается в отсутствие ЦОДов для таких сервисов и каналов связи должного качества. Он также подчеркивает, что помимо технических проблем перед российскими заказчиками остро стоит проблема доверия и что передаче обеспечения ИБ внешней организации противится психика российского ИБ-специалиста. С тем, что дело в ментальности специалистов по защите информации, согласна Юлия Грекова, глава московского представительства компании Check Point, по мнению которой никаких технологических проблем в плане защиты облаков нет, поскольку там используются уже существующие, проверенные технологические средства.

В облачных вычислениях, как заметил Александр Гостев, есть обстоятельства, смущающие не только заказчиков, но и вендоров. “Эта технология создает проблему злоупотребления интеллектуальной собственностью со стороны разработчиков антивирусной защиты. Из облака украсть вендорские антивирусные детекты гораздо проще, чем традиционные антивирусные базы и сигнатуры. Решения этой проблемы, характерной для всей ИБ-индустрии, мы пока не знаем”, — сказал он.

Кроме упомянутых причин, тормозящих развитие ИБ-сервисов, есть еще и экономические. Как показывают опросы, пользователи в любой стране мира считают, что чистый трафик — обязанность провайдера, а не дополнительная услуга, и не хотят за это платить. “Когда операторы начнут понимать, что прошла пора конкуренции за счет снижения стоимости подключения к Интернету и сервисов в виде пиратского контента, когда пользователи будут готовы платить за чистый трафик, за другие ИБ-сервисы, провайдеры начнут заниматься этим вплотную, — считает Алексей Лукацкий. — ИБ — одна из областей, на базе услуг в которой операторам можно пытаться выиграть в конкуренции, ориентируясь при этом на возврат инвестиций через три-четыре года, а не год, как они привыкли”.

Сегодня во главу угла при организации ИБ нужно ставить не технологии, а ИБ-политики, регламенты, процедуры...

Сегодня провайдеров в некоторой мере обязывают следить за содержимым трафика и вводить фильтрацию для защиты детей от негативной информации и запреты на интернет-казино. Однако к этим нормативным инициативам наряду с провайдерами должны быть готовы и пользователи. А для этого нужно вложить силы и средства в повышение осведомленности населения в области ИБ при использовании Интернета. “Пока среди провайдеров такую работу организовал только “Билайн”, среди прочих мероприятий запустивший программу “Мобильная грамотность”. У других операторов есть более денежные темы. Так, операторам, получающим 50% от стоимости каждого SMS-сообщения, невыгодно следить за их содержимым, точно так же как блокировать DDoS-атаки, поскольку они обеспечивают оплачиваемый объем трафика”, — сказал Алексей Лукацкий.

Вместе с тем, по наблюдениям экспертов, интерес к ИБ-сервисам в России есть, и в первую очередь со стороны малого бизнеса и провайдеров, работающих с домашними пользователями. Согласно прогнозам Вениамина Левцова, в этом году мы увидим рост спроса на сервис фильтрации интернет-трафика на стороне и ресурсах провайдеров с возможностью управления сервисом через веб-интрефейс на стороне заказчика. В то же время он полагает, что спрос на аналогичный сервис для корпоративного почтового трафика пока мало вероятен.

Вклад силовиков. Борис Мирошников отметил, что заметное увеличение количества преступлений в сфере ИТ, доведенных до стадии заведения уголовных дел, в сравнении с количеством зафиксированных дел (8 тыс. заведенных при 17,5 тыс. зафиксированных в 2009 г. против 5,5 тыс. заведенных при 14 тыс. зафиксированных в 2008 г.) служит показателем растущей квалификации его сотрудников, что особенно важно, поскольку, по его оценкам, киберпреступники, действующие на территории нашей страны, интеллектуальны, знают не только современные технологии, но и юридическое право (в том числе и международное), психологию, ориентируются в специфике нашей экономики. Он считает, что большие проблемы в расследовании и пресечении киберпреступлений создает анонимность пользователей в информационных сетях. “Во многих странах разработаны средства борьбы с этой глупостью [анонимностью]. К сожалению, у нас в этом направлении ничего не делается”, — посетовал он. Как свидетельствуют факты расследований, даже там, где положено регистрировать пользователей ИКТ-ресурсов, правила не соблюдаются в угоду “золотому тельцу”. По словам Бориса Мирошникова, ни один мобильный телефон, изъятый у преступников, не зарегистрирован на их имена. “Это не только потому, что некоторые из аппаратов были украдены, — сегодня салоны связи за небольшую плату предоставляют “услугу по регистрации”, которая позволяет не предъявлять документы при покупке телефона. На одного владельца можно зарегистрировать сотни доменных имен, но его персональные данные могут оказаться липовыми — так организована процедура регистрации. Все это благоприятствует преступникам”, — с сожалением констатировал он.

Консолидация в борьбе с киберпреступностью. Помимо ИБ-вендоров заметный вклад в борьбу с вирусописателями в 2009 г. внесли также, по мнению “Лаборатории Касперского”, правоохранительные органы, надзорные структуры и телекоммуникационные компании, в результате чего были закрыты такие активно потворствующие киберпреступникам веб-ресурсы, как UkrTeleGroup, RealHost и 3FN.

Для борьбы со эпидемией Kido была создана специальная группа Conficker Working Group, объединившая антивирусные компании, интернет-провайдеров, независимые исследовательские организации, учебные заведения и регулирующие правительственные органы. Александр Гостев отметил, что создание этой группы стало первым эффективным опытом широкого и представительного международного сотрудничества, вышедшего за рамки обычных контактов между антивирусными экспертами. Отработанная схема может послужить основой для постоянно действующей организации по борьбе с угрозами, терроризирующими весь мир.

Заключение

Пытаясь ответить на основной вопрос, касающийся ИБ, — стали ли наши организации и производственные структуры за прошедший год более защищенными, — стоит вспомнить смысл высказывания литературного классика о счастливых и несчастливых семьях. Перенося его на область ИБ, можно заключить, что без понимания особенностей своих собственных бизнес-процессов и связанных с ними рисков не разобраться в причинах незащищенности своей компании, не понять, откуда конкретно ждать атаки, не выстроить эффективной защиты. Этого понимания, как считают эксперты, можно достичь, сместив фокус усилий на решение организационных ИБ-задач: заняться классификацией корпоративной информации по важности с позиций ИБ и требований регуляторов, определить типы актуальных угроз, построить модели нарушителей, определить и ранжировать по возможному ущербу ИБ-риски. И не забывать, что эту работу нужно регулярно повторять — хотя бы раз в год. А еще правильнее построить систему управления ИБ, руководствуясь в этом деле стандартом ISO 27001.

ПОТРАТИВ ВСЕГО 5 МИНУТ НА ЗАПОЛНЕНИЕ АНКЕТЫ, ВЫ БУДЕТЕ БЕСПЛАТНО ПОЛУЧАТЬ PC Week/RE 50 НЕДЕЛЬ

PC WEEK RUSSIAN EDITION

КОРПОРАТИВНАЯ ПОДПИСКА

Уважаемые читатели!

Только полностью заполненная анкета, рассчитанная на руководителей, отвечающих за автоматизацию предприятий; специалистов по аппаратному и программному обеспечению, телекоммуникациям, сетевым и информационным технологиям из организаций, имеющих **более 10 компьютеров**, дает право на **бесплатную** подписку на газету PC Week/RE в течение года с момента получения анкеты. Вы также можете заполнить анкету на сайте: www.pcweek.ru/subscribe_print/.

Примечание. На домашний адрес еженедельник по бесплатной корпоративной подписке не высылается. Данная форма подписки распространяется только на территорию РФ.

Я хочу, чтобы моя организация получала PC Week/RE !

Название организации:

Почтовый адрес организации:

Индекс: Область:

Город:

Улица: Дом:

Фамилия, имя, отчество:

Подразделение / отдел:

Должность:

Телефон: Факс:

E-mail: WWW:

(Заполните анкету печатными буквами!)

1. К какой отрасли относится Ваше предприятие?

1. Энергетика ❑
2. Связь и телекоммуникации ❑
3. Производство, не связанное с вычислительной техникой (добывающие и перерабатывающие отрасли, машиностроение и т. п.) ❑
4. Финансовый сектор (кроме банков) ❑
5. Банковский сектор ❑
6. Архитектура и строительство ❑
7. Торговля товарами, не связанными с информационными технологиями ❑
8. Транспорт ❑
9. Информационные технологии (см. также вопрос 2) ❑
10. Реклама и маркетинг ❑
11. Научно-исследовательская деятельность (НИИ и вузы) ❑
12. Государственно-административные структуры ❑
13. Военные организации ❑
14. Образование ❑
15. Медицина ❑
16. Издательская деятельность и полиграфия ❑
17. Иное (что именно)

2. Если основной профиль Вашего предприятия – информационные технологии, то уточните, пожалуйста, сегмент, в котором предприятие работает:

1. Системная интеграция ❑
2. Дистрибуция ❑
3. Телекоммуникации ❑
4. Производство средств ВТ ❑
5. Продажа компьютеров ❑
6. Ремонт компьютерного оборудования ❑
7. Разработка и продажа ПО ❑
8. Консалтинг ❑
9. Иное (что именно)

3. Форма собственности Вашей организации (отметьте только один пункт)

1. Госпредприятие ❑
2. ОАО (открытое акционерное общество) ❑
3. ЗАО (закрытое акционерное общество) ❑
4. Зарубежная фирма ❑
5. СП (совместное предприятие) ❑
6. ТОО (товарищество с ограниченной ответственностью) или ООО (Общество с ограниченной ответственностью) ❑
7. ИЧП (индивидуальное частное предприятие) ❑
8. Иное (что именно)

4. К какой категории относится подразделение, в котором Вы работаете? (отметьте только один пункт)

1. Дирекция ❑
2. Информационно-аналитический отдел ❑
3. Техническая поддержка ❑
4. Служба АСУ/ИТ ❑
5. ВЦ ❑
6. Инженерно-конструкторский отдел (САПР) ❑
7. Отдел рекламы и маркетинга ❑
8. Бухгалтерия/Финансы ❑
9. Производственное подразделение ❑
10. Научно-исследовательское подразделение ❑
11. Учебное подразделение ❑
12. Отдел продаж ❑
13. Отдел закупок/логистики ❑
14. Иное (что именно)

5. Ваш должностной статус (отметьте только один пункт)

1. Директор / президент / владелец ❑
2. Зам. директора / вице-президент ❑
3. Руководитель подразделения ❑
4. Сотрудник / менеджер ❑
5. Консультант ❑
6. Иное (что именно)

6. Ваш возраст

1. До 20 лет ❑
2. 21–25 лет ❑
3. 26–30 лет ❑
4. 31–35 лет ❑
5. 36–40 лет ❑
6. 41–50 лет ❑
7. 51–60 лет ❑
8. Более 60 лет ❑

7. Численность сотрудников в Вашей организации

1. Менее 10 человек ❑
2. 10–100 человек ❑
3. 101–500 человек ❑
4. 501–1000 человек ❑
5. 1001–5000 человек ❑
6. Более 5000 человек ❑

8. Численность компьютерного парка Вашей организации

1. 10–20 компьютеров ❑
2. 21–50 компьютеров ❑
3. 51–100 компьютеров ❑
4. 101–500 компьютеров ❑
5. 501–1000 компьютеров ❑
6. 1001–3000 компьютеров ❑
7. 3001–5000 компьютеров ❑
8. Более 5000 компьютеров ❑

9. Какие ОС используются в Вашей организации ?

1. DOS ❑
2. Windows 3.xx ❑
3. Windows 9x/ME ❑
4. Windows NT/2K/XP/2003 ❑
5. OS/2 ❑
6. Mac OS ❑
7. Linux ❑
8. AIX ❑
9. Solaris/SunOS ❑
10. Free BSD ❑
11. HP/UX ❑
12. Novell NetWare ❑
13. OS/400 ❑
14. Другие варианты UNIX ❑
15. Иное (что именно)

10. Коммуникационные возможности компьютеров Вашей организации

1. Имеют выход в Интернет по выделенной линии ❑
2. Объединены в intranet ❑
3. Объединены в extranet ❑
4. Подключены к ЛВС ❑
5. Не объединены в сеть ❑
6. Dial Up доступ в Интернет ❑

11. Имеет ли сеть Вашей организации территориально распределенную структуру (охватывает более одного здания)?

Да ❑ Нет ❑

12. Собирается ли Ваше предприятие устанавливать интрасети (intranet) в ближайший год ?

Да ❑ Нет ❑

13. Сколько серверов в сети Вашей организации ?

14. Если в Вашей организации используются мэйнфреймы, то какие именно?

1. ЕС ЭВМ ❑
2. IBM ❑
3. Unisys ❑
4. VAX ❑
5. Иное (что именно)
6. Не используются ❑

15. Компьютеры каких фирм-изготовителей используются на Вашем предприятии?

	Настольные ПК	Портативные ПК	Серверы
"Аквариус"	❑	❑	❑
ВИСТ	❑	❑	❑
"Формоза"	❑	❑	❑
Acer	❑	❑	❑
Apple	❑	❑	❑
CLR	❑	❑	❑
Compaq	❑	❑	❑
Dell	❑	❑	❑
Fujitsu Siemens	❑	❑	❑
Gateway	❑	❑	❑
Hewlett-Packard	❑	❑	❑
IBM	❑	❑	❑
Kraftway	❑	❑	❑
R.&K.	❑	❑	❑
R-Style	❑	❑	❑
Rover Computers	❑	❑	❑
Sun	❑	❑	❑
Siemens Nixdorf	❑	❑	❑
Toshiba	❑	❑	❑

Иное (что именно)

16. Какое прикладное ПО используется в Вашей организации?

1. Средства разработки ПО ❑
2. Офисные приложения ❑
3. СУБД ❑
4. Бухгалтерские и складские программы ❑
5. Издательские системы ❑
6. Графические системы ❑
7. Статистические пакеты ❑
8. ПО для управления производственными процессами ❑
9. Программы электронной почты ❑
10. САПР ❑
11. Браузеры Internet ❑
12. Web-серверы ❑
13. Иное (что именно)

17. Если в Вашей организации установлено ПО масштаба предприятия, то каких фирм-разработчиков?

1. "1С" ❑
2. "АйТи" ❑
3. "Галактика" ❑
4. "Парус" ❑
5. BAAN ❑
6. Navision ❑
7. Oracle ❑
8. SAP ❑
9. Epicor Scala ❑
10. ПО собственной разработки ❑
11. Иное (что именно)
12. Не установлено никакое ❑

18. Существует ли на Вашем предприятии единая корпоративная информационная система?

Да ❑ Нет ❑

19. Если Ваша организация не имеет своего Web-узла, то собирается ли она в ближайший год завести его?

Да ❑ Нет ❑

20. Если Вы используете СУБД в своей деятельности, то какие именно?

1. Adabas ❑
2. Cache ❑
3. DB2 ❑
4. dBase ❑
5. FoxPro ❑
6. Informix ❑
7. Ingress ❑
8. MS Access ❑
9. MS SQL Server ❑
10. Oracle ❑
11. Progress ❑
12. Sybase ❑
13. Иное (что именно)
14. Не используем ❑

21. Как Вы оцениваете свое влияние на решение о покупке средств информационных технологий для своей организации? (отметьте только один пункт)

1. Принимаю решение о покупке (подписываю документ) ❑
2. Составляю спецификацию (выбираю средства) и рекомендую приобрести ❑
3. Не участвую в этом процессе ❑
4. Иное (что именно)

22. На приобретение каких из перечисленных групп продуктов или услуг Вы оказываете влияние (покупаете, рекомендуете, составляете спецификацию)?

Системы

1. Мэйнфреймы ❑
2. Миникомпьютеры ❑
3. Серверы ❑
4. Рабочие станции ❑
5. ПК ❑
6. Тонкие клиенты ❑
7. Ноутбуки ❑
8. Карманные ПК ❑

Сети

9. Концентраторы ❑
10. Коммутаторы ❑
11. Мосты ❑
12. Шлюзы ❑
13. Маршрутизаторы ❑
14. Сетевые адаптеры ❑
15. Беспроводные сети ❑
16. Глобальные сети ❑
17. Локальные сети ❑
18. Телекоммуникации ❑

Периферийное оборудование

19. Лазерные принтеры ❑
20. Струйные принтеры ❑
21. Мониторы ❑
22. Сканеры ❑
23. Модемы ❑
24. ИБП (UPS) ❑

Память

25. Жесткие диски ❑
26. CD-ROM ❑
27. Системы архивирования ❑
28. RAID ❑
29. Системы хранения данных ❑

Программное обеспечение

30. Электронная почта ❑
31. Групповое ПО ❑
32. СУБД ❑
33. Сетевое ПО ❑
34. Хранилища данных ❑
35. Электронная коммерция ❑
36. ПО для Web-дизайна ❑
37. ПО для Интернета ❑
38. Java ❑
39. Операционные системы ❑
40. Мультимедийные приложения ❑
41. Средства разработки программ ❑
42. CASE-системы ❑
43. САПР (CAD/CAM) ❑
44. Системы управления проектами ❑
45. ПО для архивирования ❑

Внешние сервисы

46. ❑

Ничего из вышеперечисленного

47. ❑

23. Каков наивысший уровень, для которого Вы оказываете влияние на покупку компьютерных изделий или услуг (служб)?

1. Более чем для одной компании ❑
2. Для всего предприятия ❑
3. Для подразделения, располагающегося в нескольких местах ❑
4. Для нескольких подразделений в одном здании ❑
5. Для одного подразделения ❑
6. Для рабочей группы ❑
7. Только для себя ❑
8. Не влияю ❑
9. Иное (что именно)

24. Через каких провайдеров в настоящее время Ваша фирма получает доступ в интернет и другие интернет-услуги?

1. "Демос" ❑
2. МТУ-Интел ❑
3. "Релком" ❑
4. Combellga ❑
5. Comstar ❑
6. Golden Telecom ❑
7. Equant ❑
8. ORC ❑
9. Telmos ❑
10. Zebra Telecom ❑
11. Через других (каких именно)

Дата заполнения

Отдайте заполненную анкету представителям PC Week/RE либо пришлите ее по адресу: **109147, Москва, ул. Марксистская, д. 34, корп. 10, PC Week/RE.**

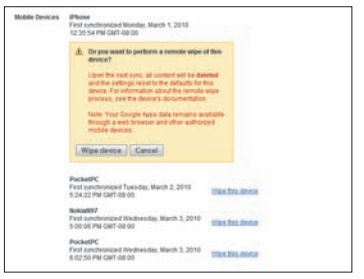
Анкету можно отправить на e-mail: info@pcweek.ru

Google Apps...

◀ ПРОДОЛЖЕНИЕ СО С. 8

На странице пользователя сообщается чрезвычайно ограниченная информация об устройстве. Трудно сказать, является это упущением Google или же изготовителей устройств, так как они часто реализуют ActiveSync чуть по-разному, да и сам протокол не оговаривает четко, что должны сообщить о себе изготовители. Так что, хотя я видел, что Nokia N97 появился на странице администратора Google именно как N97, iPhone 3GS был показан просто как iPhone, iPod Touch — как iPod, а оба телефона с Windows Mobile — просто как устройства PocketPC, и не было никаких других отличительных подробностей вроде международной идентификации IMEI или серийного номера.

Google также не сообщает о дальнейшем использовании устройства. Я мог видеть дату и время первой синхронизации каждого устройства с доменом, но не видел последний сеанс синхронизации, так что администратор не может сказать, используется ли еще данное устройство.



Администратор может дистанционно уничтожить данные на мобильном устройстве, которое потеряно или украдено. Соответствующая команда будет послана на устройство при очередной попытке синхронизации

Последняя функция, доступная администратору, это команда стирания данных. На странице управления пользователями у администратора каждое устройство, синхронизированное с аккаунтом, снабжено ссылкой, чтобы дать команду дистанционного удаления данных в следующий раз, когда оно запросит синхронизацию. Я попробовал такую операцию для iPhone, телефонов с Windows Mobile и N97 и нашел, что команда была дана и успешно выполнена спустя несколько минут (при условии, что устройство было подключено к сотовой сети передачи данных или к сети Wi-Fi).

Однако, как администратор, я не всегда мог ясно видеть, что уничтожение данных прошло успешно. В частности, для HTC Fuze с Windows Mobile 6.1 административная консоль показала, что команда успешно выполнена (с меткой времени). Для всех остальных тестированных устройств консоль не получила (или не сообщила, что получила) подтверждение, что команда стирания была дана и выполнена. Для каждого из них было лишь показано, что "устройство будет дистанционно очищено при следующей синхронизации".

Так что теоретически, если пользователь сообщит, что телефон потерян или украден, и попросит администратора стереть информацию в нем, но потом вдруг найдет телефон и попробует вновь активировать его и подключиться к домену, очистка его содержимого будет повторяться до тех пор, пока пользователь не догадается еще раз позвонить администратору и попросить об отмене команды.

В самом деле, ввиду ограниченного набора возможностей, предлагаемых Google на текущий момент, имело бы смысл разрешить пользователям давать команду на уничтожение данных в принадлежащих им устройствах со страницы настроек веб-интерфейса Gmail. На сегодня лишь администратор домена может дистанционно стереть информацию в телефоне или отменить данную команду. Если бы администратор мог разрешить пользователям дистанционно очищать их собственные устройства (с уведомлением, высылаемым при этом администратору домена), то это могло бы уменьшить количество звонков в службу поддержки.

ВКРАТЦЕ

СИСТЕМНАЯ ИНТЕГРАЦИЯ

Сложные проекты помогли "Энвижн Груп"

Интеграторская компания "Энвижн Груп" (NVision Group) объявила об итогах своей деятельности в 2009 г. Сообщается, что за минувший год оборот компании составил 12,885 млрд. руб., что примерно на 2% выше показателя 2008 г. При этом в общей структуре оборота выручка филиалов увеличилась до 20,7%.

"Мы работаем на рынке сложных проектов. Такие проекты в кризис востребованы — они позволяют создавать информационные системы, значительно экономящие средства заказчика и оптимизирующие его бизнес-процессы. В 2009 г. наша экспертиза была востребована, особенно операторами связи, государственными заказчиками, банками, компаниями ТЭК", — сообщил первый заместитель генерального директора "Энвижн Груп" Евгений Закрепин.

Сообщается также, что в минувшем году в структуре оборота "Энвижн Груп" доля оказания сложных ИТ-услуг возросла до 34,5%, что связано с созданием в ней на основе сервисных подразделений компании федерального центра технической поддержки, который в круглосуточном режиме предоставляет консультации и услуги заказчикам по более чем 200 решениям и видам оборудования.

В 2010 г. NVision Group планирует увеличить свой оборот не менее чем на 50%. Предполагается увеличение региональной составляющей в этом обороте до 30%. Кроме того, в планах компании открытие офисов на Дальнем Востоке и Юге России. ***В. М.***

С — значит Cloud

◀ ПРОДОЛЖЕНИЕ СО С. 1

В качестве ОС для Primergy CX1000 S1 могут использоваться Red Hat Enterprise Linux и Microsoft Windows Server 2008 R2.

Практически одновременно с Fujitsu свое решение для облачных вычислений представила компания Dell. Ее новая серия серверов PowerEdge C разработана с учетом собственного опыта по выпуску серверов в заказной конфигурации для гигантских вычислительных центров Google, Microsoft и нескольких других крупных клиентов. В отличие от Fujitsu американская компания предлагает три модели узлов облачных систем — одноюнитовый вычислительный узел PowerEdge C1100 (прямой конкурент Primergy CX1000 S1), вмещающий два Intel Xeon, до 144 Гб оперативной памяти, до десяти 2,5-дюймовых жестких дисков и интерфейсную карту 10 Gigabit Ethernet, двухъюнитовый двухпроцессорный узел хранения PowerEdge C2100, в который можно установить дюжину полноразмерных винчестеров, и двухъюнитовое шасси PowerEdge C6100, рассчитанное на установку четырех двухпроцессорных вычислительных узлов

Шасси Dell PowerEdge C6100 вмещает четыре вычислительных узла

половинного форм-фактора. Отметим, что PowerEdge C6100 использует тот же подход к повышению плотности процессорной мощности, который компания Hewlett-Packard ранее применила в своем HP ProLiant SL2x170z G6 из серии серверов для горизонтально масштабируемых систем HP ProLiant SL6000. Вычислительные узлы PowerEdge C поддерживают дистрибутивы Linux от Red Hat Novell Suse.

РАСПРОСТРАНЕНИЕ PC WEEK/RUSSIAN EDITION

Подписку можно оформить в любом почтовом отделении по каталогам:

- **"Газеты журналы"** (индекс 82143). ОАО "Агентство "Роспечать"
- **"Пресса России. Объединенный каталог"** (индекс 44098) ОАО "АРЗИ"
- **"Почта России. Каталог российской прессы"** (индекс 16763) ООО "МАП"
- **"Подписка на рабочий стол"** (индекс 82143) Агентство Деловая Пресса

Альтернативная подписка в агентствах:

- **ООО "Интер-Почта-2003"** — осуществляет подписку во всех регионах РФ и странах СНГ. Тел./факс (495) 580-9-580; 500-00-60; e-mail: interpochta@interpochta.ru; www.interpochta.ru
- **ООО "Агентство Артос-ГАЛ"** — осуществляет подписку всех государственных библиотек, юридических лиц в Москве, Московской области и крупных регионах РФ. Тел./факс (495) 788-39-88; e-mail: shop@setbook.ru; www.setbook.ru
- **ООО "Урал-Пресс"** г. Екатеринбург — осуществляет подписку крупнейших российских предприятий в более чем 60 своих филиалах и представительствах. Тел./факс (343) 26-26-543 (многоканальный); (343) 26-26-135; e-mail: info@ural-press.ru; www.ural-press.ru

ПРЕДСТАВИТЕЛЬСТВО В МОСКВЕ

Тел. (495) 789-86-36; факс(495) 789-86-37; e-mail: moskva@ural-press.ru

ПРЕДСТАВИТЕЛЬСТВО В САНКТ-ПЕТЕРБУРГЕ

Тел./факс (812) 962-91-89

ПРЕДСТАВИТЕЛЬСТВО В КАЗАХСТАНЕ

тел./факс 8(3152) 47-42-41; e-mail: kazahstan@ural-press.ru

- **ЗАО "МК-Периодика"** — осуществляет подписку физических и юридических лиц в РФ, ближнем и дальнем зарубежье. Факс (495) 306-37-57; тел. (495) 672-71-93, 672-70-89; e-mail: catalog@periodikals.ru; info@periodicals.ru; www.periodicals.ru
- **ООО "Вся Пресса"** — осуществляет подписку во всех федеральных округах и регионах России, республиках Башкортостан, Молдова, Украина, Белоруссия, Татарстан, Казахстан, Армения, странах Балтии. Тел. (495) 234-03-07
- **Подписное Агентство KSS** — осуществляет подписку в Украине. Тел./факс — 8-1038- (044)585-8080 www.kss.kiev.ua, e-mail: kss@kss.kiev.ua

ВНИМАНИЕ!
Для оформления бесплатной корпоративной подписки на PC Week/RE можно обращаться в отдел распространения по тел. (495) 323-1455 или E-mail: deliver@skpress.ru.
Если у Вас возникли проблемы с получением номеров PC Week/RE по корпоративной подписке, пожалуйста, сообщите об этом в редакцию PC Week/RE по адресу: editorial@pcweek.ru или по телефону: (495) 974-2260. ***Редакция***

ЭТОТ НОМЕР ВЫПУСКАЛИ

Выпускающий редактор: Игорь Лапинский

Ответственный за компьютерную графику и верстку: Алексей Мануйлов

ПОДПИШИСЬ НА 2010 ГОД

Я подписываюсь

	на 3 месяца и плачу за 12 журналов 660 рублей (в т. ч. НДС 10%)
	на 6 месяцев и плачу за 24 журнала 1180 рублей (в т. ч. НДС 10%)
	на 12 месяцев и плачу за 48 журналов 2100 рублей (в т. ч. НДС 10%)

Ф.И.О._____
_____дата рождения_____индекс_____
обл./край_____р-н_____
город_____улица_____
дом_____корп._____этаж_____кв._____домофон_____
код_____тел._____

Копия квитанции об оплате от _____ с отметкой банка прилагается

ИЗВЕЩЕНИЕ

ИНН 7707010704 КПП 770701001
ЗАО “СК Пресс”
получатель платежа
Учреждение банка Сбербанка России, ОАО Вернадское ОСБ г. Москвы № 7970

Расчетный счет №	**40702810938100100746**	**БИК**	**044525225**
Кор. счет:	**30101810400000000225**		

фамилия, и. о., адрес

Назначение платежа	**Дата**	**Сумма**
Подписка на журнал «PC WEEK»		
	Всего:	

Плательщик:

Кассир

КВИТАНЦИЯ

ИНН 7707010704 КПП 770701001
ЗАО “СК Пресс”
получатель платежа
Учреждение банка Сбербанка России, ОАО Вернадское ОСБ г. Москвы № 7970

Расчетный счет №	**40702810938100100746**	**БИК**	**044525225**
Кор. счет:	**30101810400000000225**		

фамилия, и. о., адрес

Назначение платежа	**Дата**	**Сумма**
Подписка на журнал «PC WEEK»		
	Всего:	

Плательщик:

Кассир

СК ПРЕСС

PC WEEK RUSSIAN EDITION

Стоимость подписки:

На 3 месяца (12 журналов) — 660 рублей (в т. ч. НДС 10%)
На 6 месяцев (24 журнала) — 1180 рублей (в т. ч. НДС 10%)
На 12 месяцев (48 журналов) — 2100 рублей (в т. ч. НДС 10%)
Данное предложение на подписку и указанные цены действительны до 30.06.2010

Чтобы оформить подписку Вам необходимо:

— Заполнить прилагаемый купон-заявку и платежное поручение.
— Перевести деньги (стоимость подписного комплекта) на указанный р/с в любом отделении Сбербанка.
— Отправить заполненный купон-заявку и копию квитанции о переводе денег по адресу:
109147, г. Москва, ул. Марксистская, 34, корп.10,
3 этаж, оф. 328 (отдел распространения, подписка),
или по факсу: (495) 974-2263. Тел. (495) 974-2260,
отдел распространения, менеджеру по подписке.

Журнал высылается заказной бандеролью.

Цена подписки включает в себя стоимость доставки в пределах РФ.

Если мы получили Вашу заявку до 10-го числа текущего месяца и деньги поступили на р/с ООО «СК Пресс», подписка начинается со следующего месяца.
Не забудьте, пожалуйста, указать в квитанции Ваши фамилию и инициалы, а также Ваш точный адрес с почтовым индексом.

Внимание! Отдел подписки не несет ответственность, если подписка оформлена через другие фирмы.

Редакционная подписка осуществляется только в пределах РФ.

Деньги за принятую подписку не возвращаются.

Условия подписки:

* Минимальный период подписки — 3 месяца.
** Начало доставки — следующий месяц за месяцем, в котором оплачена подписка.
*** Оформляя подписку, подписчик соглашается, что его персональные данные могут быть предоставлены третьим лицам для выполнения доставки издания.

Справки по телефону: +7 (495) 974-2260, доб. 1736; e-mail: distribution@skpress.ru.