ГАЗЕТА ДЛЯ КОРПОРАТИВНЫХ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И РЕШЕНИЙ

18+

PC WEEK RUSSIAN EDITION

СК ПРЕСС

№ 13 (833) • 21 МАЯ • 2013 • МОСКВА

http://www.pcweek.ru

Точки доступа Wi-Fi из Твери

ПЕТР ЧАЧИН

Cisco Systems продолжает политику расширения производства своих продуктов в России. На сей раз в Твери освоена сборка точек доступа Wi-Fi из компонентов и материалов американской компании. В итоге Cisco избавилась от головной боли из-за сложной процедуры ввоза в РФ радиоэлектронного оборудования и сокращения сроки поставки данной техники отечественным заказчикам, а российская сторона получила несколько десятков новых рабочих мест.

ПРОИЗВОДСТВО

Андрей Харитонов: "Точки доступа 2600 представляют собой совершенно новый продукт из семейства беспроводных устройств Cisco"

Как сообщил Михаил Пахомов, директор Cisco по взаимодействию с органами государственной власти, в Твери налажен процесс производства унифицированных точек беспроводного доступа Cisco AIR-CAP2602I-R-K9 и AIR-CAP2602E-R-K9 со встроенными и внешними антеннами. По его словам, таким образом компания вносит свой вклад в поддержку инновационного развития России в соответствии с долгосрочными договоренностями, достигнутыми с участием президента РФ. "Для нас стратегическое партнерство с государством остается приоритетом", — сказал Михаил Пахомов.

Это уже четвертое семейство продуктов Cisco, выпускаемых в России на производственных мощностях одного из глобальных подрядчиков компании Cisco. Ранее Cisco наладила производство в РФ маршрутизаторов Cisco 2911R с интеграцией сервисов (ISR), аппаратных VPN-модулей и цифровых телевизионных приставок.

Cisco 2600 относятся к корпоративному сегменту WLAN-рынка, который, по данным компании, вырос в России с 2010 г. в 20—25 раз. Общий объем WLAN-рынка в РФ составляет 150 млн. долл., его корпоративный сегмент оценивается в 82 млн. долл., доля Cisco в корпоративном сегменте — около 50%.

Точки доступа 2600 поддерживают скорость обмена данными до 450 Мбит/с и представляют собой совершенно новый продукт из семейства беспроводных устройств Cisco, утверждает Андрей Харитонов, менеджер Cisco по развитию бизнеса. Он был анонсирован в сентябре прошлого года и разработан с учетом быстро меняющихся требований мобильных абонентов.

Cisco 2600 предназначены для корпоративных сетей любого размера, где необходимы высокая производительность, безопасность и надежные каналы

ПРОДОЛЖЕНИЕ НА С. 8 ▸

Windows 8.1 выйдет в этом году

КАК И ОЖИДАЛОСЬ, WINDOWS BLUE ОКАЗАЛАСЬ WINDOWS 8 SP1

АНДРЕЙ КОЛЕСОВ

Обновленный вариант настольной ОС Microsoft, уже несколько месяцев известный под кодовым названием "Windows Blue" ("оконная синева"), отныне официально именуется Windows 8.1 и бесплатно доступен пользователям текущей версии Windows 8 через механизмы обновления системы, в том числе через Windows Store. Правда, сначала новый продукт будет представлен в виде публичной предварительной версии (это произойдет на очередной, третьей по счету конференции Microsoft Build'2013 для независимых разработчиков ПО, которая на этот раз пройдет в Сан-Франциско в конце июня), выпуск финального же варианта Windows 8.1 (как для Windows 8, так и для Windows RT) состоится позднее, но точно в этом году. Обо всем этом 14 мая официально объявила на проходившей в Бостоне (США) JP Morgan Technology, Media & Telecom Conference корпоративный вице-президент подразделения Windows Microsoft Тами Реллер, которая, отвечая за финансы и маркетинг направления настольных ОС, выполняет также функции официального рупора корпорации в этой сфере.

ОС

Тами Реллер: "Windows 8.1 поможет нам при поддержке наших OEM-партнеров предоставить рынку новое поколение ПК и планшетов"

Впрочем, ничего неожиданного в такой новости нет: Microsoft просто официально сообщила то, что уже давно известно на рынке из "утечек", инициированных, кажется, самой же компанией, и простого анализа рыночной ситуации. В этой связи нужно напомнить, что согласно "законам жанра" (создание маркетингового антуража вокруг выпуска очередной версии Windows) первые разговоры о "Windows Next" начались еще за год до выпуска Windows 8 и резко активизировались сразу после ее выхода в октябре 2012-го. Поначалу речь шла о "Windows 9" (т. е. о новом варианте именно основной версии ОС), но уже прошлой осенью стало использоваться кодовое имя "Windows Blue", что сразу навело на мысль, что речь будет идти лишь о создании сервисного пакета для текущей Windows 8. Подтверждением такому развитию событий послужило появление "утечек" о том, что "голубая Windows" будет иметь номер 8.1. Но то, что

ПРОДОЛЖЕНИЕ НА С. 8 ▸

В НОМЕРЕ:

ISSN 1560-6929

9 771560 692004 13013 >

ПОДПИСНОЙ ИНДЕКС 32485 (по каталогу ЦРПА "Роспечать")

EMC призывает заказчиков и партнеров трансформироваться

АНДРЕЙ КОЛЕСОВ

Корпорация EMC намерена и дальше расширять свое присутствие на ИТ-рынке в роли поставщика широкого спектра ИТ-решений и сервисов для создания современных корпоративных систем, смело осваивая новые технологии и модели их применения в ответ на появляющиеся вызовы времени. Призывая своих существующих и потенциальных клиентов к трансформации не только своих ИТ-систем, но и самого бизнеса на их основе, компания своим собственным примером показывает, как нужно действовать в эпоху ИТ-перемен.

КОНФЕРЕНЦИИ

Наверное, именно так в очень сжатом виде можно сформулировать основные тезисы выступления президента и CEO EMC Джо Туччи на открытии очередной ежегодной конференции EMC World'2013, традиционно прошедшей в Лас-Вегасе (США) в начале мая. Он отметил, что хотя руководимая им компания до сих пор по старой памяти часто именуется в СМИ как storage giant, EMC — это уже давно не только устройства хранения данных, но и представительный спектр ИТ-решений, который будет расширяться и в дальнейшем. Любопытно, что сама история конференций EMC World довольно наглядно отражает путь развития самой компании: первое такое мероприятие состоялось в 2002 г.,

Джо Туччи: "Когда вы мыслите масштабами петабайтов, вам нужно создавать качественно новые приложения на основе самых современных технологий и моделей их применения"

когда EMC, в условиях тогдашнего мирового экономического кризиса, начала свое движение от производства средств хранения данных в сторону создания ИТ-платформ.

"Lead Your IT Trasfomafion" ("возглавь свою ИТ-трансформацию") — именно таким был лозунг нынешней конференции, который воспринимался как призыв ко всем участникам (а их было около 15 тыс.) не оставаться пассивными зрителями происходящих в ИТ-мире преобразований, а самым активным образом возглавить их. В целом в обществе уже сложилось вполне четкое понимание того, что ИТ-отрасль переживает сейчас важный качественный этап смены поколений ИТ-платформ, причем рынку еще только предстоит перейти от использования доминирующих сегодня решений и технологий второго поколения к системам третьего.

В этой ситуации сама EMC, расширяя сферу своего присутствия на ИТ-рынке, организационно трансформируется в группу компаний, которая сейчас состоит из трех предприятий — самой EMC, лидера виртуализационного рынка VMware и недавно созданной Pivotal. Говоря о принципах взаимодействия внутри этого холдинга, Джо Туччи в качестве иллюстрации привел изображения копья, в котором функции основы-древка выполняет аппаратно-программная платформа информационной инфраструктуры EMC, а острием-наконечником является система облачно-виртуализационных средств VMware. Поясняя эту схему, руководитель EMC отметил,

ПРОДОЛЖЕНИЕ НА С. 8 ▸

Intel противопоставляет решениям ARM архитектуру Silvermont

ДЖЕФФРИ БЕРТ

Спустя пять лет после выпуска первых чипов Atom Intel переводит эту платформу на новую микроархитектуру, которая, как утверждают в корпорации, позволит значительно превзойти по производительности и энергосбережению всё, что может предложить ARM и ее партнеры. Остается только посмотреть, окажутся ли доводы в пользу новых систем на кристалле с микроархитектурой Silvermont столь убедительными, чтобы производители стали использовать их в своих планшетах и смартфонах, а пользователи — приобретать такие устройства.

Дэди Перлмуттер: "Мы развенчиваем миф о том, что ARM может делать то, что не в состоянии сделать Intel"

"Мы развенчиваем миф о том, что ARM может делать то, что не в состоянии сделать Intel", — заявил в ходе состоявшейся 6 мая онлайн-презентации Silvermont исполнительный вице-президент и генеральный менеджер подразделения Intel Architecture Group Дэди Перлмуттер.

Чипы на базе Silvermont будут применяться везде — от серверов до ПК и встроенных систем, но область мобильных и малопотребляющих устройств, в частности смартфонов, планшетов и микросерверов, где новые кристаллы будут напрямую конкурировать с продуктами ARM, — это как раз та сфера, которая будет определять успех или провал новой микроархитектуры.

На протяжении нескольких лет Intel продвигала свою платформу Atom (и в меньшей степени процессоры Core) в качестве технологии, которая должна была обеспечить выход корпорации на быстро растущий рынок мобильных устройств. Сегодня подавляющее большинство представленных на рынке планшетов и смартфонов базируются на SoC-кристаллах, разработанных ARM специально для мобильных устройств и выпускаемых такими компаниями, как Qualcomm, Samsung и Nvidia. Чтобы конкурировать с ними, Intel, в свою очередь, предпринимала попытки снизить энергопотребление своих x86-совместимых кристаллов Atom и лежащей в их основе микроархитектуры Bonnell.

Всё должно измениться в конце нынешнего и начале следующего года, когда на рынок начнут поступать планшеты с процессорами Bay Trail и смартфоны с процессорами Merrifild, выполненными уже по 22-нм технологии. Как заявил Перлмуттер, микроархитектура Silvermont обеспечит Intel широкую дорогу в мир мобильных устройств.

Кроме того, Silvermont будет реализована в кристаллах Avoton, предназначенных для малопотребляющих микросерверов с высокой плотностью размещения, а также в SoC Rangeley, ориентированных на использование в маршрутизаторах и коммутаторах. Начало поставок Avoton и Rangeley запланировано на вторую половину 2013 г. Помимо этого предполагается выпуск кристаллов (у них пока нет названия) для информационно-развлекательных систем.

Агрессивные планы гиганта в области микропроцессоров предусматривают также замену Silvermont в следующем году 14-нм микроархитектурой Airmont, на смену которой годом позже придет новая, пока еще не имеющая кодового названия.

В ходе продолжительной онлайн-презентаации Перлмуттер и главный архитектор Белли Куттанна рассказали о тех инновациях, которые обеспечат кристаллам с Silvermont не только высокую энергоэффективность, но и повышенную производительность. "Действительно важная новость состоит в том, что нам удалось помимо значительного снижения энергопотребления кристаллов существенно поднять их производительность, — заявил Перлмуттер. — Мы знаем, как это обеспечить".

По словам Перлмуттера, кристаллы Atom с микроархитектурой Silvermont будут потреблять в пять раз меньше энергии, а работать они станут в три раза быстрее нынешних версий процессора.

Что еще более важно, по сравнению с четырехъядерными ARM-процессорами двухъядерные Atom с Silvermont для смартфонов будут иметь превосходство в производительности в 1,6 раза, а в энергопотреблении — в 2,4. В свою очередь, четырехъядерные Atom для планшетов будут функционировать вдвое быстрее и потреблять в 4,3 раза меньше электроэнергии, чем четырехъядерные ARM-кристаллы.

В Intel считают, что по инженерному и производственному потенциалам корпорация значительно превосходит конкурирующих с нею производителей, включая Advanced Micro Devices и ARM. Как заявили Перлмуттер и Куттанна, микроархитектура Silvermont подтверждает это преимущество.

В числе реализованных в Silvermont инноваций отмечены транзисторы с трехмерной структурой затвора 3D Trigate, впервые представленные в 2011 г. в 22-нм кристаллах Ivy Bridge, а теперь оптимизированные для Silvermont. Они обеспечивают улучшение производительности и энергоэффективности новых процессоров. Кроме того, новый механизм изменения очередности выполнения команд повышает однопоточную производительность, поддерживая исполнение уже готовых инструкций вместо строгого соблюдения их порядка с затратой времени на ожидание еще не готовых для исполнения команд. Новая архитектура масштабируется до восьми процессорных ядер, а обновленная система команд помимо повышения производительности процессора поддерживает расширенные функции управления виртуализацией и обеспечением безопасности.

В новой микроархитектуре также реализована усовершенствованная технология Intel Burst, а для улучшения отвода тепла обеспечено перераспределение мощности не только между ядрами кристалла, но и между другими его компонентами, включая GPU.

В Intel утверждают, что готовящиеся к выводу на рынок новые кристаллы Atom по производительности и энергосбережению оставят ARM-процессоры позади.

Куттанна также пояснил, что новые системы на кристалле строятся с использованием двухъядерных модулей с разделяемой кэш-памятью второго уровня (L2) емкостью до 1 Мб и непосредственным интерфейсом связи с коммутационной матрицей SoC. Масштабирование SoC, по его словам, осуществляется простым добавлением модулей.

Представители Intel заявили, что благодаря превосходству Silvermont над продуктами ARM и ее партнеров они ожидают поворота индустрии в сторону предлагаемых корпорацией решений. Перлмуттер отметил рост интереса к микроархитектуре Silvermont со стороны производителей устройств после того, как о ней было объявлено, и их заинтересованность в ее использовании в самых разных системах. Куттанна также прокомментировал предыдущие шаги компании по продвижению в мобильную сферу, заявив, что корпорация занимает то положение, которое хочет занимать. "Теперь, лучше представляя мобильный мир и его потребности, мы используем преимущества, которыми обладает Intel", — заявил он.

Microsoft продвигает стандарт разработки защищенного ПО

РОБЕРТ ЛЕМОС

Ряд крупных компаний, специализирующихся в области разработки ПО, поддержал инициативы, которые должны упростить небольшим софтверным фирмам внедрение процессов разработки защищенного программного обеспечения.

В первый день Security Development Conference, пришедшийся на 14 мая, корпорация Microsoft объявила о своей поддержке международного стандарта ISO 27034, определяющего процессы и практики такой разработки. Одновременно отраслевая ассоциация SAFECode (Software Assurance Forum for Excellence in Code), продвигающая передовые практики разработки, сообщила о готовности первых учебных модулей, создаваемых в рамках бесплатной веб-программы подготовки разработчиков ПО и предназначенных для освоения практик безопасного кодирования.

Тем самым крупные софтверные вендоры подчеркивают важность принятия мер по обеспечению защиты ПО с первых стадий его разработки, пояснил представителю *eWeek* Тим Райнс, возглавляющий в Microsoft направление Trustworthy Computing. "Мы считаем, что компании не могут больше позволять себе выполнение бизнес-операций в режиме онлайн, не поставив во главу угла вопросы безопасности, — заявил он. — Разработчикам следует ознакомиться с данным стандартом ISO. Соответствующие материалы и инструменты предлагаются бесплатно".

Microsoft всерьез озаботилась проблемами создания защищенного ПО с тех пор, как сооснователь корпорации, а впоследствии член совета директоров Билл Гейтс выступил с инициативой Trustworthy Computing (это произошло в 2002 г.), обратившись к сотрудникам компании с призывом ставить вопросы безопасности ПО выше его функциональности, именно им уделяя внимание в первую очередь. Это принесло свои результаты: Microsoft оказалась единственной компанией, которой, согласно исследованию NSS Labs, удалось в 2012 г. уменьшить число уязвимостей в своем ПО по сравнению с усредненным за последнее десятилетие показателем.

Microsoft объявила о поддержке международного стандарта безопасной разработки ПО, а группа представителей индустрии предложила бесплатную программу обучения разработчиков.

Еще в ноябре 2011-го Международная организация по стандартизации (ISO) выпустила первую часть документа по технологиям безопасного программирования — 27034-1. Этот документ, в котором дается обзор элементов процесса безопасной разработки ПО, может стать хорошим подспорьем для компаний, стремящихся определить набор требований к безопасности приобретаемого ими ПО. А для разработчиков он может послужить отправной точкой для формирования программ, направленных на повышение защищенности создаваемых приложений.

"Мы видим в этом выгоды как для поставщиков программного обеспечения, так и для тех, кто его приобретает, поскольку стандарт позволяет обеим сторонам говорить на одном языке, когда обсуждаются практики безопасной разработки ПО, — пояснил Райнс. — Стандарт фокусируется именно на разработке ПО и является первым среди такого рода стандартов, который описывает процессы и инструменты, действительно необходимые для формирования комплексного подхода к созданию защищенного ПО".

На Security Development Conference было также объявлено о готовности шести учебных модулей, позволяющих программистам и менеджерам проектов ознакомиться с практиками безопасной разработки программного обеспечения. Модули разработаны по инициативе ассоциации SAFECode, которая объединяет ряд технологических компаний, заинтересованных в повышении безопасности софтверных и аппаратных продуктов, и в числе прочих позволяют обеспечить защиту от подделки запросов, защиту паролей и контроль доступа в Windows. Все они представлены на специально созданном новом веб-сайте (https://training.safecode.org), а по содержанию являются вводными, в силу чего снабжены индексом 101. В дальнейшем на сайте появятся углубленные курсы с индексами 201 и 301, сообщил изданию *eWeek* Ховард Шмидт, исполнительный директор SAFECode, а в прошлом советник по вопросам кибербезопасности в администрации Белого дома. "Важно, чтобы ИТ-менеджеры, которые сами, может быть, и не занимаются разработками, но управляют коллективами программистов, хорошо понимали, что вопросы безопасности нельзя откладывать на потом и заниматься ими необходимо с самого начала проекта", — пояснил он.

Спонсором программы обучения является компания Adobe, которая в 2009 г. выступила со своей инициативой в области обеспечения безопасности ПО. Компания пересмотрела собственные практики разработки и сосредоточилась на том, чтобы затруднить злоумышленникам использование ее широко распространенных продуктов Acrobat и Flash для атак на системы пользователей.

Samsung рекомендует Windows 8.

SAMSUNG

Samsung ATIV smart PC Pro

Мощность ноутбука. Свобода планшета.

Свобода и удобство планшета в сочетании с функционалом мощного ноутбука: процессор Intel® Core™ i5 третьего поколения — в тонком и легком корпусе, с ярким сенсорным FullHD-экраном с диагональю 11,6", полной поддержкой Windows-программ, включая Microsoft Office, рукописным вводом с пером (S Pen) и 8* часами работы на одной зарядке. ATIV Smart PC Pro — незаменимый планшетный ПК для работы и развлечений!

Конфигурация и комплект поставки зависят от конкретной модели планшетного ПК.

*Время работы на батарее указано по результатам теста MobileMark (МобайлМарк) и может зависеть от конфигурации, настроек и запущенных приложений.

Красивая, быстрая, плавная Windows 8

ATIV – Art of Technology, Inspiration of Versatility*.
*Искусство Технологий, Безграничные Возможности. Smart PC – Умный ПК, Pro – Профессиональный, FullHD – высокая четкость. Товар сертифицирован. Реклама.

СОДЕРЖАНИЕ

№ 13 (833) • 21 МАЯ, 2013 • Страница 4

НОВОСТИ

ЭКСПЕРТИЗА

ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ

НОВОСТИ PC WEEK/RE — в App Store и Google Play

PC Week/RE в App Store

PC Week/RE в Google Play

Чтобы ознакомиться с последними публикациями сайта PC Week Live, читатели нашего издания, имеющие смартфоны или планшеты под управлением Apple iOS и Google Android, могут воспользоваться бесплатным мобильным приложением PC Week/RE. Приложение открывает доступ как к материалам уже выпущенных бумажных номеров PC Week/RE, так и к ежедневно обновляемой онлайновой ленте. И главное — почитать их можно в любое удобное время и в любом месте даже в отсутствие качественной связи (в офлайне), если предварительно вы потратите пару минут, чтобы запустить приложение и загрузить свежие публикации.

Приложение можно скачать из онлайновых магазинов App Store и Google Play, воспользовавшись, например, представленными QR-кодами.

PC WEEK REVIEW: ИТ-БЕЗОПАСНОСТЬ

УПОМИНАНИЕ ФИРМ В НОМЕРЕ

БЛОГОСФЕРА PCWEEK.RU

Ни слова о BlackBerry

Сергей Бобровский,
pcweek.ru/mobile/blog

В наших рейтингах постоянно висят материалы, посвящённые айфонам, андроидам и Windows-гаджетам. Давайте попробуем восстановить справедливость и посмотрим на другие мобильные платформы. Правда, смотреть сегодня особо и нечего: кроме iOS, Android и Windows Phone, на рынке не осталось почти ничего.

Как-то ещё мало-мальски заметно живут только Symbian и BlackBerry (RIM), хотя и их доли тают. Впрочем, в абсолютных цифрах продажи этих ОС несильно отличаются от Windows Phone, которую не упоминает только ленивый. При этом Symbian была фактически официально похоронена Nokia в нынешнем январе и сейчас поддерживается лишь формально. Остаётся только BlackBerry, которая за год потеряла львиную долю и без того маленькой своей части, а ведь лет пять-семь назад любой американский менеджер рангом чуть выше среднего считал обязательным иметь именно этот гаджет — за счёт непревзойдённой безопасности и иных удобных корпоративных фишек (рыночная доля RIM составляла тогда 46%!). Барак Обама, кстати, и по сей день использует телефон BlackBerry.

Однако списывать RIM со счетов пока рано, потому что она в этом году выпускает два устройства, Z10 и Q10, под управлением новой OS 10, фактически поставив "на десятку" всё. Дальше — либо долгожданная стабильность, либо банкротство.

OS 10 принципиально отличается от предыдущих ОС RIM. Она основана на полноценной версии ОС PB QNX, купленной RIM в 2010-м и хорошо известной разработчикам АСУ ТП и встраиваемых систем, включая военные. Программировать для OS 10 можно на Си/C++ в переделанной среде Eclipse (QNX Momentics IDE); BlackBerry API весьма хорош и поддерживает как уже знакомые BB-программистам легаси-интерфейсы, так и новые возможности. Имеются и высокоуровневые расширения наподобие WebWorks (Sencha Ext JavaScript API) для разработки на HTML5/JavaScript. Прямая поддержка OS 10 обещана в кросс-платформенных движках Unity и Marmalade.

Ситуация у RIM с её OS 10 в точности такая же, как у Microsoft с Windows Phone 8: удастся ли привлечь разработчиков, появится ли для неё достаточно софта? И тут RIM придерживается определенной тактики: "В целях привлечения сторонних разработчиков приложений под BlackBerry 10 гарантируется, что каждый девелопер заработает как минимум 10 тыс. долл. от торговли программой за первый год её выставления на витринах BlackBerry App World. Если сумма поступлений от продаж приложения окажется меньше названной суммы, компания выпишет чек на эту разницу. Программа, понятно, не может быть абсолютно бесполезным софтверным мусором — она должна принести своему автору хотя бы тысячу долларов, чтобы попасть под условия гарантий"…

Регулирование Интернета в мире. Сопоставление по странам

Денис Воейков,
pcweek.ru/gover/blog

РАЭК опубликовал результаты своего исследования международных тенденций регулирования и саморегулирования Интернета в различных странах мира. Выводы выглядят весьма обобщенно, но, возможно, прессе разослали какой-то усеченный вариант.

Лично мое внимание привлекло деление стран на группы в зависимости от принятой в них модели регулирования. В данном плане, как и ожидалось, меньше всего свобод в Иране и Китае. Несколько больше в Саудовской Аравии, ОАЭ, Йемене, Бирме, Вьетнаме, Пакистане, Омане, Узбекистане, Сирии, Тунисе, Бахрейне и, что весьма неожиданно, в Южной Корее. Может быть, ее просто с Северной перепутали?

Далее идет группа стран, где фильтры блокируют небольшое количество специфических сайтов в одной-единственной или в нескольких категориях, — Азербайджан, Казахстан, Таджикистан, Индия, Сингапур, Германия, Франция, Австралия, Малайзия и, кстати, Белоруссия.

Отсутствие каких бы то ни было режимов фильтрации на государственном уровне или на уровне провайдера, поощрение саморегуляции на уровне конечного пользователя отмечено в США, Великобритании, Дании, Финляндии и Венесуэле.

Ну а для России специалисты РАЭК придумали специальную категорию. У нас применяются "гибкие тактические механизмы фильтрации": существует набор заготовленных планов обеспечения информационной безопасности, включающих шаблоны фильтрации, которые активируются исходя из конкретной военной и политической обстановки. Профили могут быстро модифицироваться и настраиваться на конкретный контент.

Кстати, данная категория находится как бы всего в одном шаге от группы стран с полной свободой…

Big Data — это глобальная тенденция или "голый король"?

Андрей Колесов,
pcweek.ru/its/blog

Тема Big Data уже несколько лет (кстати, сколько — два или три года?) присутствует на ИТ-рынке как отражение одной из ведущих тенденций в области современных ИТ, занимая, наверное, третью позицию по популярности после облачности и мобильности. Но насколько этот тренд действительно глобален и долгосрочен? Возможно (или скорее всего), долгосрочным он действительно является. А вот по поводу его глобальности (широты использования) есть большие сомнения.

На мой взгляд, пока тема Big Data выглядит скорее "модной", нежели "актуальной". А "модность" сопровождается известным эффектом "голого короля", когда участники разговоров на тему уже просто не могут сказать ничего, кроме "да, конечно, классно и очень нужно". Хотя при этом зачастую возникает ощущение ситуации, описанной в известном анекдоте:

— Вы Хемингуэя читали?

— Да, но только не помню, кто автор…

Надолго ли воспарит Adobe в Creative Cloud?

Сергей Свинарев,
pcweek.ru/business/blog

"Всё, это конец! Никогда не думал, что компания, в которой работает так много талантливых людей, добровольно совершит коммерческий суицид". Это одна из далеко не самых резких реплик, появившихся в форумах вслед за "революционным" пересмотром компанией Adobe своей лицензионной политики. Начиная с июня она прекращает продажи лицензий всех продуктов, входящих в пакет Adobe Creative Suite (включая и суперпопулярный Photoshop), предлагая своим клиентам перейти в так называемый Creative Cloud и платить 50 долл. в месяц за право использовать любые продукты этого пакета по подписке. Облачное название Creative Cloud способно ввести в заблуждение: на самом деле кроме подписки и удаленного хранилища контента здесь ничего облачного нет. Сами приложения предоставляются не в виде услуги (SaaS), а, насколько можно понять, устанавливаются и работают на клиентских машинах.

Достоинства у такой модели, несомненно, есть, но о них говорят в основном представители самой Adobe. Цена лицензии всего пакета Adobe Creative Suite 6 Master Collection довольно велика (в России — около 95 тыс. руб.), а потому переход на помесячную оплату для многих окажется более удобным. Теперь не будет "торжественных" обновлений версий: новые функции станут добавляться по мере их разработки. Просматривать и редактировать файлы, находящиеся в облачном хранилище, можно с разных устройств (ноутбук, десктоп, планшет, смартфон). Появляется возможность организации распределенной коллективной работы над контентом.

Чем же недовольна общественность? Раньше вы могли купить, к примеру, Photoshop и, если его функциональность вас устраивает, не переходить на новые версии и не платить за апгрейды. Теперь такой возможности не будет: как только перестал платить, прекращай пользоваться программой. А что делать, если у вас к этому времени накопился архив материалов, созданных инструментами Adobe и нуждающихся в дальнейшей обработке, не требующей новых функций? Многих не устраивают цены: если платить 600 долл. в год, то за десять лет набежит 6 тысяч. Учитывая, что из полутора десятков приложений Creative Suite большинство клиентов использует одно-два, большого энтузиазма такая перспектива не вызывает. Для недовольных оставлена возможность использовать последнюю "традиционную версию" Adobe Creative Suite 6 по старой схеме, но эта версия не будет развиваться и поддерживаться. А потому рано или поздно решение принимать придется. Каким оно будет?..

От базовых задач до важнейших бизнес-приложений. Серверы IBM System x легко справятся с любой рабочей нагрузкой

Нет двух компаний с одинаковыми требованиями к ИТ. Поэтому IBM предлагает новую линейку серверов System x, предназначенных для обработки рабочих нагрузок, начиная от простых задач и до сложных облачных бизнес-приложений. Эти серверы на базе новейших процессоров Intel® Xeon® серий E5-2600 и E5-2400 допускают настройку конфигурации: заказчик может выбрать компоненты, необходимые ему сегодня, и впоследствии добавлять новые по мере изменения задач, стоящих перед компанией. Кроме того, бизнес-партнеры IBM могут помочь в выборе сервера в соответствии с конкретными потребностями и дополнить решение подходящей системой хранения данных, сетевыми средствами и программными решениями IBM, что позволит действительно оптимизировать ИТ-инфраструктуру.

Новая линейка настраиваемых серверов для решения задач вашей компании.

IBM System x3550 M4 Express

От 118 016 руб.*

P/N: 7914K3G

- Один процессор Intel® Xeon® E5-2630 6C с тактовой частотой 2,3 ГГц и кеш-памятью 15 МБ с частотой 1333 МГц (95 Вт)
- Память 16 ГБ (два модуля RDIMM[1] емкостью 8 ГБ (2Rx4, 1,35 В, 1333 МГц))
- Внешний отсек для подключения 2,5-дюймовых твердотельных дисков SAS[2]/SATA[3] с функцией горячей замены
- Контроллер MS110 (512 МБ флеш), устройство записи дисков, два блока питания с функцией горячей замены – 2x550 Вт
- Гарантия – 3 года

IBM System Storage DS3500 Express

От 157 648 руб.*

P/N: 1746-xxx

- 1 или 2 контроллера
- Кеш-память – 2/4 ГБ
- Внешние интерфейсы – SAS[2] 4/8 портов 6 ГБ/с, 8 портов FC[4] 8 ГБ/с, iSCSI[5] 8 портов 1 ГБ/с или 4 порта 10 ГБ/с
- До 192 дисков
- Flash/VolumeCopy[6], Dynamic Disk Pooling[7], расширенная удаленная репликация, монитор производительности, опция повышения производительности по требованию
- 3,5- и 2,5-дюймовые диски
- Гарантия – 3 года

IBM System x3500 M4 Express

От 75 008 руб.*

P/N: 7383K3G

- Один процессор Intel® Xeon® E5-2620 6C с тактовой частотой 2,0 ГГц и кеш-памятью 15 МБ с частотой 1333 МГц (95 Вт)
- Память 8 ГБ (один модуль RDIMM[1] емкостью 8 ГБ (2Rx4, 1,35 В, 1333 МГц))
- Внешний отсек для подключения 2,5-дюймовых твердотельных дисков SAS[2]/SATA[3] с функцией горячей замены
- Контроллер M5110 (512 МБ кеш с батареей), устройство записи дисков, два блока питания с функцией горячей замены – 2x750 Вт
- Гарантия – 3 года

Убедитесь сами

Новый инструмент подбора серверов IBM System x поможет выбрать подходящий сервер и сэкономить средства.

ibm.com/systems/ru/express1

Обратитесь в службу IBM Express Advantage для поиска ближайшего к вам бизнес-партнера IBM:

8 800 2006 900

[1] RDIMM – регистровый модуль памяти с двусторонним расположением микросхем. [2] SAS – последовательный интерфейс. [3] SATA – последовательный интерфейс IDE (IDE – параллельный интерфейс подключения накопителя). [4] FC – волоконно-оптический канал. [5] iSCSI – интерфейс малых вычислительных систем, предназначенный для передачи данных посредством межсетевого канала. [6] VolumeCopy – функция, обеспечивающая полную репликацию одного логического тома на другой. [7] Dynamic Disk Pooling – объединение дисков в единый виртуализованный ресурс хранения данных. Заменяет собой стандартную RAID-группу, повышает надежность, производительность и скорость восстановления после ошибки.

* Все указанные цены – рекомендованные розничные цены для базовой конфигурации, приведены исключительно для информационных целей и не являются офертой. Цены не включают в себя 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. IBM, логотип IBM, ibm.com, System Storage, System x, Express Advantage, FlashCopy, ServerProven, ClusterProven являются товарными знаками или зарегистрированными товарными знаками International Business Machines Corporation в США и/или других странах. Список товарных знаков, зарегистрированных IBM на настоящий момент, представлен по адресу www.ibm.com/legal/copytrade.shtml. Intel, Intel logo и Xeon являются товарными знаками либо зарегистрированными товарными знаками, права на которые принадлежат корпорации Intel или ее подразделениям на территории США и других стран. Наименования других компаний, продуктов и услуг могут быть товарными знаками или знаками обслуживания третьих лиц.

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
Шеф-редактор группы ИТ
Р. ГЕРР

Редакция

Главный редактор
А. МАКСИМОВ
1-й заместитель главного редактора
И. ЛАПИНСКИЙ
Научные редакторы:
В. ВАСИЛЬЕВ,
Е. ГОРЕТКИНА, Л. ЛЕВИН,
О. ПАВЛОВА, С. СВИНАРЕВ,
П. ЧАЧИН
Обозреватели:
Д. ВОЕЙКОВ, А. ВОРОНИН,
С. ГОЛУБЕВ, С. БОБРОВСКИЙ,
А. КОЛЕСОВ
Специальный корреспондент:
В. МИТИН
Корреспонденты:
О. ЗВОНАРЕВА, 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
Группа компьютерной верстки:
С. АМОСОВ, А. МАНУЙЛОВ
Техническая поддержка:
К. ГУЩИН, С. РОГОНОВ
Корректор: И. 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.

HP Networking стремится стать SDN-лидером

ЛЕВ ЛЕВИН

Ник Уотсон, вице-президент HP Networking по региону EMEA, заявил в Москве, что его компания надеется в течение ближайших двух лет увеличить свою долю на рынке Ethernet-коммутаторов корпоративного класса до 20%. По его словам, сейчас на долю HP приходится 12% этого рынка и после приобретения в 2010 г. компании 3Com она уверенно занимает второе место после корпорации Cisco, которую надеется потеснить с помощью своей стратегии внедрения программно-конфигурируемых сетей (software defined networks, SDN), анонсированной осенью прошлого года.

СЕТИ

Одной из своих основных задач Александр Столяров считает повышение узнаваемости бренда HP Networking в российских регионах

Основная идея SDN состоит в том, чтобы переложить на ПО большинство функций управления сетями, которые обычно обеспечиваются на уровне коммутаторов и маршрутизаторов и до сих пор осуществлялись отдельными устройствами сетевой инфраструктуры. Многие специалисты рассматривают SDN как следующий шаг в процессе виртуализации инфраструктуры современных ЦОДов вслед за виртуализацией их серверов и систем хранения. IDC прогнозирует, что к 2016 г. по мере роста потребностей в масштабируемости и программируемости корпоративных сетей рынок SDN-решений вырастет почти до 2 млрд. долл.

Стоит отметить, что концепцию SDN активно используют Cisco и другие поставщики оборудования для сетей Ethernet. Например, недавно Dell представила свою реализацию SDN на основе "активной фабрики" из модульных коммутаторов.

Руководитель подразделения сетевых решений HP в России Александр Столяров привел некоторые данные о текущем положении HP Networking на российском рынке. Компания контролирует около 20% сектора Ethernet-коммутаторов корпоративного класса, который в прошлом году вырос на 16% — до 348 млн. долл. В секторе маршрутизаторов уровня предприятия доля HP составляет порядка 6%, но объем этого сектора существенно меньше — 81 млн. долл., причем за 2012 г. он вырос только на 8%. В относительно недавно возникшем сегменте беспроводных решений для корпоративных заказчиков, объем которого в 2012 г. составил 36 млн. долл., HP пока занимает лишь четвертое место. Стоит отметить, что в нашей стране за 2012 г. этот сегмент вырос только на 11%, в то время как в мире он увеличился на 20%. По итогам прошлого года у HP Networking в России было более тысячи заказчиков (стоит учитывать, что часть из них достались HP в наследство от 3Com) и 87 специализированных партнеров.

Сетевая фабрика Dell из модульных коммутаторов

ЛЕВ ЛЕВИН

В середине апреля компания Dell представила свои новые решения, предназначенные для построения сетей ЦОДов и основанные на технологиях приобретенного ею два года назад производителя Ethernet-коммутаторов старшего класса Force10 Networking. Сегодня администраторы ЦОДов сталкиваются с рядом сетевых проблем в связи с широким внедрением серверной виртуализации, значительно повышающей сетевой трафик и меняющей его характер, переходом серверов на 10-гигабитный Ethernet и конвергенцией сетевых технологий LAN и SAN, а также с растущей популярностью концепции программно определяемых сетей (software defined network, SDN).

РЕШЕНИЯ

Предлагаемая Dell "активная сетевая фабрика" Active Fabric реализует "плоскую" архитектуру сети SDN с альтернативными маршрутами (multipath) и соединениями any-to-any, которая достаточно гибка для растущих объемов горизонтального трафика в виртуализованных ЦОДах и частных облаках. Active Fabric строится с помощью легко развертываемых и масштабируемых коммутаторов фиксированной конфигурации 10 Gigabit Ethernet/40 Gigabit Ethernet (10GbE/40GbE) с низкими задержками при передаче пакетов и высокой плотностью размещения портов. Как утверждает Dell, использование этих компактных устройств вместо традиционных шассийных коммутаторов ядра сети сокращает на 59% расходы и на 77% энергопотребление сетевого оборудования ЦОДа, а также упрощает обслуживание сетевой инфраструктуры ЦОДа.

Для автоматизации управления своей фабрикой Dell выпустила программную утилиту с графическим интерфейсом пользователя Active Fabric Manager, в состав которой входит программа-мастер для проектирования сети и инструменты для быстрого развертывания спроектированной конфигурации, а также для управления и мониторинга сети. Вместе с этой утилитой было представлено первое устройство для построения активной фабрики Dell Networking S5000 — коммутатор 10GbE/40GbE класса top-of-rack (т. е. размещаемый вверху серверной стойки) для конвергированных сетей LAN/SAN с "родной" поддержкой технологий сетей хранения Fibre Channel (FC) и Fibre Channel over Ethernet (FCoE).

Выполненный в однюнитовом конструктиве Dell Networking S5000 состоит из четырех модулей, причем коммутатор можно приобретать даже с одним модулем и постепенно наращивать его конфигурацию по мере расширения сети. Его максимальная конфигурация состоит из 64 портов 10GbE либо 48 комбинированных портов Ethernet/FC плюс 16 портов 10GbE, а также четырех 40-гигабитных портов Ethernet для подключения к сети ЦОДа. По данным Dell, этот коммутатор по плотности размещения портов в 1,3 — 2,6 раза превосходит шассийные коммутаторы Cisco Nexus 5548 и Brocade VDX 6730. Он работает под управлением разработанной Force10 Networking операционной системы FTOS и поддерживает различные протоколы сетей хранения, включая iSCSI, RoCE (RDMA over Converged Ethernet), Fibre Channel, FCoE, а также NAS.

HP представляет коммутаторы FlexFabric

ЛЕВ ЛЕВИН

Компания Hewlett-Packard анонсировала новую серию продуктов и решений для построения программно-определяемых сетей (SDN) ЦОДов на основе концепции "гибкой фабрики" FlexFabric, которые должны усилить ее портфель оборудования для ЦОДов, куда также входят ее серверы, системы хранения и ПО управления инфраструктурой.

ЦОДЫ

Шассийный коммутатор уровня ядра сети HP FlexFabric 12900 заменит HP 12500, разработанный H3C еще до того, как HP купила компанию 3Com в 2010 г. Он выпускается в двух модификациях с 10 и 16 отсеками для плат, в которых воздух в шасси идет соответственно от передней панели к задней (модель 12910) и между боковыми панелями (модель 12916). В максимальной конфигурации этот продукт обеспечивает производительность коммутации до 36 Тбит/с, перенаправление (forwarding) до 19,2 млрд. пакетов в секунду и поддерживает до 768 портов 10 Gigabit Ethernet либо 256 портов 40 Gigabit Ethernet (в ближайшем будущем HP планирует реализовать для него и поддержку до 64 стогигабитных портов Ethernet).

Шассийный коммутатор HP FlexFabric 12900 поддерживает до 768 десятигигабитных портов либо 256 сорокагигабитных

Как утверждает производитель, FlexFabric 12900 является первым в индустрии коммутатором уровня ядра сети, в котором реализована поддержка используемого в сетях SDN протокола OpenFlow. Для решения проблемы масштабирования сетевой фабрики ЦОДа в нем применяются сетевые стандарты Transparent Interconnection of Lots of Links (TRILL) и Shortest Path Bridging, которые постепенно заменяют классический протокол Spanning Tree (стоит отметить, что аналогичные коммутаторы Cisco и других ведущих вендоров сетевого оборудования поддерживают только один из этих новых стандартов).

Новый коммутатор HP поддерживает оба варианта открытых стандартов для конвергированных сетей — Data Center Bridging и Fibre Channel over Ethernet (FCoE). Как утверждает вендор, в отличие от аналогичных шассийных коммутаторов уровня ядра сети от Cisco продукт HP не требует приобретения дополнительных лицензий на использование расширенных функций коммутации.

Коммутатор уровня агрегирования сети FlexFabric 11908, также поддерживающий OpenFlow, обеспечивает подключение по десяти- или сорокагигабитному Ethernet для блейд-серверов HP BladeSystem c-Class, оборудованных модулями Virtual Connect FlexFabric. Этот коммутатор обеспечивает неблокирующую пропускную способность до 7,7 Тбит/с и масштабируется до 384 портов 10 Gigabit Ethernet либо 64 портов 40 Gigabit Ethernet. Как и старшая модель серии FlexFabric, он поддерживает TRILL, Shortest Path Bridging, Data Center Bridging и FCoE.

Компания также представила программный пакет виртуального коммутатора FlexFabric Virtual Switch 5900v, который при использовании в комбинации с новым аппаратным коммутатором уровня агрегирования трафика сети FlexFabric 5900 класса top-of-rack (ToR) реализует для среды виртуальных машин VMware такой функционал, как политики и управление качеством сервиса. Интегрированная в FlexFabric Virtual Switch технология Integrated Virtual Ethernet Port Aggregator (VEPA) обеспечивает перенос некоторых функций коммутатора с сервера на физический коммутатор. Маршрутизатор виртуализованных сервисов HP Virtualized Services Router (VSR) доставля-

SAP предлагает облачный хостинг на платформе HANA

СЕРГЕЙ СВИНАРЕВ

Незадолго до своей ежегодной конференции SAPPHIRE NOW, которая запланирована на середину мая, компания SAP объявила о доступности нового облачного сервиса SAP Hana Enterprise Cloud, призванного предоставить клиентам удаленный доступ к хранилищу данных под управлением SAP NetWeaver Business Warehouse, а также к приложениям SAP ERP и SAP CRM на базе СУБД реального времени SAP HANA. Если вспомнить, что облачная парадигма в сегменте ответственных бизнес-приложений приживается с большим трудом, такой шаг SAP выглядит весьма революционно. Но дьявол, как всегда, в деталях.

СЕРВИСЫ

Вишал Сикка: "При расчете стоимости сервиса SAP Hana Enterprise Cloud будут компенсироваться затраты заказчика, сделанные им при покупке традиционных лицензий"

На самом деле речь не идет о предоставлении прикладного ПО как услуги (SaaS): клиентам предлагается удаленная платформа на основе SAP HANA, на которой они могут запускать свои системы. Подчеркнем: именно свои. Заказчик должен уже иметь купленные лицензии на ПО SAP; более того, приложения к моменту переноса в облако должны быть развернуты и настроены на его площадке (модель, названная по аналогии с BYOD, — BYOL, Bring Your Own Licence). Как поясняет SAP, миграция приложения в облако включает три этапа. Сначала совместно с экспертами вендора проводится обследование ИС заказчика, используемых в ней данных и приложений с тем, чтобы определить, какие из них получат наибольший выигрыш от перемещения в HANA Enterprise Cloud. Затем с помощью специалистов SAP осуществляется процесс адаптации и миграции, после чего начинается продуктивная эксплуатация с оплатой по подписке, размер которой будет определяться используемыми приложениями, объемом обрабатываемых данных и масштабом решения. По сути речь идет о хостинге платформы, который не вполне соответствует определению PaaS.

Не ясно, в частности, насколько указанная платформа эластична и способна оперативно и гибко подстраиваться к потребностям клиентов. Руководители SAP подтверждают, что многоарендность (multitenancy) в ней не поддерживается, и связано это с тем, что multitenancy не реализована в базовых продуктах SAP. Казалось бы, эластичность и масштабируемость — это проблемы SAP, выступающей в качестве сервис-провайдера. Однако вендор намерен разрешить предоставление услуг HANA Enterprise Cloud и своим партнерам, располагающим необходимыми ресурсами в собственных дата-центрах. Финансовые и организационные моменты соответствующей партнерской программы должны быть обнародованы на SAPPHIRE NOW. Следует иметь в виду, что облачному провайдеру услуг HANA Enterprise Cloud следует располагать парком сертифицированных программно-аппаратных комплексов HANA, а не просто массивом стандартных серверов и систем хранения. Кроме того, сервис-провайдер, будь то SAP или ее партнер, должен взять на себя заботы по управлению облачным решением.

Объясняя свой шаг, руководители SAP отмечают большой интерес к платформе HANA со стороны заказчиков, которым наряду с традиционной моделью развертывания теперь будет доступна и облачная. Разумеется, вариант облачного хостинга для сомневающегося клиента менее рискован (в случае неудачи можно вернуть решение в привычную среду на собственной площадке), но следует признать, что клиент при этом как бы рискует дважды — переходя на неизвестную ему платформу СУБД и вынося ответственное приложение в облако. Говоря о невысокой совокупной стоимости владения облачным решением, директор SAP по технологиям Вишал Сикка пообещал, что при расчете стоимости сервиса будут компенсироваться затраты заказчика, сделанные им при покупке традиционных лицензий. Он сообщил также, что около шестидесяти компаний уже используют сервис SAP Hana Enterprise Cloud, а сорок ISV-разработчиков приступили к созданию собственных приложений для этой платформы.

ет сервисы непосредственно на виртуальную машину, которая их запросила, с помощью программно-реализуемой технологии операторского класса Network Function Virtualization (NFV). VSR заменяет специализированное оборудование для доставки сервисов, за счет чего высвобождается часть пространства ЦОДа.

Коммутатор HP FlexFabric 5900 предназначен для установки в серверной стойке

Физический маршрутизатор HP HSR 6800 для сетей WAN консолидирует в одном устройстве функции маршрутизации, межсетевого экрана и построения виртуальных частных сетей VPN. Он обеспечивает производительность 2 Тбит/с на уровне backplane и пропускную способность маршрутизации 420 Мбит/с. Маршрутизатор поддерживает до 32 10-гигабитных портов Ethernet и быстрое восстановление соединения с помощью функции HP Intelligent Resilient Framework (IRF).

HP предварительно анонсировала и новое ПО из серии HP Intelligent Management Center (IMC), которое она разработала для администрирования сетей SDN. Пакет IMC Virtual Application Network Resource Automation Manager предоставляет шаблоны сетевых сервисов, упрощающие конфигурирование сети, а IMC SDN Manager обеспечивает мониторинг и управление политиками в сетях ЦОДов, кампусов и филиалов компаний.

Поставки коммутаторов FlexFabric 12900 и FlexFabric Virtual Switch 5900V начнутся в октябре, FlexFabric 5900 уже продается в США по цене от 14 990 долл., FlexFabric 11908 будет доступен для заказа в июне (цена начальной конфигурации — 83 тыс. долл.), маршрутизатор HP HSR 6800r поставляется по цене от 46 тыс. долл. Выпуск HP Virtualized Services Router запланирован на второе полугодие, а HP IMC Virtual Application Network Resource Automation Manager и HP IMC SDN Manager выйдут в декабре.

Windows 8.1...

ПРОДОЛЖЕНИЕ СО С. 1

речь идет именно о пакете обновлений, было изначально понятно из простых соображений "здравого смысла": хорошо известно, что качественно новый вариант ОС не может делаться быстрее, чем за три-четыре года. Точнее, сделать-то его, вероятно, и можно, но только это будет резко противоречить принципам функционирования ИТ-рынка.

Интерес к теме выпуска обновленной настольной ОС Microsoft конечно же вызван тем, что все это направление, бывшее в свое время фундаментом "империи Microsoft" и до сих пор остающееся одним из краеугольных камней бизнеса корпорации, переживает сложный период. Причем нет никакого сомнения, что это отлично понимают и в самой Microsoft, ведь еще осенью 2011 г. CEO компании Стив Балмер заявил, что Windows 8 — это один из самых рискованных проектов корпорации за все годы ее существования. При этом имелось в виду, что в данном продукте будет совершена серьезная коррекция курса развития настольных ОС компании и что от успеха проекта во многом зависит будущее корпорации в целом.

То, что речь идет именно о пакете обновлений, было изначально понятно из простых соображений "здравого смысла": хорошо известно, что качественно новый вариант ОС не может делаться быстрее, чем за три-четыре года. Точнее, сделать-то его, вероятно, и можно, но только это будет резко противоречить принципам функционирования ИТ-рынка.

Насколько успешным оказался проект? Прошло уже более полугода после начала его "рыночной жизни", но однозначного ответа на этот вопрос так и нет. С одной стороны, по оценкам аналитиков, Microsoft пока явно не смогла выйти на заметные позиции в области планшетов, никакого прорыва тут не произошло. С другой — из отчетов компании видно, что финансовые результаты деятельности Windows-направления весьма позитивны, в чем-то даже лучше, чему у Windows 7, рыночный успех которой никем не подвергается сомнениям.

Но, может быть, ожидавшегося публикой "переворота" на планшетном фронте не могло произойти в принципе, во всяком случае быстро, и успехом является уже то, что компания смогла "зацепиться за плацдарм", и теперь, переведя дух, выполнив перегруппировку сил и введя в сражение свежие резервы, Microsoft начнет генеральное наступление?

За неделю до официального объявления о названии Windows 8.1 на сайте Microsoft было опубликовано интервью Тами Реллер (вопросы задавал PR-сотрудник Microsoft), которое ряд западных, а затем и российских СМИ интерпретировали как "признание провала Windows 8". На самом деле топ-менеджер сказала лишь о проблемах с восприятием рынком новой ОС и о маркетинговых ошибках в деле продвижения этого продукта со стороны Microsoft, но ни о каком провале речи там не было.

В начале мая Тами Реллер обещала, что в Windows Blue будут изменены ключевые элементы операционной системы, но в чем именно заключается такая коррекция, не уточнила. Аналитики и СМИ тоже не могут предложить своих версий развития продукта Microsoft и в качестве главного шага возможной модернизации называют возвращение на рабочий стол интерфейса кнопки "Пуск". Согласно такой логике следующим революционным ходом могло бы стать изменение фона этой кнопки с синего цвета на зеленый…

Ни о каких технических подробностях Windows 8.1 не говорится и в бостонском заявлении Microsoft, но уже по тому факту, что речь идет именно о бесплатном обновлении для текущей версии Windows 8, можно сделать вывод, что состав новшеств будет носить скорее косметический характер, характерный для SP1. Однако нужно отметить, что Microsoft еще раз подтвердила свой курс на интеграцию мира настольных ПК с планшетными возможностями: "Windows 8 была построена для тех пользователей, которые хотят объединить сферы своей деловой деятельности и личной жизни. Эта ОС определяет вектор нашего развития от традиционных ПК в сторону мобильных вычислений".

EMC призывает...

ПРОДОЛЖЕНИЕ СО С. 1

что именно виртуализация стала той революционной технологией, которая, создав качественно новый изолирующий слой между традиционными ОС и аппаратными вычислительными средствами, позволила реализовать идею программно-конфигурируемых (software defined) дата-центров, в свою очередь являющихся основой ИТ-платформы 3-го поколения.

На этой схеме с копьем новая компания Pivotal не была нарисована, но развивая подобную аллегорию, наверное, ее можно было бы представить в виде чудесного меча, который должен помочь EMC достичь новых вершин в иерархии мировой ИТ-отрасли, а ее клиентам — выйти на новый уровень эффективности бизнеса. Важность этого проекта для ECM и VMware представляется вполне очевидной, и актуальность темы была еще раз продемонстрирована на конференции: вторая половина пленарной части была посвящена именно планам действий Pivotal, о которых подробно рассказал ее руководитель Пол Мариц.

Он обстоятельно разъяснил аудитории, что новая, облачно-мобильная эпоха развития ИТ требует создания качественно новой ИТ-платформы, которая должна при этом решать две взаимосвязанные задачи: поддержку унаследованных систем и создания новых, изначально ориентированных на облачно-мобильную архитектуру их применения. Пол Мариц пояснил, что создаваемая его компанией платформа — она уже получила название Pivotal One — базируется на пяти основных принципах: открытые стандартны и открытое ПО, дата-центрическая архитектура, поддержка широкого спектра облачных платформ, дружественность для разработчиков и дружественность для заказчиков. В ее состав войдут три основных набора компонентов для работы с облачной инфраструктурой (Cloud Fabric), с приложениями (Application Fabric) и данными (Data Fabric). И все это — не отдаленные планы, а очень близкие перспективы: по мнению руководителя Pivotal почти все компоненты платформы уже доступны на рынке, нужно лишь увязать их в единый набор, дополнив еще рядом средств. Как уверил Пол Мариц, новая система Pivotal One будет доступна в конце текущего года.

Пол Мариц: "Рынок требует создания ИТ-платформ третьего поколения, которые соответствовали бы сегодняшним и завтрашним вызовам времени"

Разумеется, помимо общего анализа ситуации на рынке и обнародования планов действий EMC на конференции был сделан и целый ряд вполне конкретных анонсов. Так, была впервые представлена новая платформа для программно-определяемого хранилища (Software-Defined Storage Platform) ViPR, которая появится на рынке во второй половине этого года. По мнению EMC, уникальность данного решения заключается в возможности одновременно управлять инфраструктурой хранения данных (уровень управления) и данными, размещенными в этой инфраструктуре (уровень данных). При этом для традиционных рабочих нагрузок контроллер EMC ViPR использует существующую инфраструктуру хранения, а для рабочих нагрузок следующего поколения выделяет новые объектные сервисы данных ViPR (с доступом через API-интерфейсы Amazon S3 или HDFS). Объектные сервисы данных ViPR интегрируются с OpenStack через Swift и могут выполняться в корпоративном или стандартном хранилище данных. EMC ViPR обеспечивает прозрачную интеграцию с программно-определяемым ЦОДом VMware через стандартные отраслевые API, а также обеспечивает совместимость с платформами Microsoft и OpenStack.

Важные обновления и новые возможности интеграции реализованы для систем хранения данных EMC VMAX, VPLEX и RecoverPoint, а также для корпоративного гибридного облачного решения хранения данных EMC Syncplicity. На конференции было объявлено о завершении трансформации всего портфеля приложений управления содержанием, предоставляющего заказчикам надежный набор средств для реализации стратегий перехода на облачные технологии. Были анонсированы новые продукты, дополнившие портфель решений Documentum, включая официально выпущенное на рынок решение EMC Documentum EMA (Enterprise Migration Appliance).

На конференции впервые было сказано о начале подготовки новой версии операционной системы OneFS для горизонтально масштабируемой NAS-системы EMC Isilon. Это ПО должно расширить возможности текущего варианта OneFS 7.0, выпущенного в конце прошлого года, в том числе в плане использования потенциала больших данных. Новая версия будет включать функции дедупликации, аудита и обеспечения безопасности, а также усовершенствования для объектно-ориентированного хранилища, Hadoop HDFS 2.0 и корпоративного сервиса общего онлайн-доступа к файлам Syncplicity.

Уже доступны новый пакет EMC Service Assurance Suite и обновленный вариант пакета EMC Storage Resource Management Suite для управления ИТ-ресурсами, которые обеспечивают полную прозрачность инфраструктур хранения данных, сетей и вычислений, поддерживая при этом интеграцию с EMC ViPR. Кроме того, было объявлено о выпуске пакета Data Protection Suite, который упрощает приобретение, внедрение и использование решений EMC для резервного копирования и архивирования.

Точки доступа...

ПРОДОЛЖЕНИЕ СО С. 1

Wi-Fi для подключения пользовательских устройств, высокопроизводительных ноутбуков и специализированного отраслевого оборудования (например, кассовых терминалов или беспроводных медицинских приборов).

Эти устройства входят в состав унифицированной беспроводной сети Cisco (Cisco Unified Wireless Network, CUWN), поддерживающей до 72 000 беспроводных точек доступа с полной мобильностью на третьем сетевом уровне OSI в центральных и удаленных зонах, в том числе в корпоративных штаб-квартирах, отделениях компаний и на других удаленных площадках.


Точки доступа Aironet 2600i/2600e

CUWN представляет собой, по утверждению представителей компании, гибкую, надежную и масштабируемую архитектуру для безопасной доставки мобильных услуг и приложений. Эта архитектура обеспечивает минимальную совокупную стоимость владения и защищает инвестиции заказчика благодаря легкой интеграции с существующей проводной сетью.

В 2010 г. ужесточились требования к точкам доступа Wi-Fi, ввозимым на территорию РФ. По российским законам, отмечает Михаил Кадер, инженер-консультант Cisco, на каждую партию одного и того же продукта, ввозимого на территорию нашей страны, нужна лицензия Минпромторга. Ежемесячно ввозятся тысячи точек доступа, и если сегодня оформляется партия в 20 штук, ей нужна лицензия Минпромторга, завтра оформляется партия еще в 30 штук, ей нужна еще одна лицензия и т. д. Это постоянная головная боль для компании.

В результате создания собственного производства в России упрощается процедура ввоза таких изделий и сокращаются сроки поставки с двух с половиной месяцев до трех недель. Кроме того, госструктуры испытывают повышенное доверие к оборудованию, собранному в стране. И это открывает дополнительные возможности для новых контрактов. Уже с сентября нынешнего года все точки доступа Aironet 2600i/2600e, заказанные в России, не будут ввозиться из-за рубежа, а будут собираться в РФ.

Вдохновляем на яркие впечатления

Картриджи XL помогают вам экономить

до **50%** **ЭКОНОМИИ** на печати одной страницы*

you can**

Canon

* На основе исследования Canon, по сравнению PG-440XL и CL-441XL с эквивалентными не XL картриджами Canon, при использовании стандарта заполнения страницы ISO/IEC24712

canon.ru/XL

** Вы можете. Реклама

"Самое сложное — научить ИТ-специалистов слушать пользователей"

ИНТЕРВЬЮ

*В рамках нашей традиционной рубрики "Кто он, современный ИТ-руководитель?" мы, как правило, обсуждаем технологические и управленческие аспекты использования ИТ в организации. Однако, как известно, любая компьютерная система — всего лишь инструмент, эффективность применения которого зависит от людей. То, как пользователи воспринимают внедряемые технологии, насколько быстро и легко их осваивают и как активно встраивают их в свою повседневную деятельность, не может не сказываться на конечном результате. Именно вопросы взаимоотношений ИТ-специалистов с представителями бизнес-подразделений стали предметом беседы менеджера по стандартизации ИТ-процессов в департаменте информационных технологий группы компаний "Дикси" **Дмитрия Мельникова** с научным редактором PC Week/RE **Ольгой Павловой**.*

Дмитрий Мельников

PC Week: Вы ведете семинары на тему, как построить правильное управление сервисами в ИТ-службе. А как вы сами стали экспертом в этой области?

ДМИТРИЙ МЕЛЬНИКОВ: До 1994 г. я служил офицером АСУ в Вооруженных силах РФ. Мой "гражданский" путь в ИТ начался в 1997 г. с работы в одном из московских банков, в то время ни о каких ИТ-сервисах речь вообще не велась. В 2000-м я перешел на Лианозовский молочный комбинат (компания "Вимм-Билль-Данн"), а чуть позже туда пришла ИТ-команда, перед которой стояла задача внедрения сервисной модели путем надлежащего построения ИТ-процессов. Я занимал пост руководителя отдела техподдержки, и для нас весь этот сервисный подход представлялся чем-то необычным, непонятным. Изначально мы воспринимали его в штыки. Перестройка шла с трудом, но именно тогда мое мировоззрение стало меняться, я понял, что если я, как руководитель, постигну тонкости методологии ITIL, то и подчиненные смогут разобраться.

В 2005 г. я ушел из "Вимм-Билль-Данна", сменив впоследствии несколько организаций, среди которых были компания "Связной", организации Департамента градостроительной политики города Москвы, проектный институт и, наконец, компания "Дикси", где я тружусь и по сей день. И везде я в той или иной степени занимался внедрением сервисного подхода: организовывал сервис-деск, развертывал систему управления сервисами, выстраивал ИТ-процессы.

Параллельно с приобретением практического опыта я много читал. Всё началось с книги Джона Хувера "Как работать на идиота", которую мне порекомендовал один из знакомых ИТ-директоров. За нею последовали "Переговоры, которые работают. 12 стратегий, которые помогут вам получить больше в любой ситуации" Стюарта Даймонда и целый ряд других. Эта литература помогла мне "встряхнуться" и понять, что для успешного внедрения сервисного подхода в организации требуется некий особый подход к людям, а для этого прежде всего надо изменить самого себя. Решив найти что-нибудь на данную тему в Интернете, я провел целое исследование, которое, к сожалению, закончилось неудачей. Я не нашел там ничего, касающегося психологических аспектов внедрения информационных систем, не говоря уже о внедрении сервисной модели. Более того, у меня сложилось убеждение, что многие ИТ-специалисты, в частности руководители ИТ-проектов, ИТ-менеджеры и иногда ИТ-директора, рассматривают вопросы применения информационных технологий исключительно с технической стороны. При этом полностью забывая о людях, что, с моей точки зрения, и ведет к непониманию между бизнесом и ИТ.

PC Week: В чём же проявляется такое непонимание?

Д. М.: Я сейчас работаю в сфере розничной торговли и периодически провожу аудит процесса предоставления ИТ-услуг магазинам. Часто я сталкиваюсь с тем, что люди, являющиеся большими профессионалами в области продаж, но имеющие небольшие познания в ИТ, боятся обращаться к ИТ-специалистам за помощью. На вопрос, почему они не жалуются руководству, если что-то сделано не так, ответ обычно бывает один: "Лучше не надо, мы сейчас сами как-нибудь попробуем сделать, а то в следующий раз нам придется еще неизвестно сколько ждать айтишников".

Такая ситуация, к сожалению, наблюдается во многих организациях. Чтобы ее исправить, надо прежде всего научить пользователей взаимодействовать с ИТ-специалистами, то есть объяснить им, что те — тоже люди, с которыми можно и нужно нормально решать вопросы. С другой стороны, необходимо донести до сознания ИТ-специалистов, что пользователи вовсе не обязаны отлично знать информационные технологии и они также требуют нормального к себе отношения.

Вместе с тем я считаю, что определенная доля вины за сложившуюся пропасть между ИТ-специалистами и пользователями зачастую лежит на руководящих сотрудниках в ИТ. Да, конечно, проблема ИТ-кадров существует везде, но нельзя позволять айтишнику вести себя так, как будто он главный в организации. Не он приносит прибыль компании, и не надо бояться ставить его на место, опасаясь, что он возьмет и уволится.

PC Week: Что еще, на ваш взгляд, могло бы помочь убрать это противостояние между пользователями и ИТ-специалистами?

Д. М.: С людьми надо разговаривать. И совсем не обязательно для этого где-то собираться. ИТ-руководителям надо выходить с предложениями об организации встреч с пользователями прямо у них в кабинетах. Пусть это будет "классный час", мини-тренинг, пятиминутка — называйте как угодно. Встречи на 10—20 минут в удобное время между ИТ-сотрудниками и пользователями в рамках определенной, наболевшей тематики. Их результатом могут стать конкретные предложения по решению каких-то вопросов, получение новой, порой не видной внутри подразделений информации. В конце концов, люди будут просто знакомиться друг с другом, а это уже много значит.

PC Week: Исходя из вашего опыта, в чём вы видите основные проблемы внедрения сервисного подхода?

Д. М.: Самые первые проблемы возникают еще на этапе описания бизнес-процессов. Как правило, пользователям удобнее, чтобы нажимать меньше кнопок и система работала сама собой. Это реализуемо, если процесс типовой. Его легче формализовать и спустить до нужного исполнителя. Но так бывает не всегда. Поэтому наилучший вариант для пользователей — это подкованный, грамотный сотрудник первой линии поддержки, который всё им расскажет и не будет двадцать раз переводить от специалиста к специалисту.

Так что на данном этапе не надо бросаться покупать некую программу, а сначала стоит разобраться, для чего она нужна и что она даст. Необходимо провести аудит текущего состояния процесса и найти общий язык с внутренним заказчиком. Причем проводить аудит лучше силами специалистов своего ИТ-подразделения в плотной связке с заказчиком. Надо, правда, быть осторожными в отношении внешних консультантов. Они, конечно, нужны, чтобы рассказать теорию, подсказать, как лучше решить ту или иную задачу, но они чаще всего приходят с типовыми решениями. Я работал в абсолютно разных сферах, и везде требуется серьезная адаптация под специфику конкретного бизнеса.

Следующая проблема внедрения сервисного подхода заключается в том, что не всё можно автоматизировать. Сегодня можно нередко наблюдать, как из сервис-деска пытаются сделать систему контроля за подчиненными. Это вообще разные вещи, их нельзя путать. Нельзя целью перехода к сервисной модели ставить только управление ИТ-специалистами. Нельзя допускать, чтобы ИТ работали только ради ИТ. Для бизнеса это никакой пользы не принесет.

PC Week: При внедрении сервисного подхода с кем проще находить общий язык — с ИТ-специалистами, людьми, принимающими решения, или с конечными пользователями?

Д. М.: Мне, наверное, повезло, что все реализованные мною проекты имели поддержку со стороны бизнеса, по крайней мере соответствующее ПО было уже приобретено и его надо было внедрить.

Поэтому я убежден, что, приступая к проекту по внедрению сервисной модели, надо заходить со стороны бизнеса. Следует объяснить собственникам, во что они вкладывают деньги, и тогда, если решение будет принято, его просто-напросто заставят выполнить. Иногда бывает, что ИТ-директору сервисный подход не нужен — по его мнению, всё и так построено и хорошо работает. Для него система управления сервисами — дополнительная нагрузка, поскольку эту систему надо сначала внедрить, а затем — управлять ею.

С пользователями находить общий язык проще, если им внятно объяснить, что они получат в результате. Я обычно начинаю с вопроса: "Вам всё нравится в качестве предоставляемого сервиса?". И в ходе беседы, понимая "больные" места в обслуживании пользователей, уже начинаю рассказывать о "лечении" с помощью внедрения сервисного подхода. Но обязательно с реальными примерами!

Если же говорить об ИТ-специалистах, то тут нужны веские доводы. Аргументы консультантов и тренеров не всегда и не полностью достигают цели. Французский философ XVI века Блез Паскаль писал: 'Доводы, до которых человек додумывается сам, обычно убеждают его больше, нежели те, которые пришли в голову другим". Поэтому ИТ-руководителю необходимо понять, к каким доводам он должен подвести свою команду.

PC Week: Как вы считаете, почему в России так медленно идет внедрение сервисного подхода в ИТ?

Д. М.: Прежде всего мне хотелось бы отметить однобокое соблюдение соглашений, причем на разных уровнях. У нас руководители, как правило, не соблюдают SLA, и редкий ИТ-директор осмелится предпринять какие-либо действия, идущие вразрез с пожеланиями топ-менеджмента. Например, представьте, что в московском офисе согласован перерыв в связи на четыре часа, вызванный ремонтом почтового сервера в соответствии с условиями SLA. Вдруг в это время генеральному директору срочно понадобится отправить почту! Как он отнесется к тому, что простой системы согласован? Ответ, по-моему, очевиден. А вот за рубежом SLA соблюдаются обеими сторонами, и я сам видел это на практике.

Другая причина — отсутствие качественной рекламы. Нужна не реклама какого-либо конкретного продукта, а нужно четкое объяснение на простом языке, доступном для любого человека, что сервис-деск — это точка входа, которая ответит на любые ваши вопросы. А вот то, как сегодня сплошь и рядом реализован сервис-деск, — просто анахронизм. Вы звоните, например, в банк, а вам в ответ предлагают сначала нажать "1", затем — "2" и т. д. Такой сервис-деск никому не интересен.

PC Week: А можно ли посчитать результаты внедрения сервис-деска?

Д. М.: Это сложный вопрос, над которым бьются многие консультанты. Лично для себя я понял, что как только мы уходим от хаоса в приеме заявок и упорядочиваем их, так сразу же освобождаем ресурсы, хотя это и не является основной целью внедрения сервисного подхода. Например, в проектном институте мы научились управлять рабочим временем сотрудников, более того, мы научились не обманывать пользователей. Они понимали, что если в ответ на свою заявку получают сообщение типа "Вам все отремонтируют до 13:00", то именно так и будет. Следовательно, они могли планировать свое рабочее время, что косвенно вело к уменьшению простоев сотрудников.

Что же касается денежного эквивалента, то здесь результат не столь очевиден. Но, например, в том же проектном институте только за счет организации управления выдачей картриджей нам удалось сэкономить за год порядка 3 млн. руб.

PC Week: Все эти результаты видны только после того, как сервис-деск уже заработал. А какие доводы следует приводить руководству, когда вы пытаетесь убедить его в необходимости внедрения сервисного подхода?

Д. М.: Для убеждения я использую следующий план. Сначала найдите "больное" место и предложите соответствующее лекарство, причем обязательно с реальным примером его действия. Затем дайте его попробовать, то есть проведите "тест-драйв". Но помните, что не надо ничего "впаривать" — дождитесь, пока сами попросят. После этого надо всё "разжевать", уделяя особое внимание ключевым аргументам. Во-первых, сервисный подход обеспечивает минимизацию прямых потерь, в том числе сокращение времени вынужденного простоя персонала по техническим причинам. Во-вторых, благодаря управлению сервисами все бизнес-пользователи всегда будут знать, когда их запрос будет выполнен, причем в утвержденные ими же сроки. В-третьих, ни одна заявка не будет потеряна. В худшем случае она будет отклонена, но только с объяснением причин. В-четвертых, сервисная модель помогает в планировании бюджета.

Исходя из специфики бизнеса, аргументы могут быть разные. Не вызывает никакого сомнения, что такие предложения покажутся привлекательными для бизнеса. Конечно, здесь может встать во-

ПРОДОЛЖЕНИЕ НА С. 12 ▶

Как выжить и преуспеть в эпоху BYOD

ДАН МИЛЛЕР

Безумие под названием "принеси на работу свое устройство" (BYOD) начинается с появлением каждого нового поколения смартфонов, планшетов или мобильных операционных систем. Сотрудники, выбравшие себе нового идеального электронного помощника, не желают на работе пользоваться технологией, которую считают допотопной.

Они хотят получать немедленный доступ к людям, информации и прочим ресурсам, необходимым для выполнения своих задач, и в свою очередь сами хотят быть доступными для других в любом месте и в любое время. Это, во-первых, означает использование собственных устройств как на работе, так и вне ее. А во-вторых, что надежность сети становится важной, как никогда, но основная масса работников воспринимает это как нечто само собой разумеющееся.

Исчез утверждаемый ИТ-менеджерами список допустимых приложений для мобильных устройств. Вместо него действуют следующие правила.

1. Признайте, что у каждого есть своя любимая игрушка. Такие мобильные устройства, как смартфоны и планшеты, часто адаптируются к потребностям владельца и становятся жизненно важны для него.

2. Упростите процесс обнаружения и добавления функций. Используемое компанией решение для управления мобильными устройствами должно поддерживать приложения сотрудников в актуальном состоянии, обеспечивать их безопасность и совместимость.

3. Применяйте большие данные и аналитику для прогнозирования и повышения производительности труда. С помощью персональных сведений и метаданных (тегирование концепций и т. д.) можно повышать производительность труда рабочих групп и отдельных сотрудников и более жестко управлять проектами, в работе над которыми они применяют свои мобильные устройства.

4. Соблюдайте баланс безопасности и удобства использования. Каждое устройство представляет уникальную угрозу для целостности сети. Действуйте в трех направлениях: одни устройства относятся к одобренной платформе и полностью поддерживаются, другие поддерживаются на уровне приложений, но не на уровне устройств, третьи поддерживаются на платной основе с последующим возмещением затрат.

5. Защитите свои сети. Когда сотрудники находят новое применение взаимодействию с помощью мобильных устройств и приложений для них, они ожидают, что будет использоваться единая сеть, работающая без сбоев и задержек. А значит, гарантированная работа сети имеет важнейшее значение не только для мобильных устройств, но и для применяемых во взаимодействии между людьми систем бэк-офиса и баз данных.

Показатели эффективности BYOD

Практически для всех корпоративных операций разработаны ключевые показатели эффективности (key performance indicator, KPI), на основании которых менеджеры узнают, всё ли у них функционирует должным образом. Для понимания состояния BYOD тоже необходимы KPI. Если нужно использовать новейшие устройства, в компании следует изучить, как быстро это можно сделать и насколько прост будет доступ к приложениям для них.

Компании, допускающие BYOD, должны измерять скорость и эффективность процедур аутентификации. Это можно сделать посредством эмпирического наблюдения или опроса сотрудников, позволяющего определить степень их удовлетворенности и эффективность работы.

В IP-сетях часто трудно бывает обеспечить высокий уровень доступности и надежности при управлении непредсказуемым и весьма непостоянным трафиком. Тестирование, мониторинг и коррекция — вот постоянные процессы, с помощью которых можно заметно повысить качество сети.

Среди KPI, подлежащих мониторингу, отметим дрожание фазы (особенно при передаче голоса и видео в реальном времени), скорость передачи в обоих направлениях, задержки установления сессий и обрывы связи. Непрерывное тестирование и мониторинг обеспечивают эффективное распределение доступной пропускной способности и успешное предоставление услуг.

Главный измеряемый показатель — качество обслуживания сотрудников ИТ-подразделением. В начале 2012 г. Cisco изучила тенденции виртуализации рабочих столов в компаниях США и пришла к выводу, что BYOD позволяет сократить затраты на одного работника на 300—1400 долл., а главными преимуществами BYOD являются рост производительности труда и удовлетворенность сотрудников работой. Масштабная программа гарантии качества способна избавить от сложностей и поднять эффективность труда.

BYOD — это надолго. Позитивный момент заключается в том, что благодаря поддержке этой концепции ИТ-подразделения получают возможность разрабатывать новые приложения, повышающие надежность, безопасность и производительность сети.

Внутренняя ставка как инструмент оценки эффективности собственного ИТ-подразделения

ВСЕВОЛОД КРАСИН, ИЛЬЯ СНИГИРЕВ

Сегодня многие компании задаются вопросом, как можно оценить эффективность работы собственных ИТ-служб. Этот вопрос тем более актуален, чем более "ИТ-чувствителен" бизнес компании. При этом, если для оценки качества и удовлетворенности пользователей ИТ-сервисами, предоставляемыми ИТ-подразделением, существует целый ряд методик, то относительно оценки эффективности работы самого ИТ-подразделения пока нет единства мнений.

Исходя из нашего опыта, одним из параметров оценки эффективности собственных ИТ-подразделений большой компании может являться внутренняя ставка ИТ-сотрудников. Кажется, что понятие "ставка сотрудника" применимо только к отдельным ИТ-компаниям, однако это не совсем так. Ставку ИТ-сотрудника можно рассчитать и для внутреннего ИТ-подразделения компании. При этом у руководителей ИТ-отделов и руководителей компании появляется возможность сравнить свои внутренние ставки со ставками сервисных ИТ-компаний.

В данной статье мы попытаемся проанализировать, как именно с помощью ставки сотрудника можно оценивать эффективность ИТ и насколько применим расчет и процессы управления ставкой для внутреннего ИТ-подразделения, а не для отдельной компании.

Подход к расчету ставки

Так что же такое ставка ИТ-сотрудника и как она рассчитывается. В рыночных ИТ-компаниях ставка сотрудника рассчитывается следующим образом:

Ставка = ставка себестоимости × норма прибыли × премия за риск.

Здесь:

Ставка себестоимости = расходы на содержание ИТ-подразделения/количество сотрудников/утилизация.

Утилизация = оплачиваемое время ИТ-сотрудника/общее количество рабочего времени ИТ-сотрудника.

Для внутреннего ИТ-подразделения формула расчета ставки видоизменяется:

Ставка = ставка себестоимости ~~× норма прибыли × премия за риск~~.

Данное обстоятельство вызвано тем, что сотрудники внутренних служб не ориентированы на получение прибыли с заказчика, таким образом ставка ИТ-сотрудника внутреннего подразделения равна ставке себестоимости данного сотрудника. Кроме этого утилизация сотрудников внутренних ИТ-подразделений стремится к 100%, так как внутренним ИТ-подразделениям, в отличие от рыночных компаний, при расчете ставки нет необходимости закладывать риски, связанные с отсутствием продаж в конкретный момент времени.

Расходы на содержание являются наиболее сложным и неоднозначным для расчета показателем. В основном это связано с двумя причинами. Во-первых, расходы на содержание сотрудников включают как прямые, так и косвенные расходы, и если с прямыми расходами все более или менее понятно, то какие именно косвенные расходы необходимо включать в расчет ставки — это большой вопрос. В наших расчетах мы стараемся учитывать максимальное количество статей косвенных расходов, включая, например, офисные расходы, распределение расходов на содержание административно-хозяйственных подразделений, расходы на проведение корпоративных мероприятий и т. д. Во-вторых, далеко не во всех компаниях внутренняя финансовая отчетность позволяет выявить и выделить из общего числа расходов именно те, которые можно аллоцировать на ИТ-сотрудников. Так, во время нашего недавнего проекта в одной крупной российской организации, нам предоставили информацию о том, что средний расход ИТ-сотрудника на мобильную связь составляет 1,5 руб. в месяц, притом что почти у каждого сотрудника головного офиса, к которому относится и ИТ-отдел, есть оплачиваемый мобильный телефон. Столь маленькая сумма поставила под сомнение корректность данных, предоставляемых нам в ходе проекта. В последующем наша догадка подтвердилась. Оказалось, что в автоматизированной системе финансового учета данной организации просто напросто не существует необходимых аналитик, позволяющих получить качественную информацию для расчета ставки. Случай с мобильными телефонами довольно прост и очевиден. Все мы владеем мобильными телефонами и примерно понимаем, сколько могут стоить услуги связи. По остальным статьям расходов это сделать гораздо сложнее. Так что же делать, если в компании недостаточно аналитических данных, которые могут быть использованы для расчета стоимости сотрудника? С одной стороны, по наиболее непрозрачным из них можно использовать примерные рыночные оценки. С другой — можно сформировать эти показатели совместно с сотрудниками финансовых служб, и это поможет повысить прозрачность расходов.

Важно отметить, что общепринятые подходы к расчету ставки рыночных ИТ-компаний помимо коэффициентов прибыли и рисков зачастую подразумевают включение дополнительных коэффициентов, таких как утилизация и доля неоплачиваемого персонала. Данные коэффициенты позволяют ИТ-компаниям увеличивать ставку, обеспечивая необходимый уровень дохода, тем самым покрывать расходы на выполнение их сотрудниками функций, ценность которых для заказчика неочевидна. Примерами таких функций могут быть: выполнение внутренних проектов ИТ-компании, контроль качества, линейное руководство, отпуска, больничные, время, в которое сотрудник не занят, и т. д. Увеличение ставки за счет использования такого рода коэффициентов необходимо учитывать при сравнении ставок внутреннего ИТ-подразделения со ставками коммерческих ИТ-компаний, например при попытке сопоставить косвенные расходы.

Ставка и эффективность расходов на ИТ

Практически все более-менее крупные ИТ-проекты и активности перед началом реализации проходят оценку целесообразности на основе инвестиционного анализа. Любой, даже самый простой метод данного анализа базируется на оценке предстоящих расходов. Ставка сотрудника внутреннего подразделения позволяет более полно оценивать стоимость инвестиций. Стоимость услуг внешних консультантов, интеграторов и аутсорсеров обычно учитывают при расчете стоимости проекта, стоимость собственного персонала — не всегда. Даже если стоимость участия собственных ИТ-специалистов учитывается, то зачастую это происходит только в части зарплаты без учета прочих расходов, которые компания вынуждена нести для обеспечения работы сотрудника. Речь идет о расходах на содержание офиса, административно-хозяйственных расходах, расходах на медицинское страхование и т. д.

Использование ставки сотрудника позволит более точно оценить расходы и соответственно сделать выводы о том, целесообразно ли вообще реализовывать данную активность, оправдывает ли она вложения, как лучше ее выполнить, самостоятельно или с помощью субподрядчика, каков приоритет данной задачи по отношению к другим и т. д. Помимо этого при правильном клиентоориентированном подходе к обсуждению целесообразности и методов выполнения задач ИТ-подразделением само оно имеет шанс повысить в глазах бизнеса уровень удовлетворенности своей деятельностью. Добиться этого будет нелегко. Возможно, понадобится изменить корпоративную культуру ИТ-сотрудников, сделать ее более клиентоориентированной, правильно выстроить систему мотивации, добиться прозрачности в расходах на ИТ и т. д. Однако запуск механизмов обсуждения целесообразности (инвестиционной привлекательности) задачи с использованием ставки может стать одним из элементов повышения удовлетворенности бизнеса работой ИТ-подразделения, а следовательно, и эффективности этого подразделения.

Ставка и прозрачность расходов на ИТ

Одной из причин, по которой собственники и бизнес могут быть не довольны деятельностью ИТ-отдела, — отсутствие прозрачности в расходах. Проще говоря, собственники и бизнес хотят получить ответ на вопрос: на что конкретно тратятся деньги?

И если затраты на оборудование и услуги сторонних организаций достаточно прозрачны, как понятна и привязка этих затрат к конкретным задачам и результатам, то привязать затраты на ИТ-сотрудников к решаемым ими задачам (т. е. понять, сколько стоит выполнение той или иной задачи силами собственного ИТ-отдела) бывает достаточно сложно.

Любой ИТ-руководитель должен понимать, что для его компании стоимость содержания ИТ-подразделения складывается не только из заработной платы и премии сотрудников. Помимо оплаты труда компания несет расходы по размещению и содержанию рабочего места, приобретению компьютеров и другого оборудования, лицензий на ПО и т. д. В ходе исторического развития ИТ-подразделения сумма таких расходов может достигать существенной доли в бюджете всей компании, становится непрозрачной для ее руководителей и собственников. Бизнес понимает важность ИТ, понимает, что ИТ-сотрудники заняты решением тех или иных задач, однако зачастую не может ответить на вопросы, чем конкретно они занимаются и не платит ли бизнес слишком много за содержание ИТ-подразделения.

Так как же ставка сотрудника может повлиять на достижение прозрачности расходов на ИТ?

Во-первых, определенный уровень прозрачности появится уже за счет обсуждения необходимости выполнения той или иной задачи, в сравнении с оценкой стоимости ее выполнения и проведения оценки эффективности по инвестиционным принципам.

Во-вторых, сам механизм расчета и управления ставкой основан на анализе и контроле расходов, включаемых в ставку сотрудников. Расчет ставки влечет за собой необходимость появления специальных аналитик в финансовом учете, а следовательно, и возможность получения финансовых отчетов о деятельности ИТ-подразделений с глубокой детализацией расходов. В-третьих, наличие ставки как параметра оценки стоимости услуг собственного ИТ-подразделения поможет более точно распределить расходы ИТ на конкретные текущие задачи. В случае использования внутренней ставки инвестиции компании в решение этих задач обретут понятное руководству выражение.

В то же время хотелось бы предостеречь читателя от концентрации на финансовой составляющей как на единственном инструменте оценки эффективности ИТ-подразделений. Исходя из нашего опыта, внутренние ИТ-подразделения выполняют ряд задач, для которых чрезвычайно трудно найти заказчика со стороны. В этом случае у руководства компании будет периодически возникать вопрос, зачем нужно тратить деньги на эти задачи. Очевидно, что существует ряд задач, которые необходимо решать для обеспечения стабильности ИТ-систем и их развития. Это в том числе интеграционное тестирование, поддержка актуальной технической документации, обучение сотрудников, участие в конференциях и т. д. Отказ от решения этих задач приведет к тому, что в течение непродолжительного времени ИТ-системы и ИТ-подразделения потеряют способность адекватно поддерживать текущие и перспективные потребности бизнеса.

Обобщая все вышеизложенное, можно утверждать, что на фоне все более пристального внимания к эффективности внутренних ИТ-подразделений внутренняя ставка сотрудников является весьма интересным показателем, позволяющим сравнить различные варианты развития собственного ИТ-подразделения. Но не стоит забывать, что помимо финансовых показателей при рассмотрении различных вариантов развития и выборе, скажем, между реализацией проектов собственными силами или силами подрядчика нужно принимать во внимание множество других факторов. Такими факторами в первую очередь будут наличие уникальной собственной экспертизы по имеющимся системам, знание специфики работы бизнеса и наличие выстроенных отношений с бизнесом.

Об авторах: Всеволод Красин — директор практики бизнес-консалтинга AT Consulting, Илья Снигирев — ведущий менеджер направления организационного консалтинга AT Consulting.

"Самое сложное...

◀ ПРОДОЛЖЕНИЕ СО С. 10

прос денег — ведь любое внедрение требует затрат. Но тщательно взвесив все "за" и "против", изучив, что конкретно входит в стоимость решения, ответ, скорее всего, будет в пользу реализации проекта.

PC Week: Заставляет ли внедрение сервисного подхода людей меняться?

Д. М.: Меняться — это, наверное, громко сказано. Если говорить о пользователях, то сервисная модель заставляет их поиному относиться к своим запросам. Они уже не пишут что попало, стараются более понятно изложить свою проблему. Помимо этого сервисная модель дисциплинирует, что в первую очередь касается ИТ-специалистов. Меняются правила "игры", правила оказания услуг. Взаимодействие пользователей и ИТ-специалистов становится прозрачным, чего, собственно говоря, бизнес постоянно и требует. Для того чтобы это взаимодействие было наиболее эффективным, очень важно слышать друг друга. А это самое сложное для любого человека — уметь слушать других.

PC Week: Спасибо за беседу.

ТОНКИЙ КЛИЕНТ GP3300 E5 НА БАЗЕ ПРОЦЕССОРА Intel® Atom™ D2550

БЕЗОПАСНОСТЬ. КОМПАКТНОСТЬ. УПРАВЛЯЕМОСТЬ.

● Является оптимальной платформой по соотношению цены и качества для построения корпоративных сетей и удовлетворяет требованиям самого разного уровня.

● Тонкие клиенты AK-Systems на базе процессора Intel® Atom™ D2550 с минимальным энергопотреблением обеспечивают высокую производительность, а также гарантируют скорость, гибкость и безопасность сети.

процессор:
Intel® Atom™ D2550, 1.86GHz
чипсет:
Intel® NM10
оперативная память:
до 8GB
Внутренний накопитель:
до 1 TB
(flash или HDD)
операционная система:
Windows CE70 (поддержка Remote FX)
Windows Embedded Standard 7
(Поддержка Remote FX)
Windows XP Embedded
Linux Embedded

115093 • Москва • ул. Павловская, д. 27/29
e-mail: sales@ak-systems.ru
тел./факс: (495) 221 6488 • www.ak-systems.ru

"Нам нужно было адекватно и быстро реагировать на новые вызовы"

Основной темой конференции компании VMware "К эре пост-ПК через облака", прошедшей в Москве в конце марта, было обсуждение предложений компании для работы в клиентской ИТ-среде, в том числе представление новых возможностей пакета VMware Horizon Suite. Однако как раз за неделю до этого мероприятия стало известно о серьезной корректировке объединенного стратегического курса EMC+VMware в направлении дальнейшего освоения облачной ИТ-сферы. Поэтому именно с этого вопроса началась беседа вице-президента VMware по региону Центральной Европы ***Томаса Кулевайна*** *с обозревателем PC Week/RE* ***Андреем Колесовым****.*

ИНТЕРВЬЮ

Томас Кулевайн

PC Week: Как вы оцениваете изменения, произошедшие на рынке облачных вычислений за последние годы?

ТОМАС КУЛЕВАЙН: Прежде всего нужно сказать, что облачные вычисления — это новая модель использования ИТ, основанная на новых архитектурно-технологических принципах. И мы с удовлетворением констатируем, что VMware внесла, можно сказать, решающий вклад в реализацию этой концепции, поскольку одной из ключевых облачных технологий является виртуализация, которая позволила вывести на качественно иной уровень решение задачи независимости ПО от используемых аппаратных средств. И как первопроходец на современном рынке виртуализации для x86-систем мы хорошо осознаем и свою ответственность за развитие данного направления ИТ. Эта ответственность проявляется, в частности, в том, что мы должны быстро и эффективно реагировать на изменения рыночной ситуации, на потребности наших клиентов, анализировать появление трудностей и препятствий на этом пути и, конечно, предлагать решение возникающих проблем.

Говоря о прогрессе в области облаков, нужно сказать, что, возможно, самым показательным является неуклонное смещение спектра востребованных клиентами облачных сервисов от инфраструктурных к прикладным, от IaaS к SaaS. Я думаю, что именно соотношение инфраструктурные/прикладные сервисы — важный индикатор уровня зрелости облачного направления. И если посмотреть на пример нашей компании, то хорошо видно, как сфера нашей деятельности также смещалась именно в эту сторону.

Главным итогом последних лет в облачной сфере является то, что этап пилотного опробования данных моделей и технологий в целом уже заканчивается, накоплен достаточно большой отраслевой опыт, на основании которого можно говорить о надежности и безопасности облаков, об их эффективности для бизнеса. Хотя, конечно, нужно понимать, что универсальной эффективности не бывает, всегда есть оптимальные границы применимости тех или иных средств. Нам процесс такого освоения рынком новых технологий хорошо известен. Ведь виртуализацию тоже начали применять сначала разработчики и тестировщики ПО, потом она охватила продуктивные, но не очень важные для бизнеса приложения, затем — критически важные для предприятий системы. То же самое сейчас происходит с облаками — мы сейчас находимся перед началом переноса туда критически важных приложений.

Но такое изменение в использовании облаков, разумеется, накладывает и на нас, поставщиков, повышенные требования к качеству предлагаемых решений. Поэтому может показаться, что наши шаги от версии к версии не столь уж велики. Но на самом деле это не так: известно, что переход от уровня надежности 99,0 до 99,9 дается тяжелее, чем от 90 до 99. Так и в нашем случае.

Еще один важный аспект развития темы виртуализации. Как вы знаете, создание средств виртуализации для x86-архитектуры началось в конце 1990-х с персональных компьютеров, потом основной акцент был перенесен на серверы. Затем в конце прошлого десятилетия опять стала быстро расти значимость виртуализации для клиентских систем, но все же это были две как бы параллельные линии — клиентская и серверная. Сейчас можно говорить о существенном их переплетении в гибридном варианте облачных вычислительных сред.

PC Week: А что можно сказать о конкурентной ситуации на облачно-виртуализационном рынке? Я помню, как четыре-пять лет назад ведущие аналитики, вроде Gartner, предрекали, что с выходом в эту сферу группы ИТ-ветеранов (Microsoft, IBM, Oracle) "молодой" VMware вряд ли удастся удержать ведущие позиции. Но, кажется, прогнозы признанных ИТ-оракулов не сбываются…

Т. К.: Могу согласиться с вашими оценками и отметить, что последние два-три года уже не видно прогнозов, что кто-то другой займет лидирующую позицию в области виртуализации вместо VMware. Знаете, я пришел на работу в компанию примерно десять лет назад и на протяжении всего этого времени постоянно слышу вопросы типа: "Вы чувствуете конкуренцию со стороны Microsoft?", на которые столь же постоянно искренне отвечаю: "Не чувствую". Другой регулярный вопрос — в чем причина успеха VMware? Я думаю, что ответ тут кроется в том, что виртуализация, а теперь и облака — это наша ключевая специализация, наша целевая задача, решение которой подразумевает делать так, чтобы наши средства действительно приносили пользу заказчикам и были бы достаточно простыми в применении. А для многих наших конкурентов виртуализация — это все же, скорее, средство для решения несколько иных задач, что является в какой-то мере для них "тормозом" при движении в инновационном направлении. Разумеется, конкуренция в области серверной виртуализации растет, мы видим повышение значимости средств Open Source, но в целом лидирующие позиции VMware продолжают сохраняться, и я не вижу реальных угроз для них.

В области клиентских систем ситуация несколько иная. Тут мы, скорее, являемся атакующей стороной, а не обороняющейся. Пионером освоения идей исполнения клиентских приложения на серверной части была в свое время Citrix, и эта компания исторически занимает тут сильные позиции. Но мы уверены, что и здесь у нас есть возможность выйти в лидеры, потому что мы предлагаем во многом качественно иные технологии и подходы для решения подобных задач. Собственно, сама постановка вопроса в клиентской сфере выглядит сейчас совсем не так, как еще десять лет назад. Тогда речь шла во многом о необходимости поддержки унаследованных приложений и устройств. А сейчас сюда вторгаются не унаследованные, а наоборот — самые новейшие и самые разнообразные средства. Это уже совсем иная постановка задачи, в которой мы себя чувствуем на своей территории.

Что касается Microsoft, то мы считаем, что эта компания так и осталась в старом ИТ-мире, привязанной к Windows. Мы не видим, что она делает для клиентов, которые хотят жить в новой ИТ-реальности с наличием разнообразия устройств и программных платформ. Ситуация с Citrix видится иной. С целью решить проблемы гетерогенности компания приобрела множество технологий "точка-точка", решающих частные, а не общие задачи взаимодействия. Потом она их объединила в один набор, объявив интегрированным решением. Но пока это решение очень сложно и дорого в обслуживании, что не отвечает требованиям заказчиков. Кроме того, Citrix постоянно пытается перенести центр управления работой клиента на само клиентское устройство. Наш подход принципиально отличается: мы считаем, что управление данными и приложениями должны выполняться централизованно, что позволит в том числе делать это и самому пользователю, причем с любой точки доступа.

PC Week: В 2008-м VMware взяла курс на расширение своего присутствия на ИТ-рынке, в том числе за счет выхода в такие качественно новые для себя области, как прикладные решения и сервисы, но пока компания продолжает ассоциироваться в общественном ИТ-мнении с позицией именно "виртуализационного гиганта", причем во многом именно серверного. Что можно сказать о достижениях VMware в новых для нее видах деятельности? С какими проблемами тут столкнулась компания и как она их решает?

Т. К.: Да, несколько лет назад VMware качественно изменила свою стратегию развития, заявив о расширении сферы своих интересов. И можно точно сказать, что она очень многого добилась в реализации этих планов. Другое дело, что изменение имиджа компании, того, что о ней думает публика, это часто еще более сложный и долгий процесс, чем создание новых технологий и новых направлений деятельности. Примеры этому мы видим постоянно.

В 2008 г. компания взяла курс на выход за пределы традиционного позиционирования в качестве поставщика инфраструктурного ПО, пополняя арсенал своих предложений, в том числе за счет прикладных решений. В этом деле были заметные успехи, но стали нарастать и некоторые проблемы, причем больше не технического, а организационного характера. К тому же менялся сам рынок, его требования, и нам нужно было адекватным образом и быстро реагировать на новые вызовы.

Как вы знаете, еще в конце лета прошлого года было объявлено об изменениях в руководстве VMware, когда на смену Полу Марицу на пост CEO был назначен Пэт Гелсингер. Это была не просто ротация кадров, а начало серьезной коррекции облачно-виртуализационной стратегии, причем не только VMware, но в связке с корпорацией EMC. Чем закончилась эта коррекция курса, какие организационные формы они приобрела, было сказано в середине марта: сервисно-прикладное направление EMC и VMware теперь выделены в самостоятельную компанию Pivotal, которую возглавил Пол Мариц. В результате VMware как бы возвращается в более узкие рамки инфраструктурного ПО, но на самом деле это огромное поле деятельности, границы которого за последние годы сильно расширились и продолжают раздвигаться.

В этой инфраструктурной сфере мы видим для себя сейчас три основных направления работы. Первое — это реализация концепции программно-определяемых (software-defined) дата-центров, что на практике означает, что мы создаем полный слой абстракции прикладного ПО от аппаратных средств, добавляя к серверной виртуализации виртуализацию устройств хранения данных и сетей. Второе направление — системы для конечных пользователей. И третий вектор — это бизнес-модель гибридного облака, подразумевающая создание экосистемы облачных инфраструктурных сервисов от широкого круга независимых сервис-провайдеров, что обеспечит наличие конкурентной среды на рынке (а значит, борьбу за качество предложений и за снижение стоимости услуг), а для заказчика — еще и возможности выбора, отсутствия зависимости от конкретного поставщика.

PC Week: В марте VMware заявила, что все же решилась начать выступать на рынке в качестве поставщика собственных инфраструктурных сервисов, а не только как софтверный вендор. Что вы можете сказать о планах работы в этом направлении?

Т. К.: Это давно ожидаемый рынком шаг с нашей стороны, и это действительно серьезное для нас решение. Должен подчеркнуть, что оно вызвано совсем не намерением вторгнуться в новую для нас сферу деятельности и уж тем более не желанием отнять хлеб у наших партнеров. Это — требование рынка, причем в значительной степени со стороны не только клиентов, но и как раз партнеров, поскольку для создания таких глобальных инфраструктурных сервисов требуется решать серьезные, во многом качественно новые задачи, и мы должны показать, как это можно и должно делать собственным примером. Надо подчеркнуть, что при этом мы выводим на качественно другой уровень возможности построения гибридных систем, дополняя их глобальными сервисами под собственной торговой маркой.

Должен заметить, что появление наших сервисов ожидается в конце текущего года, конкретные схемы реализации бизнес-моделей, особенно на местных рынках, в том числе в России, еще только прорабатываются. Вполне возможен, например, такой вариант, когда мы будем продавать свои сервисы через партнеров.

PC Week: На каких вычислительных мощностях вы будете развертывать свои сервисы: в своих дата-центрах или на арендованной аппаратной инфраструктуре?

Т. К.: У нас пока нет точного ответа на этот вопрос, мы его сейчас прорабатываем. Возможно, будет использована и смешанная схема — что-то в своих ЦОДах, что-то в арендуемых. Но суть не в этом. Наша методология создания программно-определяемого дата-центра позволяет абстрагироваться от физической инфраструктуры и переводит вопрос "свой" или "арендуемый" ЦОД в разряд второстепенных. Главное то, что мы хотим предложить заказчикам нечто, соизмеримое по масштабам с сегодняшними сервисами Amazon, но в намного более расширенном варианте именно гибридной среды, в которой заказчик сможет перемещаться со своими виртуальными машинами между любыми ЦОДами — нашими, наших партнеров и собственными, выбирая наиболее подходящий именно для него вариант.

PC Week: Спасибо за беседу.

НПП и НФАП на распутье?

АЛЕКСАНДР ЧУБУКОВ

ГОСПРОЕКТЫ

Тема Национальной программной платформы (НПП) продолжает привлекать внимание ИТ-сообщества, несмотря на ослабевающий интерес к своему детищу со стороны родителя-государства. Именно поэтому ей был посвящен круглый стол "Национальная программная платформа, Национальный фонд алгоритмов и программ (НФАП), СПО vs. ППО", ставший одним из наиболее востребованных мероприятий апрельской конференции по свободному ПО ROSS'2013.

Владимир Рубанов: "В постановлении правительства о НФАП осталась лишь маленькая верхушка айсберга от пятилетних наработок"

На нем были заявлены позиции разных сторон отечественного ИТ-сообщества. К сожалению, с точкой зрения "хозяина" НПП — Минкомсвязи — познакомиться не удалось (ввиду отсутствия его представителей).

Модератор круглого стола Александр Айгистов, руководитель Российского агентства развития информационного общества (РАРИО), отметил, что за последнее время в рамках проекта НПП был реализован ряд инициатив в сфере СПО, связанных с развитием информационного общества в стране.

Дмитрий Комиссаров ("ПингВин Софтвер") напомнил, что пик развития НПП пришелся на 2011-й. Тогда по инициативе Минкомсвязи для реализации начальных этапов НПП, "сердцем" которой является НФАП и которая изначально базировалась на СПО, был запущен проект, успешно завершенный под эгидой РАСПО созданием прототипов ОС, систем сборки и т. п.

С тех пор государством, по его словам, больше не делалось ничего. Однако созданные в рамках проекта НПП прототипы ОС развивались в 2012 г. силами членов РАСПО, без участия государства.

В результате с помощью НФАП, в котором размещались созданные прототипы ОС, появилась возможность сборки разных дистрибутивов — "МСВСфера", ROSA и др. В перспективе, полагает он, разработчики смогут использовать системы автоматизированной сборки, в том числе для госпредприятий.

Как считает г-н Комиссаров: "В настоящий момент непонятны намерения и цели государства в отношении НПП и НФАП и не ясно, что будет, если государство повернется опять лицом к проблеме, — станет лучше или хуже. Быть может, стоит двигаться в выбранном направлении без государства? Ситуация неоднозначна и требует обсуждения".

Павел Фролов: "Для внедрения НПП понадобится лет пять на развертывание базовой инфраструктуры и столько же — на обучение персонала и решение проблем, которые вскроются при внедрении"

Павел Фролов ("ГНУ/Линуксцентр"), имеющий опыт внедрения фондов алгоритмов и программ (ФАП) в медучреждениях Минздрава, воспринимает создавшуюся ситуацию спокойно: "То, что сейчас буксует НПП, для меня не удивительно — это очень инерционный механизм. НПП — проект большой и неповоротливый, и в этом его слабость и его сила".

По его мнению, для внедрения НПП понадобится лет пять на развертывание базовой инфраструктуры и столько же — на обучение персонала и решение проблем, которые вскроются при внедрении. "Всем думающим специалистам очевидно, что это большой путь, и если взять известное распоряжение № 2299-р, то оно как раз и рассчитано на пять лет и заканчивается планированием мероприятий на следующее пятилетие", — добавил он.

Дмитрий Комиссаров: "При создании инфраструктуры НПП ни одно мероприятие более чем на 10% (по объемам работ) не выполнено"

Владимир Рубанов (РОСА), входящий в рабочую группу по этой проблеме, созданную при Минкомсвязи, отметил, что радикальные изменения с точки зрения перспектив развития НПП произошли в конце 2012 г. и связаны с инициативами нового руководства министерства. Тридцатого января этого года вышло Постановление Правительства РФ № 62 о НФАП, в котором, по его словам, "осталась маленькая верхушка айсберга от пятилетних наработок". Но даже эта верхушка полезна, считает он. Согласно данному постановлению с 1 мая планируется разработка методических указаний по работе с НФАП, который должен заработать 1 июля.

В новом НФАП, поясняет г-н Рубанов, будет размещаться ПО, сделанное по заказу государства с нуля, либо ПО, на которое есть права модификации (то есть СПО). Но хотя суть нового НФАП не изменилась (в нем будет храниться исходный код и документация на ПО), в нем все же "потерялась необходимость технологической документации с описанием процесса создания ПО. Надеемся включить", — заметил он.

В рабочую группу, отметил г-н Рубанов, входит представитель Microsoft, который старается снизить уровень технологической независимости НФАП, внося соответствующие предложения.

Дмитрий Комиссаров, входящий в ту же рабочую группу, считает, что Минкомсвязи должно выбрать вариант, по которому будет создаваться НФАП. Он пояснил при этом: "Мы стараемся убедить Минкомсвязи, что НФАП — это не только витрина. Наша цель, совпадающая с интересами государства, — не подпадать под монополизм любого производителя ПО". НФАП должен предоставить возможность другому поставщику взять код, модифицировать его и оказывать поддержку заказчику. В то же время полностью переход на СПО невозможен, уверен он. Требует также решения вопрос о размещении в НФАП закрытых программ.

Размещать полезное ПО в НФАП в соответствии с постановлением № 62 может от своего имени только орган госвласти, пояснил г-н Рубанов.

По его словам, остается открытым вопрос о поддержке СПО в НФАП, так как ответственность поставщика такого ПО не заложена: разработчик, взявший СПО из НФАП на свой риск, берет ответственность на себя.

Павел Фролов предложил воспользоваться опытом разработки ведомственного ФАП для медицинских учреждений, где подобные вопросы уже решались. Так, в рабочей версии ФАП, которой пользуются в Минздраве, хранятся типовые про-

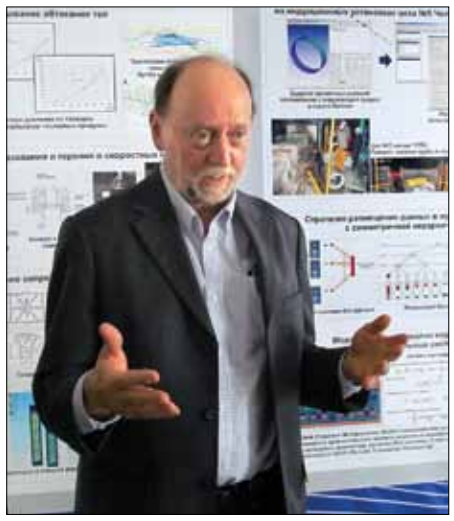
ПРОДОЛЖЕНИЕ НА С. 23 ▶

18-й Top 50, ПаВТ-2013 и перспективы рынка суперкомпьютеров в России

ДЕНИС ВОЕЙКОВ

В апреле в Челябинске прошла очередная конференция "Параллельные вычислительные технологии (ПаВТ) 2013", которую в этом году посетил основатель и куратор самого известного рейтинга мощнейших вычислительных систем мира Top 500, профессор университета Теннеси Джек Донгарра. На мероприятии была представлена 18-я редакция младшего брата его детища — рейтинга мощнейших систем России и СНГ Top 50, которая традиционно дает экспертам повод оценить состояние и перспективы отечественного рынка высокопроизводительных вычислений (HPC).

СУПЕРКОМПЬЮТЕРЫ



Джек Донгарра на ПаВТ-2013 в ЮУрГУ

Конференция и рейтинг

Конференция ПаВТ считается в России одним из двух крупнейших мероприятий подобного рода, а визит г-на Донгарры, как надеются организаторы, сможет поднять ее на новый уровень. Генеральный директор компании "РСК Технологии" Александр Московский справедливо отмечает, что зарубежный гость является не только заметной фигурой в мире, но и истинно независимым экспертом, поэтому есть шанс, что о ПаВТе появятся англоязычные публикации в СМИ и о конференции узнают за пределами нашей страны.

Программное выступление г-на Донгарры вряд ли стало для кого-то откровением, однако его доклад более чем наглядно продемонстрировал, насколько быстро развиваются технологии: обычный пользовательский ноутбук профессора, с которого он демонстрировал презентацию, судя по представленной статистике, двадцать лет назад оказался бы на первом месте в Top 500.

Александр Московский: "Складывается ощущение, что на конференции появляется все больше молодежи и людей, которые занимаются реальными задачами. Всё это весьма позитивно для рынка HPC"

Отечественный рейтинг Top 50 столь долгой историей не обладает, однако и по его данным эксперты могут сделать ряд концептуальных выводов. Обратимся к цифрам. За последние полгода, прошедшие с предыдущей редакции списка, суммарная производительность представленных в нем систем в стандартном тесте Linpack выросла с 2568,66 до 3355,9 Тфлопс. Суммарная пиковая производительность увеличилась с 4452,32 до 5707,4 Тфлопс.

Лидером остался гибридный суперкомпьютер МГУ "Ломоносов" производства компании "Т-Платформы". Его пиковая производительность составляет 1700,21 Тфлопс, по Linpack — 901,9 Тфлопс. На втором месте списка оказался новый суперкомпьютер МВС-10П производства группы компаний РСК, установленный в Межведомственном суперкомпьютерном центре (МСЦ) РАН и построенный с применением новых сопроцессоров Intel Xeon Phi: 523,83 и 375,70 Тфлопс соответственно. В третьей строчке расположилась новая система Hewlett-Packard с неуказанным местом базирования: 317,40 и 160,90 Тфлопс. Четвертое место закрепилось за новой инсталяцией "РСК Торнадо" в Южно-Уральском государственом университете (ЮУрГУ): 236,82 и 146,80 Тфлопс. И замыкает первую пятерку еще одна система Hewlett-Packard из МСЦ РАН (227,84 и 119,93 Тфлопс).

Как отмечают кураторы Top 50, в рейтинге продолжают доминировать системы, построенные на процессорах Intel. Их число увеличилось с 45 до 46. На процессорах AMD построено три системы — на одну меньше, чем в предыдущей редакции списка. На процессорах IBM — одна. Число гибридных систем, использующих для вычислений графические процессоры, уменьшилось с 15 до 14, однако появились две системы с ускорителями Intel Xeon Phi. Количество инсталляций, задействующих более 1024 традиционных процессорных ядер в системе, выросло с 43 до 47.

Число компьютеров, использующих для взаимодействия узлов лишь коммуникационную сеть Gigabit Ethernet, увеличилось с 13 до 15, а число систем, использующих InfiniBand, уменьшилось с 35 до 33.

Количество систем, используемых в науке и образовании, уменьшилось с 24 до 22; систем, ориентированных на конкретные прикладные исследования, увеличилось с 6 до 8; число систем, используемых в промышленности, осталось равным пяти, а в финансовой области — трем.

По количеству машин, входящих в список, лидируют IBM, уменьшившая свою долю с 18 до 17 систем, и HP, сохранившая долю в 16 систем. Далее идет компания "Т-Платформы", уменьшившая свою долю с 9 до 8 суперкомпьютеров, за ней — группа РСК, увеличившая свое присутствие в списке с 3 до 5 машин.

Рассматривая рейтинг в долгосрочной ретроспективе, директор по развитию корпоративных проектов Intel в России и СНГ Николай Местер отмечает, что за последние годы на фоне традиционно доминирующих кластеров научно-исследовательского назначения в Top 50 начинают появляться и промышленные системы. Явно заметно и увеличение доли суперкомпьютеров российского производства (причем на первых местах). По словам г-на Местера, еще пять-семь лет назад на фоне тотального превосходства HP и IBM отечественные системы были явной редкостью, да и то в основном речь шла о примитивной пользовательской сборке кластеров — не более того.

Директор технологического сектора высокопроизводительных вычислений Intel в регионе EMEA Андрей Семин обращает внимание на стоимость так называемого входного билета в рейтинг. Совсем недавно попасть на последние строчки Top 50 можно было, просто состыковав несколько машин, которые имелись в организации. Теперь так сделать не удастся: система на 50-м месте обладает производительностью по тесту Linpack в 12,36 Тфлопс. То есть, как поясняет г-н Местер, сегодня попадание в Top 50 означает, что ты начал заниматься HPC более или менее серьезно. Рейтинг повзрослел, и определенным образом созрел российский рынок — на нем начинают появляться профессионалы.

Андрей Семин: "Хотел бы обратить внимание на входной билет в Top 50. Буквально несколько лет назад в рейтинг можно было попасть, состыковав несколько машин, имеющихся в организации. Теперь так не получится"

Рассмотрим отечественный рынок с точки зрения потребителя.

Сегментация рынка

По уверению г-на Семина, реальный суперкомпьютинг рамками рейтингов отнюдь не ограничен. Областью применения HPC целесообразно называть задачи моделирования продуктов и процессов, которые могут быть формализованы алгоритмически и требуют вычислительных ресурсов больше, чем может предоставить один обычный компьютер. Для решения упомянутых задач требуется объединение процессоров или создание заново больших машин. Если вычислительных узлов в системе хотя бы четыре (и этого достаточно), это уже HPC. В Top такая система не войдет, но она определенно принадлежит к области высокопроизводительных вычислений.

Николай Местер: "Когда-нибудь государство все же начнет вкладывать деньги в реальный сектор экономики. А в России уже будет костяк людей, которые смогут стать основой для рынка"

С точки зрения г-на Семина, более или менее точная сегментация рынка выглядит следующим образом. Изрядную долю берет на себя государство. Это и военно-промышленный комплекс, и прогнозирование погоды (одна из старейших задач для HPC), и академический сектор, в том числе завязанный на фундаментальную науку (проверка гипотез и пр.).

В прикладной сфере, в бизнесе особое место традиционно занимает область нефтегазовых вычислений (обработка сейсмических данных и моделирование резервуаров). Помимо этого г-н Семин отмечает сектор, связанный с инженерными расчетами, — в первую очередь авто-, мото- и авиастроение. Еще одна область применения — биоинформатика, иногда в связке с химией, и отдельно — моделирование материалов и химических производств. Заслуживает внимания и сфера финансовых вычислений (речь не о банковских транзакциях, а о моделировании поведения рынка и устойчивости портфелей, аналитике). Это лишь основные секторы. На самом деле, как уверяет г-н Семин, рынок гораздо шире — вплоть до текстильной промышленности и ритейла. Например, если вы сегодня придете в дизайнерское бюро заказывать очень-очень дорогую мебель, то гарнитур не просто будет отрисован, но и наверняка сложным образом рассчитан.

Перспективы

По мнению Николая Местера, российский суперкомпьютерный рынок за последние десять лет изменился радикально. В начале 2000-х существовало всего несколько его очагов: Росгидромет, МСЦ РАН, Курчатовский институт — и по сути всё (за исключением, быть может, закрытых ведомств с их непубличными задачами). При этом, конечно, существовала определенная культура применения вычислительных средств в авиационной промышленности, но это вряд ли с полным правом можно назвать HPC. Скорее речь шла об использовании средств автоматизации и, скажем так, различного характера пакетов в рамках одной рабочей станции, одного сервера и т. д. Полноценная же культура применения высокопроизводительных вычислений (создание единых надежных решений на базе множества отдельных ненадежных элементов), как уверяет г-н Местер, росла буквально на наших глазах.

За прошедшие годы повысилась доступность технологий — "флопсы" стали значительно дешевле, проще и стандартнее. В итоге многие компании, которые раньше не могли позволить себе вычисления, теперь рассматривают такую возможность. Как считает г-н Местер, с некоторых пор наш рынок постепенно начал повторять пути развития рынков Европы и США — как с точки зрения принципов и подходов (государство стало вкладывать деньги похожим образом: в программы, в создаваемые им центры и т. д.), так и с точки зрения коммерческого применения. Например, во всем мире давно известен Голливуд с его визуальными компьютерными эффектами, но с недавнего времени и в России появилось множество компаний, которые занимаются созданием цифрового контента (компьютерной графики и рекламы). Рынки похожи, уверен г-н Местер. Просто российская экономика меньше — где-то в разы, где-то на порядки. Но это все равно вселяет определенную надежду, что мы все же когда-нибудь интегрируемся в мировое сообщество. (При перпендикулярных рынках сделать это было бы практически невозможно.)

Николай Местер уверен, что рано или поздно наше государство начнет все-таки вкладывать деньги в реальный сектор экономики, а в России к тому времени уже появится костяк людей, которые смогут стать основой для полноценного HPC-рынка. Лет пять-семь назад кадров практически не было совсем. В известный период старая школа уехала за рубеж почти в полном составе. Заменить этих людей сложно, но, как считает г-н Местер, с чего-то нужно и уже можно начинать.

АНОНСЫ

Форум Schneider Electric Xperience Efficiency 2013

С 4 по 7 июня в Москве в здании Академии наук состоится форум инновационных и энергоэффективных технологий Schneider Electric, который в этом году получил название Xperience Efficiency 2013. Ежегодно этот международный форум проходит в 14 крупных городах десяти стран.

На мероприятии будут представлены интегрированные энергоэффективные решения для энергетики и инфраструктуры, промышленных предприятий, объектов гражданского и жилищного строительства, а также для центров обработки данных. Главной темой Xperience Efficiency в этом году станет направление Smart City — "Умный город". 5 июня на форуме Xperience Efficiency намечено обсуждение вопросов проектирования, построения и эксплуатации энергоэффективных и надежных центров обработки данных. Ключевыми докладчиками в этот день станут Илья Звонов, вице-президент IT Business Schneider Electric, Алексей Солодовников, директор Uptime Institute в России и СНГ, и Юрий Самойлов, генеральный директор Dataline.

Зарегистрироваться на мероприятие и получить подробную информацию можно на сайте www.schneider-electric.com/site/home/index.cfm/ru/. *Александр Чубуков*

PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
МАЙ • 2013 • МОСКВА
http://www.pcweek.ru

О защите виртуализированных сред

ВАЛЕРИЙ ВАСИЛЬЕВ

Согласно результатам международного опроса, проведенного IDC в 2012 г., среди своих наиважнейших задач ИТ-руководители выдвигают на первое место консолидацию серверов и их виртуализацию. Результаты исследований этой же аналитической компании, завершенные в IV квартале 2012 г., показывают, что в России виртуализацией охвачено более 25% серверов. Это несколько больше, чем в США, и немногим меньше, чем в Германии и Великобритании.

ОБЗОРЫ

Начав с серверов и убедившись на практике в эффективности применения виртуализации в ИТ-инфраструктуре, заказчики стали распространять эту технологию на рабочие места, сетевой компонент ИТ-инфраструктуры и системы хранения данных (СХД).

Однако наряду с явными выгодами виртуализация привнесла новые, связанные с обеспечением информационной безопасности (ИБ), проблемы, специфичные для применения данной технологии в ИТ-среде. Эти проблемы можно разделить на две части: технологическую и организационную.

В нашем обзоре мы рассмотрим основные технологические особенности организации защиты составляющих ИТ-инфраструктуры — серверов, рабочих мест, корпоративной сети и систем хранения данных, которые связаны с виртуализацией этой инфраструктуры. Мы постараемся дать оценку состояния рынка средств защиты виртуализированных ИТ-ресурсов и опыта их применения, а также охарактеризуем действующую в нашей стране нормативно-правовую базу, относящуюся к аспектам регулирования использования виртуализации с позиций ИБ.

Уровень проникновения и перспективы виртуализации ИТ в России

Если объединить результаты исследований IDC с данными "Лаборатории Касперского", то можно сделать вывод, что не позднее чем через год серверную виртуализацию будут использовать более половины российских предприятий и организаций разных масштабов. При этом, как утверждает Михаил Чернышев, прогресс очевиден не только в традиционно благополучных для распространения современных технологий регионах вроде Москвы или Санкт-Петербурга — он наблюдает это практически повсюду, где в стране есть предприятия среднего и крупного масштаба (именно выйдя на такой уровень, компании, как правило, и начинают задумываться об экономии ИТ-ресурсов и повышении надежности).

Согласно наблюдениям Константина Воронкова, большая часть серверных приложений, которые компании используют сегодня в виртуальных средах (ВС), являются критически важными для бизнеса (это базы данных, электронная почта, системы ERP, CRM и т. п.), что резко отличается от ситуации, которая наблюдалась несколькими годами ранее, когда виртуализация только начинала обретать популярность и предприятия переносили в виртуальную среду свои наименее критичные приложения. Массовая виртуализация критически важных бизнес-приложений свидетельствует, как полагает г-н Воронков, о доверии заказчиков к этой технологии, а также о достижении определенного уровня зрелости самой технологии.

Виртуализация инфраструктуры рабочих станций (VDI), согласно данным "Лаборатории Касперского", пока не получила в нашей стране широкого распространения. Эксперты "Лаборатории" объясняют это тем, что VDI обычно используется в тех компаниях, чьи сотрудники выполняют типовые, строго регламентированные задачи (как, например, сотрудники call-центров, операционисты в банках, служащие многих государственных организаций).

Следует отметить, что потребность в таких рабочих местах испытывают далеко не все заказчики. Тем не менее по мере того, как технологии виртуализации рабочих станций совершенствуются, российские компании (в первую очередь крупные) всё чаще проводят пилотные внедрения VDI. В целом нынешнее положение виртуализации рабочих мест специалисты "Лаборатории Касперского" в нашей стране рассматривают как стартовое и предполагают активный рост количества внедрений решений виртуализации рабочих станций в близкой перспективе.

Основываясь на своем опыте проектной деятельности и обследования объектов ИТ и ИБ, Сергей Панин оценивает проникновение платформ виртуальных сред в России в сегментах среднего и крупного частного бизнеса примерно в 85%. Он также отмечет, что понимание преимуществ использования виртуализации есть и у российских государственных организаций. Так, проведенный им анализ сайта государственных закупок показывает большой рост количества заказов как на проектирование и внедрение виртуальных сред, так и на поставку неисключительных прав использования лицензионных виртуальных сред. При этом, как он отмечает, если не в первом же заказе, то в последующих заказчики поднимают вопрос о защите закупаемых решений.

Проникновение виртуализации в корпоративную ИТ-среду в целом в нашей стране Дмитрий Когай оценивает в 10—15% и полагает, что по этому показателю Россия существенно проигрывает экономически развитым странам. Вместе с тем темпы, которыми растет это ИТ-направление, превышают, по его мнению, таковые по ИТ-отрасли в целом. Ссылаясь на данные аналитиков из IDC, он прогнозирует, что в течение пяти ближайших лет Россия может выйти на 70% виртуализации всей ИТ-инфраструктуры.

Алексей Сабанов полагает, что виртуализация, несмотря на громкую рекламу, на практике пока еще используется слабо; в настоящее время идет тестирование технологии, устраняются нестыковки средств виртуализации разных производителей, в виртуальную среду переведено не более 8% бизнес-процессов, причем в основном в частные, полностью подконтрольные владельцам этих бизнес-процессов, виртуальные среды.

Солидарен с Алексеем Сабановым в оценке уровня проникновения средств виртуализации ИТ-ресурсов в России Вячеслав Медведев. По его мнению, этот показатель остается все еще достаточно низким. Г-н Медведев отмечает, что существует большое количество предложений по переводу всей или части ИТ-инфраструктуры в облачные структуры — частные, глобальные, гибридные. Но этих предложений, считает он, явно недостаточно для покрытия всей территории нашей страны. Но самое главное заключается в том, что потенциальные клиенты облачных ИТ-сервисов опасаются трудностей, появляющихся при переводе ИТ в облака, и прежде всего их пугает отсутствие финансовой ответственности поставщиков облачных услуг в случае возникновения различного рода ИБ-проблем, включая прерывание доступа к ИТ-сервисам и т. п. В дополнение к этому они предполагают рост затрат на безопасность, который обычно связывают с появлением новых рисков, присущих виртуализации и облачным технологиям.

К факторам, сдерживающим распространение виртуализации, Николай Романов помимо финансового аспекта относит необходимость существенного расширения систем хранения данных под виртуализацию и тщательную оценку возможных сценариев использования. Он обращает внимание на то, что до сих пор не все приложения и системы (например, графические системы, а также СХД сами по себе) могут быть перенесены в виртуальную среду. Что касается виртуализации корпоративных сетей, то это направление он оценивает как находящееся в начальной стадии.

Особенности обеспечения ИБ виртуализированных ИТ-сред

Опросы показывают, что более половины ИТ-специалистов все еще оценивают ИБ-риски для виртуализированных ИТ-ресурсов как более низкие, чем для физических. Тем, кто так считает, Алексей Воронцов напоминает, что только в идеале виртуализация позволяет строить потенциально более защищенные (по сравнению с невиртуализированными) ИТ-системы за счет грамотного применения изоляции сервисов в отдельных виртуальных машинах и возможностей фильтрации, предоставляемых виртуализированной сетевой инфраструктурой. В реальности же ситуация выглядит иначе. Виртуализированная ИТ-среда подвержена тем же угрозам, что и физическая. Кроме того, ей присущи и специфические, связанные с технологическими особенностями, уязвимости. Так, простота развертывания виртуальных машин (ВМ) приводит к тому, что обновления антивирусов и патчи на программное обеспечение не устанавливаются, а традиционные средства обнаружения сетевых атак и сетевые экраны не видят трафик внутри виртуальной сети.

Константин Воронков, в свою очередь, напоминает, что любая атака на физическую инфраструктуру может быть в итоге нацелена на виртуальные машины, и для ее проведения злоумышленникам про-

ПРОДОЛЖЕНИЕ НА С. 18 ▸

Наши эксперты

ИВАН БОЙЦОВ, *аналитик, "Код Безопасности"*

КОНСТАНТИН ВОРОНКОВ, *руководитель группы, "Лаборатория Касперского"*

АЛЕКСЕЙ ВОРОНЦОВ, *технический специалист по ПО безопасности, IBM*

ДМИТРИЙ КОГАЙ, *менеджер по продукту, "Аванпост"*

ВЯЧЕСЛАВ МЕДВЕДЕВ, *старший аналитик отдела развития, "Доктор Веб"*

СЕРГЕЙ ПАНИН, *инженер по системам информационной безопасности, LETA*

НИКОЛАЙ РОМАНОВ, *технический консультант, Trend Micro в России и странах СНГ*

АЛЕКСЕЙ САБАНОВ, *заместитель генерального директора, "Аладдин Р.Д."*

ЕЛИЗАВЕТА СПАСЕННЫХ, *менеджер по развитию бизнеса, "Информзащита"*

МИХАИЛ ЧЕРНЫШЕВ, *технический консультант, McAfee в России и СНГ*

Проблемы защиты виртуализованных ИТ-сред

ИВАН ДУДОРОВ, МЕНЕДЖЕР ПО ПРОДУКТУ КОМПАНИИ "КОД БЕЗОПАСНОСТИ"

Основные меры по защите виртуальной инфраструктуры (ВИ) складываются как из специфики работы самой виртуальной среды, так и из особенностей обрабатываемой в ней информации. Стандартные подходы для защиты физических сред в данном случае малоприменимы: существует целый ряд специфических угроз, которые необходимо принимать во внимание при построении контура защиты виртуальной инфраструктуры.

Представьте себе ситуацию, когда администратор ВИ имеет доступ и к средствам управления виртуальной машиной (ВМ) и к обрабатываемым ею данным. При этом он может скопировать образ ВМ на какой-либо внешний носитель и вынести его за пределы защищаемого периметра, тем самым получив возможность извлечения любых данных из этого образа. Таким образом, любые конфиденциальные сведения будут скомпрометированы так называемым "суперпользователем".

Другой опасной ситуацией может стать атака на сервер виртуализации и соответственно компрометация всех развернутых на нем ВМ. Уязвимым участком виртуальной инфраструктуры является и обмен между ВМ и хостом. Нередки также ситуации, когда на одном сервере развернуты несколько ВМ с различными уровнями конфиденциальности, в результате чего атака на менее защищенную машину может быть использована в качестве одного из этапов для атаки на ВМ с более высоким уровнем доступа. А ведь отследить взаимодействие между ВМ с помощью стандартного межсетевого экрана попросту невозможно. В целом, если речь идет о защите ВИ, нельзя забывать о защите и более низкого уровня, физического, на котором происходит развертывание системы, так как виртуальная среда воспринимает этот уровень как доверенный. Другими словами, вопросы защиты серверов виртуализации от НСД, сегментация сетевой инфраструктуры и прочие атрибуты ИБ должны быть реализованы заранее, иначе теряется весь смысл защиты виртуализации. Не стоит также сбрасывать со счетов возможные атаки на вспомогательные компоненты ВИ, такие как средства репликации и СХД.

Существует и другая сторона рассматриваемого вопроса — нормативно-правовая, касающаяся регулирования информационной безопасности в сфере виртуализации. В декабре 2012 г. ФСТЭК России опубликовала два проекта приказов: "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Первый документ касается далеко не всех, а вот на второй следует обратить внимание большинству компаний: впервые в нормативно-правовых документах были определены 11 мер по защите среды виртуализации, включающие в себя аутентификацию компонентов, контроль и разграничение доступа, резервное копирование данных, контроль целостности, сегментирование ВИ и т. д. Можно быть уверенным, что в той или иной степени эти меры войдут и в окончательную версию приказа, а это означает последующую необходимость приведения в соответствие с законодательством виртуальных инфраструктур многих компаний с помощью сертифицированных средств защиты.

К сожалению, защита с помощью встроенных возможностей платформы виртуализации, даже будучи сертифицированной, зачастую является либо недостаточной для реализации требуемых мер, либо ее настройка и дальнейшее обслуживание оказываются нетривиальными и ресурсоемкими. Каким образом привести все в соответствие, если встроенных возможностей платформы виртуализации недостаточно? Один из наиболее эффективных вариантов — применить специализированные средства защиты от несанкционированного доступа (НСД) для ВИ. Такие средства защиты не только способны обезопасить среду виртуализации и контролировать ее состояние в будущем, но и, как правило, обладают соответствующими сертификатами ФСТЭК России. Кроме того, эти средства располагают достаточным функционалом, чтобы "закрывать" большую часть перечисленных в проекте приказа ФСТЭК России требований. Однако не стоит забывать про резервное копирование, распределенное хранение данных и восстановление информации, антивирусную защиту и обнаружение вторжений — эти функции также являются неотъемлемой частью общей концепции и требуют принятия мер ИБ.

Сегодня производители специализированных СЗИ для защиты ВИ частично предлагают требуемые продукты (например, средства доверенной загрузки сервера виртуализации), но речь о едином законченном решении от одного вендора здесь не идет. В результате очень часто приходится "городить огород", развертывая антивирус, IDS/IPS, средства защиты ВИ и т. д. от абсолютно разных поставщиков без возможности объединения их в единую консоль управления. К чему это приводит — говорить, полагаю, не нужно. Поэтому на данный момент среди самых перспективных направлений в разработке решений можно назвать создание некой "экосистемы безопасности", позволяющей гибко управлять политиками ИБ не только в сфере виртуализации, но и во всех смежных областях, таких как защита физической инфраструктуры, включая серверы, АРМ и информационные каналы данных. В конце концов, защита любого объекта должна быть комплексной, а развертывание, управление и мониторинг ИБ из единого графического интерфейса с помощью заранее созданных профилей безопасности — мечта любого администратора.

Применяя такой универсальный инструмент, можно было бы в несколько кликов получить защищенную виртуальную среду с четким контролем и мониторингом всех производимых администраторами и пользователями действий. И одновременно привести автоматизированную систему в соответствие с требованиями российского законодательства и зарубежных рекомендательных документов, таких как PCI DSS или VMware Security Hardening Guide. Однако в настоящий момент приходится ограничиваться отдельными сертифицированными средствами защиты от разных производителей и комбинировать их оптимальным способом под специфику работы компании. Будем надеяться, что в ближайшее время на российском рынке все же произойдут соответствующие изменения и мы сможем увидеть единое решение, закрывающее широкий спектр проблем в сфере ИБ.

СПЕЦПРОЕКТ КОМПАНИИ "КОД БЕЗОПАСНОСТИ"

О защите...

◂ ПРОДОЛЖЕНИЕ СО С. 17

ще использовать обычные уязвимости ИТ-инфраструктуры, нежели вести дорогостоящие разработки специализированных средств, ориентированных именно на виртуальные среды.

Как утверждает Дмитрий Когай, в виртуализированной среде периметр защиты должен создаваться вокруг каждой отдельной ВМ и независимо от ее перемещения следовать за нею.

Иван Бойцов предлагает разделять ИБ-угрозы, свойственные для виртуализированной ИТ-среды, на несколько групп. К первой группе он относит угрозы аппаратному обеспечению, на котором развертываются компоненты ВС. Это угрозы, знакомые большинству ИБ-специалистов: физические повреждения или несанкционированные изменения аппаратного обеспечения, его кража или уничтожение, нарушения в сетевой инфраструктуре, стихийные бедствия и аварии и т. д. Компоненты виртуальной инфраструктуры должны поддерживать кластеризацию, шифрование данных и другие стандартные способы защиты от подобных угроз.

Другую группу, по мнению г-на Бойцова, составляют угрозы гипервизору. Это их новый вид, включающий угрозы, связанные с особенностями эксплуатации ВС: ошибки в настройках гипервизора, виртуальных машин и других компонентов ВС, уязвимости в программных кодах гипервизора, подмена его компонентов, атаки типа "отказ в обслуживании", несанкционированный доступ к файлам образов ВМ. Эти угрозы он рекомендует закрывать программным обеспечением гипервизора и дополнительными средствами защиты ВС.

В отдельную группу г-н Бойцов выделяет угрозы системе управления виртуализированной ИТ-средой: несанкционированный доступ к системе управления, отсутствие разделения доступа между администраторами ВС или неправильная настройка такого разделения. Против них он рекомендует использовать усиленные механизмы аутентификации и разграничения доступа.

Еще одну группу, как считает г-н Бойцов, образуют угрозы виртуальным машинам. Они похожи на угрозы физическим серверам и рабочим станциям, к которым добавляются угрозы, связанные с виртуализацией аппаратного обеспечения в виртуальных машинах, в том числе и системы BIOS. В числе таких угроз — несанкционированная загрузка, остановка и выключение виртуальных машин, загрузка ВМ со стороннего носителя, изменение и подмена файлов образов ВМ, несанкционированное изменение конфигурации виртуальных машин. Для эффективной борьбы с угрозами такого рода он рекомендует механизмы контроля целостности и доверенной загрузки виртуальных машин.

Наконец, для сети передачи данных и систем хранения данных г-н Бойцов видит угрозы, типичные для аппаратной части, и угрозы, направленные на получение несанкционированного доступа к управлению этими компонентами.

Николай Романов обращает внимание на то, что в каждом из сегментов виртуальной среды есть свои болевые точки и что ранжировать риски, связанные с информационной безопасностью, имеет смысл по типу эксплуатации виртуализированных систем. С учетом специфики серверных платформ он прежде всего выделяет те, на которых базируются публичные сервисы (в первую очередь веб-серверы). Наряду с основными механизмами периметровой защиты на сетевом уровне (системами предотвращения вторжений, средствами защиты от DoS-атак) такие системы должны иметь аналогичные средства, работающие непосредственно в той среде, где они работают. Подобная методика позволяет закрыть тот спектр угроз, против которых типовые средства могут быть малоэффективны (контроль внутри гипервизора как на файловом, так и на сетевом уровне).

Отмечая, что переход к ВС породил ряд специфических ИБ-проблем, которые не связаны с типом сервисов, г-н Романов указывает на то, что безопасность в классическом понимании (блокирование уязвимостей без установки патчей средствами систем предотвращения вторжений, защита от вирусов, сбор данных о несанкционированных изменениях и др.) была расширена на уровне защиты от несанкционированного доступа в границах эксплуатации виртуализированных систем, обеспечивающем как возможности мандатного разграничения доступа к ВС, так и контроль целостности самого гипервизора.

На примере антивируса Константин Воронков поясняет возможные издержки применения традиционных средств защиты в ВС. Он утверждает, что традиционное антивирусное решение может защитить и виртуализированную ИТ-среду, однако при этом оно потребует установки антивирусных агентов, что означает развертывание антивирусного ядра и сигнатурных баз на каждой виртуальной машине. Это вызовет необходимость избыточного использования ресурсов памяти, дискового пространства и процессора хост-сервера, что практически сведет на нет одно из основных преимуществ виртуализации — эффективное использование вычислительных ресурсов.

Созданные специально для защиты ВС виртуальные устройства (Virtual Appliance) безопасности обеспечивают безагентную антивирусную защиту сразу нескольких виртуальных машин. В этом случае антивирус работает на уровне гипервизора. Перенос антивирусной защиты на специально выделенное устройство существенно снижает расходование системных ресурсов, повышает производительность аппаратного обеспечения и увеличивает плотность ВМ на хост-сервере.

Вместе с тем, как отмечает Константин Воронков, применение специализированных средств защиты ВС нередко приводит к появлению дополнительных консолей управления, что увеличивает нагрузку на администраторов и расходы.

По мнению Ивана Бойцова, большинство архитектурных и технологических сложностей в реализации защиты виртуализированных ИТ-сред уже преодолены, а те, что остались, связаны с закрытостью средств виртуализации, отсутствием необходимых для ИБ-вендоров инструментов API и SDK и другими проблемами, касающимися проприетарности платформ виртуализации.

Алексей Воронцов указывает не только на нехватку таких инструментов, как интерфейсы прикладного программирования (API) и пакеты программ для разработки приложений (SDK), но и на необходимость единого стандарта доступа для средств защиты к ВС. Он обращает внимание на то, что у каждого поставщика гипервизоров свои подходы к формированию ВС и ИБ-вендорам приходится ориентироваться на конкретные архитектуры.

Наиболее уязвимые компоненты ВС

Несмотря на отсутствие информации о реальных ИБ-инцидентах, связанных с нарушением защищенности гипервизора, наши эксперты рекомендуют при решении вопросов обеспечения информационной безопасности уделять ▸

Враг в кармане

ВЯЧЕСЛАВ МЕДВЕДЕВ, СТАРШИЙ АНАЛИТИК ОТДЕЛА РАЗВИТИЯ КОМПАНИИ "ДОКТОР ВЕБ"

В последние годы мобильные устройства неожиданно для многих обзавелись широким функционалом. Еще какие-то пять лет назад максимум, что можно было делать с их помощью, — это запускать простейшие игрушки на java и менять мелодии. Современные смартфоны — это процессоры, превосходящие по мощности процессоры настольных компьютеров, считавшихся топовыми еще совсем недавно, большой объем памяти, современная удобная операционная система, которую дополняют все необходимые для повседневной работы офисные приложения и большое количество игровых программ.

Все больше сотрудников компаний имеют такие "продвинутые" смартфоны, все чаще эти мобильные устройства используются для работы. Бизнесу это выгодно — сотрудники постоянно находятся на связи, больше времени отдают работе и т. д.

Есть ли в данном случае "но"? Да, и огромное! Эти устройства, как правило, принадлежат самим сотрудникам, а не компании — практика раздачи корпоративных устройств распространена, но далеко не общепринята. Личные устройства зачастую никак не защищены от злоумышленников. Немного статистики на основе нескольких исследований, представленных в публичных источниках:

- 40% планшетов не имеют никакой защиты (в том числе и iPad'ы);
- 48% работников пытаются обходить требования безопасности;
- только 21% работников координируют свои действия с ИТ-отделом.

Было бы странно, если бы злоумышленники не попытались выйти на этот рынок. Поначалу их попытки были достаточно робкими — вплоть до того, что вредоносные программы распространялись с инструкциями по их установке. Когда появились первые вирусы под Android — и соответственно первые антивирусы для противодействия им — многие не верили в саму возможность угроз.

Уверенные в безопасности своих устройств и доверяющие компании-производителю пользователи даже в те далекие времена активно участвовали в распространении вирусов. Только для одного такого вируса Android.Plankton.1 (его функцией был сбор и передача информации об устройстве злоумышленнику) было зарегистрировано 150 000 загрузок с Android Market.

Но постепенно возможности "мобильных" вредоносных программ росли, и сейчас уже всё "по-взрослому": для заражения зачастую достаточно зайти не на тот сайт или подключиться к зараженному компьютеру — и там, и там устройство уже ждут с распростертыми объятиями. Вот что могут современные вредоносные программы на вашем мобильном устройстве: блокировать телефон; звонить и производить несанкционированную рассылку СМС-сообщений по команде от сервера; отслеживать входящие и исходящие телефонные звонки; собирать и переправлять "куда надо" фотографии, хранящиеся на телефоне, отправляемые и получаемые почтовые сообщения, используемые пароли, СМС-сообщения, набираемый на клавиатуре текст, GPS-координаты; включать динамик без ведома пользователя.

Вы проводите совещание? Ваш Android к услугам злоумышленников — все переговоры будут записаны. Во время переговоров вы кладете свое мобильное устройство перед собой? Отлично, фотографии участников уйдут заказчикам слежки за вами. Нужно обыскать или ограбить офис или вашу квартиру? Android подскажет, где вы находитесь, и поможет спланировать преступление.

Думаете, это всё? Мобильные устройства на данный момент предоставляют злоумышленникам куда больше возможностей, чем обычные компьютеры.

Компания работает с системами дистанционного банковского обслуживания и получает подтверждения в СМС? У вас есть счет в банке и/или пластиковая карта и вы что-то оплачиваете с мобильного устройства? Ваши деньги — это именно то, что нужно криминальным структурам. Просим не любить и не жаловать: Android.SpyEye.2.origin, Android.Panda.2.origin, Android.SmsSpy.6.origin и Android.FakeSber.1.origin.

Для обеспечения безопасности финансовых операций в Интернете банковские системы отправляют СМС-сообщения с кодами подтверждения на привязанный к клиентскому счету номер мобильного телефона. Чтобы успешно завершить транзакцию, пользователь должен ввести в специальную веб-форму полученный код. Мобильные банковские троянцы предназначены для перехвата СМС-сообщений, передачи mTAN-кодов злоумышленникам, которые выполняют различные финансовые операции с электронными счетами ничего не подозревающих жертв.

Типичный способ распространения таких вредоносных программ — социальная инженерия. А Android.FakeSber.1.origin — первый Android-троянец, направленный против клиентов российского банка, — был даже помещен злоумышленниками непосредственно в официальный каталог приложений Google play. Троянец работал не сам по себе, а "в паре" со знаменитым Trojan.Carberp.

Необходимо отметить, что большая часть вредоносных программ создается для долговременного незаметного пребывания на зараженном компьютере — "доить" постепенно всегда выгоднее и безопаснее, чем сразу попытаться увести все деньги. Заметить их неподготовленному пользователю невозможно. К такому ПО, кроме уже упоминавшихся банковских троянцев, относятся шпионские программы и ПО, разработанное для проведения APT-атак. Так, Android.Luckycat.origin должен был обеспечивать не только сбор данных с зараженного устройства, загрузку различных файлов с мобильного устройства и на него, но и выполнение команд, поступающих с управляющего сервера. Android.MailSteal.1.origin, Android.Maxbet.1.origin, Android.Loozfon.origin и Android.EmailSpy.origin собирали всю информацию из телефонной книги (включая адреса электронной почты), а также идентификаторы устройства.

Прогресс криминальных структур хорошо иллюстрирует развитие СМС-троянцев, ведущих свою родословную от Android.SmsSend, появившегося еще в 2010 г. Эти вредоносные программы предназначены для отправки дорогостоящих СМС-сообщений и подписки абонентов на различные контент-услуги.

Количество зараженных мобильных устройств все время увеличивается — в прошлом году появились сообщения о создании первых бот-сетей на основе Android. Теперь DoS-атаку можно проводить уже и с мобильных устройств!

Не стоит думать, что список написанного злоумышленниками для мобильных устройств ограничивается только вышеописанными примерами. К сожалению, угрозы для "мобильников" растут опережающими темпами по сравнению с угрозами для обычных компьютеров.

Одной из причин поражения Египта в "войне Судного дня" стало то, что его армии вышли из-под "зонтика" ПВО. Лишившись надежной защиты, танковые соединения были уничтожены, что не позволило отразить встречную атаку… Если пользователи думают, что они сами смогут заметить и устранить любую угрозу, полезно вспомнить о данном случае!

первоочередное внимание именно ему, поскольку компрометация гипервизора легко может привести к компрометации всех обслуживаемых им виртуальных машин.

Хотя разработчики гипервизоров и заявляют о высокой степени безопасности своих продуктов, говорить об их полной защищенности не стоит, тем более что на международных ИБ-конференциях хакеры уже демонстрировали возможности их взлома.

Дмитрий Когай указывает на необходимость контроля сетевого трафика между виртуальными машинами, расположенными на одном физическом сервере, поскольку обычно считается, что трафик между такими ВМ не покидает пределы сервера и поэтому якобы является заведомо защищенным от взлома снаружи. Однако если злоумышленнику удается захватить контроль хотя бы за одной из виртуальных машин, то возникает возможность компрометации и остальных ВМ этого сервера с последующей эскалацией атаки на соседние серверы, особенно если не забывать о том, что традиционные системы сетевой фильтрации и предотвращения вторжений работают до границы платформы виртуализации и не могут отслеживать вредоносную активность внутри этих границ.

Первоочередное внимание, по мнению Сергея Панина, пользователи ВС должны уделять правильному конфигурированию ИТ- и ИБ-ресурсов в ВС и мониторингу действий привилегированных пользователей, что напрямую связано с установкой корпоративных приоритетов закрываемых уязвимостей.

С позиции приоритетов угроз он также предлагает подходить и к защите компонентов платформы виртуализации. Так, если высоким в компании считается приоритет внедрения вредоносного кода, то в связи с отсутствием реальных случаев появления такого кода на уровне "гипервизор — средство управления" наиболее уязвимым компонентом ВС, по его мнению, следует считать виртуальную машину, и первоочередное внимание нужно обращать на безопасность взаимодействия ВМ между собой и с компонентами внешней среды.

Николай Романов напоминает, что каждый компонент виртуализированной ИТ-среды имеет свои ИБ-проблемы и требует своих подходов к их решению. Так, перемещаемые в рамках ЦОДа (или между ЦОДами) виртуальные машины могут оказаться брешью в защите, если из доверенной среды они перемещаются в недоверенную (или из защищенной в незащищенную).

Алексей Сабанов полагает, что самым уязвимым компонентом ВС являются системы хранения данных. За ними по степени важности рисков следуют системы управления ВС, из которых объектом атак могут оказаться прежде всего системы управления доступом к ИТ-ресурсам.

По мнению Вячеслава Медведева, не стоит выделять как наиболее уязвимый какой-либо отдельный компонент виртуализированной ИТ-среды — безопасными должны быть они все, причем в соответствии с динамично изменяющимся ландшафтом угроз. Ведь хакеры, как говорит г-н Медведев, ищут и находят уязвимости там, где вчера их вроде бы и не было.

Готовность российского ИБ-рынка к обеспечению безопасности ВС

В оценках готовности участников российского рынка ИБ к обеспечению безопасности виртуализированных ИТ-сред у наших экспертов есть как совпадения во мнениях, так и заметные расхождения. Кто-то из них акцентирует внимание на таких аспектах, которые не попали в поле аналитического рассмотрения коллег.

Вендоры. Согласно наблюдениям Алексея Воронцова, ряд ведущих ИБ-вендоров мира уже предлагают специализированные средства защиты ВС, прежде всего функционирующие через уровень гипервизора, с использованием таких технологий доступа к гипервизору, как VMSafe. Появляются актуальные средства контроля сетевого трафика между виртуальными машинами, в том числе средства обнаружения атак, использующие поведенческий анализ.

Современные специализированные ИБ-решения, по мнению Константина Воронкова, в состоянии обеспечить надежную защиту (что важно — без потерь преимуществ, получаемых за счет виртуализации) и возможность централизованно управлять защитой всей корпоративной ИТ-инфраструктуры, включая как виртуализированные компоненты ИТ, так и невиртуализированные. Конечно, внедрение специализированных решений по сравнению с внедрением традиционных стоит дороже, однако, как считает г-н Воронков, преимущества их неоспоримы и в итоге они более выгодны.

Сегодняшний рынок информационной безопасности, отмечает Сергей Панин, насыщен большим количеством конкурирующих как узконаправленных, так и комплексных решений, обеспечивающих защиту виртуализированных сред и от внешних, и от внутренних угроз. Наряду со специализированными средствами для защиты ВС заказчики используют и классические: защиту от несанкционированного доступа, средства доверенной загрузки, инструменты контроля целостности, распределенные межсетевые экраны и т. д.

Елизавета Спасенных считает, что обеспечение защиты виртуализированной ИТ-среды все еще является задачей достаточно новой, требующей более основательной проработки деталей и учета особенностей реализуемых в ВС сервисов, спектр которых непрерывно расширяется, а вместе с ним расширяется и спектр возможных ИБ-рисков. Поиск и разработка дополнительных решений по обеспечению безопасного использования ВС остается актуальным процессом для ИБ-вендоров, в котором они, по ее мнению, достаточно результативно и оперативно участвуют.

Высоко оценивая возможности доступных на рынке средств защиты ВС для нейтрализации большинства ИБ-угроз, Иван Бойцов указывает на узкий круг поддерживаемых ими средств виртуализации. По его мнению, в полной мере поддерживаются (в том числе и сертифицированными средствами) только несколько наиболее распространенных на рынке продуктов.

В России, считает Николай Романов, заказчики пока еще не задаются всерьез вопросами, связанными со сменой провайдеров облачных сервисов (например, вопросами надлежащего уничтожения данных на площадке прежнего провайдера), или выполнением требований регуляторов при обработке персональных данных в ЦОДе провайдера, предоставляющего сервисы PaaS. Он обращает внимание на то, что по мере активизации перехода от обычных виртуализированных систем к облачным готовность провайдеров ИТ-сервисов к ответу на эти вопросы должна возрастать.

Что бы ни заявляли разработчики, ИБ-индустрия, как считает Алексей Сабанов, имея в виду прежде всего использование ВС в облачной архитектуре, пока не готова реализовать комплексный и взвешенный подход к обеспечению информационной безопасности в плохо еще

ПРОДОЛЖЕНИЕ НА С. 20 ▸

Специфика комплексной защиты виртуализированных ИТ-сред

Компания Trend Micro является в настоящее время одним из немногих в мире поставщиков комплексных решений для защиты облачных и виртуальных сред. Она первой в сотрудничестве с VMware разработала модель системы безопасности без использования агентов, базирующуюся на тесно интегрированных продуктах VMware vShield Endpoint и Trend Micro Deep Security. Об актуальных проблемах, связанных с обеспечением безопасности виртуализированных ИТ-ресурсов, и текущей ситуации в этой области рассказывает технический консультант Trend Micro в России и странах СНГ ***Николай Романов****.*


Николай Романов

Согласно прогнозу компании Gartner от 2010 г. даже к 2015 г. около 30% виртуальных машин по-прежнему будут защищены хуже физических (в 2010 г. таких виртуальных машин, согласно данным этой компании, было 60%). А как обстоят дела с защищенностью виртуализированных ИТ-компонентов сегодня?

Возможно, российские ИТ-пользователи оказались более зрелыми, чем предполагалось, или же сыграл свою роль активный информационный фон вокруг ИБ-проблем, связанных с виртуализацией, но ситуация у нас в стране не так плоха, как ее прогнозировала компания Gartner. Я бы сказал, что она даже лучше, чем в европейских странах, но несколько хуже, чем в США.

Виртуализация используется российскими компаниями прежде всего в ИТ-решениях, предназначенных для обслуживания бизнес-задач и задач из области самих ИТ. ИБ-проблемы виртуализации неплохо осознаются российскими заказчиками, представляющими различные отрасли, лучше — банками, слабее — производственными предприятиями.

Корпоративные ИТ-пользователи понимают, что виртуализированные среды наряду с трансформированными под специфику виртуализации аналогами классических средств защиты (антивирусами, межсетевыми экранами и др.) требуют решения сугубо специальных ИБ-задач, таких как защита от несанкционированного доступа к системе управления виртуализацией, защита гипервизора и др. Другое дело, что им не всегда ясно, с помощью каких средств можно решить такие задачи.

На защищенности каких виртуализированных компонентов ИТ-инфраструктуры сегодня сфокусирован интерес ИТ-пользователей и ИБ-вендоров?

В первую очередь сегодня компании защищают серверные платформы, потому что на них работают их ключевые бизнес-приложения. Активная виртуализация настольных систем требует также внимания и к их защите. При этом нельзя сказать, что проблемы, связанные с их уязвимостями, проще серверных, разве что связанные с ними риски потерь оцениваются ниже. Поэтому виртуализированные рабочие места по приоритету на втором месте.

Виртуализированные сети и системы хранения данных, несмотря на прямую вовлеченность в процесс построения описываемых систем, пока составляют ничтожно малую часть в проектах, связанных с обеспечением ИБ виртуальных сред. Причем если на сетевом уровне часть задач уже может быть решена даже встроенными средствами самих систем (VMware vShield App, например), то с СХД все обстоит несколько сложнее. То, что развитие виртуализированных сетей находится все еще в активной фазе, можно заметить на примере VMware, безоговорочном лидере в области платформ виртуализации, в прошлом году купившей стартап-копанию Nicira, занимающуюся виртуализированными сетевыми системами и управлением ими. Те отдельные компоненты защиты виртуализированных сетей, которые предлагают такие вендоры, как Cisco или Checkpoint, дополняют основные решения для виртуальных сред. Что касается полномасштабных аппаратно-программных систем хранения данных (на которые, кстати, виртуальная среда опирается в значительной степени), то их виртуализация пока применима далеко не везде (по причине некоторых ограничений и стоимости, главным образом). При этом реализация основных сценариев обеспечения защищенности будет явно пересекаться с защитой самой среды, на которой построены данные сервисы.

Готовы ли средства защиты виртуализированных сред к их интеграции в такие комплексы верхнего уровня, как центры управления инцидентами ИБ и системы управления корпоративной ИБ? Есть ли в этом потребность у российских заказчиков?

Распространенный вопрос заказчика, собирающегося построить защиту своей виртуализированной ИТ-среды, который он задает поставщикам средств защиты, — умеют ли их продукты работать с высокоуровневыми системами сбора и корреляции ИБ-событий и управления корпоративной ИБ. Тут, правда, нужно сделать поправку на отрасль, которую заказчик представляет. Как я уже говорил, компании разных отраслей находятся на разных уровнях зрелости ИБ. Соответственно и требования они предъявляют разные.

На рынке существуют ИБ-продукты, располагающие необходимыми интеграционными механизмами, а в продуктах Trend Micro такие возможности реализованы нативно.

Какой вызов безопасности виртуализированных сред вы относите к самым актуальным в настоящее время и в перспективе?

Прежде всего это функционирование средств защиты виртуальной среды без помех для работы тех ИТ-ресурсов, которые они защищают. Заказчики в первую очередь ориентируются на эти свойства при выборе ИБ-продуктов для виртуализированных ИТ-средств. Следующим по важности является вопрос обеспечения безопасности гипервизора.

В комплексных проектах заказчики начинают с задач несанкционированного доступа и сетевой безопасности — межсетевого экранирования и предотвращения вторжений.

Если же говорить о перспективе, то основные вызовы здесь связаны с развитием облачных ИТ-сервисов. Такие сервисы ориентированы прежде всего на бизнес-цели, а задачи ИБ отодвигаются на второй план. Даже компания Amazon в правилах пользования своими облачными сервисами ранее возлагала ответственность за ИБ на самих пользователей сервисов.

Хотя сегодня к вопросам безопасности облачных сервисов относятся более внимательно, нежели несколько лет назад, и нередко пытаются решать их одновременно с разработкой облачной архитектуры, довлеющими все же остаются вопросы стоимости и окупаемости таких проектов. Поэтому с ростом популярности облачных сервисов будет расширяться и спектр ИБ-угроз.

Пока это не слишком проявляется на практике ввиду все еще слабого распространения облачных сервисов. Но нужно отметить, что профессиональные ассоциации, такие как Cloud Security Alliance, уже активно работают над методами защиты подобных сервисов. Опираясь на их опыт, можно сделать вывод о том, что проблемы виртуализированных корпоративных сред пополнятся проблемами, связанными с облаками, среди которых в первую очередь следует упомянуть очистку данных на стороне провайдера облачных услуг при смене провайдера, шифрование данных, а также распределение прав доступа специалистов провайдера к клиентским ресурсам.

Как вы определяете комплексность защищенности виртуализированной ИТ-среды? Можно ли сегодня говорить о том, что она реализуема?

Думаю, что говорить об этом уже можно, поскольку некоторые из представленных на рынке систем защиты виртуальных сред, среди которых и наше решение Deep Security, могут интегрироваться как с платформами виртуализации, так и с внешними ИБ-системами (такими, например, как системы управления ИБ-инцидентами и защиты от несанкционированного доступа) и работать согласованно с ними как единый комплекс. При этом каждый из интегрированных компонентов решает свой круг задач.

Какие особенности характерны для специализированных ИБ-решений для защиты виртуализированных сред?

В виртуальной среде чрезвычайно важным является контроль целостности в реальном времени как всей среды, т. е. гипервизора, так и файлов и ключей реестра операционных систем и приложений, а также контроль нежелательного сетевого трафика.

Следующая особенность ИБ-решений заключается в том, что виртуальные машины могут пребывать долгое время в неактивном режиме, в результате средства антивирусной защиты устаревают, а необходимые критические обновления ОС и приложений отсутствуют. Одновременно возможно создание новых машин, не соответствующих корпоративной политике безопасности, например без средств антивирусной защиты. Указанные проблемы в Deep Security, например, решаются благодаря специальному компоненту Virtual Appliance, который устанавливается прямо в среду ESX-сервера и благодаря использованию средств API защищает сразу все виртуальные машины, работающие на защищаемом ESX.

Хотел бы отметить еще одно важное дополнение средств защиты корпоративных систем — виртуальный патчинг. Deep Security использует глубокий пакетный анализ для выявления и предотвращения атак, направленных на эксплуатацию уязвимостей в ОС и приложениях. Выделенный центр аналитиков информационной безопасности — Trend Micro Security Center — своевременно получает информацию об уязвимостях из десятков источников, таких как SANS, CERT, CVE, Bugtraq, VulnWatch, PacketStorm, Securiteam, а также непосредственно от производителей программного обеспечения, которые, например, участвуют в программе Microsoft Active Protections. На базе этой информации аналитики Security Center выпускают обновления правил для Deep Security, которые блокируют возможность использования уязвимостей, даже без установки патчей от производителей ПО.

О защите...

◂ ПРОДОЛЖЕНИЕ СО С. 19

изведанном виртуальном пространстве. Он, например, не видит адекватных методик оценки рисков и управления системой ИБ в публичных облаках и полагает, что в ближайшее время они не появятся; по его мнению, можно ожидать в скором времени только пилотные методики, но не индустриальные, стандартизованные методы.

Пользователи. Средств обеспечения безопасности ВС, как утверждает Михаил Чернышев, на рынке представлено много: от антивирусов до инструментов глубокого анализа трафика внутри виртуальной инфраструктуры. При их выборе и применении он рекомендует заказчикам руководствоваться принципом разумной достаточности. К примеру, если защита сети выстроена качественно и корпоративные ИБ-средства “знают”, что такое сигнатуры атак на гипервизор, то совершенно не обязательно бросаться на усиление безопасности сети — лучше обратить внимание на оптимизацию работы гостевых операционных систем, тем самым сосредоточившись на решении задачи защиты конечных точек.

По мнению Вячеслава Медведева, на российском ИБ-рынке сегодня есть не только все необходимые ИБ-продукты, но даже и методики, достаточные для обеспечения безопасности виртуализированных ИТ-сред. Дело, считает он, за заказчиками, которые, по его оценкам, пока не осознают уровня угроз, что, собственно, и затрудняет защиту таких сред.

Основным фактором, затрудняющим защиту виртуализированных ИТ-сред, г-н Чернышев называет простоту (в силу специфики средств виртуализации) проведения любого рода тестов в ВС. В итоге, говорит он, клиент оказывается в очень сложной ситуации, когда все протестированные решения его в общем-то устраивают, а окончательный выбор ему сделать непросто, поскольку формализовать свои требования в такой ситуации ему крайне тяжело.

К основной сложности обеспечения ИБ виртуализированной ИТ-среды Константин Воронков относит новизну технологии виртуализации. Корпоративные ИБ-службы, как он полагает, все еще плохо с нею знакомы, у них нет готовых для этой технологии ИБ-политик и правил обеспечения безопасной работы с нею. Традиционные ИБ-средства для технологии виртуализации подходят не всегда, а специализированные, как правило, поставляются по отдельности и являются сложно интегрируемыми с общей системой корпоративной ИБ. ИТ-специалисты только осваивают работу с этими новыми инструментами.

Константин Воронков отмечает, что в компаниях, особенно крупных, нередко возникает напряжение в отношениях между ИТ-департаментом и ИБ-службой, связанное с разделением ответственности за правильную настройку ИБ-решений, за их мониторинг и т. п. В случае с виртуализацией подобные функции (приводящие к конфликтам между ИТ- и ИБ-службами) оказываются еще более консолидированными, поскольку зачастую настройки самой ВС и решений для ▸

обеспечения ее защиты неотделимы друг от друга. Г-н Воронков полагает, что ИТ- и ИБ-подразделения обязаны искать общий язык, вырабатывать общие политики для того, чтобы грамотно и качественно защищать ВС.

Регулирование. По мнению Сергея Панина, из-за отсутствия регулятивных требований к защите виртуализированных ИТ-сред тормозится распространение виртуализации, и рынок ждет от регуляторов регламентирующих документов с описанием самих ВС и методик защиты хранимых в них данных. Он отмечает, что у ФСТЭК, одного из ведущих российских регуляторов в области ИБ, есть понимание того, что в отношении ВС следует вводить специальные критерии и признаки защищенности. Еще в 2012 г. из представителей экспертного сообщества была создана инициативная группа по разработке проекта стандарта безопасности ВС. Однако о результатах ее работы г-ну Панину пока ничего неизвестно.

Он напоминает, что для использования ВС в госструктурах необходимо, чтобы средства виртуализации были сертифицированы в соответствии с требованиями ФСТЭК и ФСБ. Однако поставщики средств виртуализации, как он считает, не могут позволить себе сертифицировать каждую новую версию своих продуктов (которые появляются довольно быстро на динамично развивающемся рынке виртуализации), что существенно сужает возможности построения защищенной ВС, удовлетворяющей требованиям, обязательным для госучреждений. Госструктурам, по мнению г-на Панина, сегодня гораздо проще (с позиции выполнения требований регуляторов) организовать обработку данных (особенно содержащих государственную тайну) без виртуализации.

Елизавета Спасенных отмечает, что ввиду недостаточности нормативной базы, регулирующей защиту виртуализированных ИТ-сред, и отсутствия рекомендаций по выбору и использованию мер и средств защиты ВС заказчикам приходится руководствоваться только здравой логикой и надеяться на то, что ряд сложностей будет снят оперативными действиями регуляторов, направленными на совершенствование нормативной базы.

В то же время, как отмечает Иван Бойцов, первые шаги регуляторами по актуализации российской нормативной базы в сторону защиты виртуализированных ИТ-сред уже сделаны. В частности, проекты приказов ФСТЭК по защите конфиденциальной информации в органах государственной власти и защите ИСПДн, которые находятся на регистрации в Минюсте, содержат ряд базовых требований по защите виртуализированных ИТ-ресурсов.

Несмотря на это, у регуляторов, считает г-н Бойцов, впереди еще много работы. По его наблюдениям, защита ВС никак не учитывается в требованиях к защите автоматизированных систем, в том числе обрабатывающих данные, представляющие собой государственную тайну, отсутствуют четкие требования к средствам защиты ВС (например, в формате профилей защиты, как это сделано для антивирусов и средств обнаружения вторжений).

Алексей Воронцов полагает, что большая часть представителей наших регуляторов всё еще мыслит с позиций физической инфраструктуры, и задачи вроде таких, как поставить сертифицированный во ФСТЭК межсетевой экран в виртуальную сеть или электронный замок на виртуальную машину, остаются вне нормативной базы. Вендоры, отмечает г-н Воронцов, пытаются восполнить нехватку сертифицированных средств защиты виртуализированных ИТ-сред, сертифицируя в качестве средств защиты свои продукты, предназначенные для обеспечения виртуализации ИТ-ресурсов. Однако, по его словам, это мало что дает помимо наклеенного на продукт знака соответствия нормативным требованиям.

По мнению Николая Романова, направление виртуализации в нашей стране не развивается достаточно свободно и регуляторы не препятствуют этому, а контролю с их стороны подвергаются либо сами средства защиты ВС, либо типы сервисов, построенные на базе этой технологии.

Алексей Сабанов полагает, что было бы неразумно требовать от наших регуляторов того, чего в мире (пока) не может никто. Российская регулятивная база, по его наблюдениям, всегда немного (а иногда сильно) запаздывает по отношению к регулятивным нормам развитых капиталистических стран. Но ведь на данный момент, говорит он, и там стандартов нет — есть только рекомендации, через некоторое время появятся требования по обеспечению ИБ виртуализированных сред, а потом и стандарты.

Тренды

Что касается подходов к обеспечению безопасности виртуализированных ИТ-ресурсов, то Вячеслав Медведев настоятельно рекомендует не забывать о пройденных технологических рубежах и накопленном эксплуатационном опыте. Он обращает внимание на то, что облачные ИТ-архитектуры и виртуализация ИТ-ресурсов являются частными случаями давно известных специалистам вычислительных систем с удаленным доступом, и напоминает, что первые компьютеры работали именно так: был сервер и к нему подключались рабочие места. Сегодня спираль развития совершает свой очередной виток.

Рассуждая о перспективах развития системы обеспечения безопасности ВС, Алексей Воронцов фактически оправдывает тех ИТ-специалистов, которые считают виртуализированные ИТ-ресурсы более безопасными, нежели невиртуализированные. Согласно его наблюдениям, пользователи и разработчики всё чаще рассматривают виртуализацию не только как способ экономии ИТ-ресурсов, но и как способ обеспечения информационной безопасности. Функционирование приложений и сервисов в изолированной ВС как возможность изоляции их друг от друга и от системных сервисов является, по его убеждению, плодотворным подходом к защите от атак, основанных на уязвимостях прикладного программного обеспечения. Он рассматривает его как одно из направлений развития виртуализации.

Константин Воронков отмечает, что поставщики средств виртуализации сами постоянно реализуют в своих продуктах новые, более эффективные способы защиты ВС (что является общим трендом в ИТ: ИТ-вендоры стремятся встраивать безопасность в жизненный цикл своих продуктов, начиная с этапа их разработки).

Перспективным г-ну Воронкову представляется развитие технологии Security as a Service. Она дает возможность реализовать, например, защиту по требованию виртуальных машин в ЦОДах силами провайдера ИБ-сервисов. Являясь результатом консолидации ИТ-ресурсов и постепенной передачи функций обеспечения информационной безопасности поставщикам услуг хостинга виртуальной инфраструктуры, SaaS особенно актуальна для малых и средних компаний, которые не имеют возможности создания собственных центров обработки данных и найма квалифицированных ИТ- и ИБ-специалистов.

Согласно наблюдениям Сергея Панина, индустрия ИТ и ИБ движется к консолидации управления их ресурсами. Одним из проявлений этого тренда является стремление ИБ-вендоров унифицировать свои решения в области защиты виртуализированных ИТ-сред. Г-н Панин предполагает, что на рынке появятся многофункциональные решения (например, объединяющие межсетевой экран, систему обнаружения и предотвращения вторжений, антивирусный шлюз, антиспам-функционал, средства веб-фильтрации, инструменты управления уязвимостями, средства контроля функционирования приложений и защиты баз данных), режим использования которых будет зависеть от затребованной заказчиком лицензии. Производители средств защиты ВС будут расширять линейки своих продуктов, добавляя к уже имеющимся новые компоненты по принципу “All-in-box”. При этом специализированные средства (скажем, средства резервного копирования, аутентификации и т. д.) также будут востребованы как нишевые. У ИБ-вендоров появится стимул интегрировать свои продукты с популярными облачными сервисами.

По оценкам Дмитрия Когая, изменения, связанные с эксплуатацией виртуализированных ИТ-сред, которые отразятся на обеспечении ее ИБ, проявятся уже в ближайшие два-три года, что, полагает он, будет продиктовано изменениями в условях функционирования отечественных бизнес-структур — изменениями не только технологическими, но и ментальными. До экономического кризиса вместе с ростом цен на нефть многие российские компании развивались стремительными темпами, выстраивали свои ИТ-инфраструктуры с заделом на будущее, и к настоящему времени в стране насчитывается немало таких ИТ-инфраструктур. У их владельцев (которые, согласно наблюдениям г-на Когая, в массе своей еще не вернулись на докризисный уровень) нет нужды в новых ИТ-решениях — те, которыми они располагают, вполне способны будут справляться со своими функциями еще два-три года.

Дмитрий Когай полагает, что к тому времени, когда российские компании восстановят после экономического кризиса свои бизнес-показатели, морально и физически устареют их ИТ-инфраструктуры, и бизнесу потребуется их обновление. И вот тогда отсутствие таких средств, какими они располагали в “тучные” докризисные времена, сделает, согласно его прогнозам, аутсорсинговую схему потребления ИТ-ресурсов, реализуемую посредством облачных архитектур, насущной потребностью российского бизнеса.

У российских компаний, предполагает г-н Когай, должно поменяться отношение к “зеленым” технологиям, в первую очередь к энергосберегающим, интерес к которым в нашей стране сегодня практически отсутствует в силу того, что расходы на электроэнергию не столь высоки, как в других странах. Однако уже в будущем году тарифы на электричество в России, вероятно, сравняются с тарифами США, а еще через год-два будут на уровне западноевропейских. Это означает, что в какой-то момент более “зеленые” предприятия станут опережать своих конкурентов в плане рентабельности. Г-н Когай рекомендует готовиться уже сегодня к внедрению “зеленых” технологий, с тем чтобы завтра с их помощью оптимизировать расходы, в том числе на электроэнергию.

Он обращает внимание ИТ- и ИБ-вендоров, интеграторов и регуляторов на то, что к тому времени, когда предприятия восстановятся после кризиса, большая часть технических вопросов, связанных с использованием ИТ, должна быть уже отработана, включая и те из них, которые относятся к обеспечению (на востребованном пользователями уровне) информационной безопасности в виртуальных и облачных средах.

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

Аутсорсинг теряет свою привлекательность?

САМУЭЛЬ ГРИНГАРД

Последние пара десятилетий ознаменовались циклическим развитием аутсорсинговых инициатив. Сегодня практически невозможно найти компанию из списка 2000 наиболее крупных глобальных организаций, которая бы не отдавала на аутсорсинг какой-либо вид бизнес-деятельности или ИТ-задачи. Однако недавно обнародованный доклад Deloitte Consulting под названием "От Бенгалуру до Бостона: тенденция возвращения ИТ в организации" утверждает, что некоторые компании сворачивают аутсорсинговые инициативы и возвращают исполнение некоторых ИТ-задач в собственные подразделения.

Дейн Андерсон, директор Deloitte Consulting, описывает ситуацию как "незначительный, но развивающийся тренд". Тенденция основывается на возвращении к инсорсингу по причине низкого качества обслуживания, оплошностей и сбоев со стороны поставщиков аутсорсинговых услуг. Во многих случаях возможность сэкономить не оправдывает оттока клиентов, недовольных результатом.

Консалтинговое агентство, опросившее в ходе подготовки исследования представителей 22 ведущих отраслей в 23 странах мира, выяснило, что 48% респондентов расторгли контракт с аутсорсинговой компанией по причине невыполнения подрядчиком обязательств или неудобств в работе. Более того, 34% респондентов, разорвавших договор, решили продолжить работу силами своей компании.

В целом 62% респондентов сообщили, что для них было "очень важно" улучшить качество обслуживания и поддержки клиентов, а другие 38% охарактеризовали эту задачу как "важную". При этом 77% респондентов подчеркнули, что цена вопроса тоже была фактором, оправдавшим переход к инсорсингу.

Консалтинговое агентство выяснило, что 48% респондентов расторгли контракт с аутсорсером из-за невыполнения им обязательств или неудобств в работе.

"Нам показалось, что такой результат нелогичен, так как снижение издержек — это основная причина того, почему компании обращаются к аутсорсингу, — отметил Андерсон. — Однако полученные ответы могут означать, что качество работы аутсорсинговых поставщиков могло не соответствовать ожиданиям клиентов относительно снижения затрат или выполнения других задач".

Другими ключевыми факторами, послужившими причиной возвращения ИТ в организации, стали: желание лучше контролировать процессы (77%), переход к более гибким моделям использования человеческих ресурсов (77%), стремление консолидировать имеющиеся активы (69%), стремление повысить свою конкурентоспособность (62%), желание использовать новые технологии (54%) и возможность добиться налоговых послаблений (38%).

В целом 21% компаний, вернувшихся к практике инсорсинга, признаются, что они "очень довольны" результатами; 58% "довольны" и 21% относится к переходу "нейтрально".

Deloitte отмечает, что перед компаниями, возвращающимися к инсорсингу, стоит несколько проблем. Одной из основных можно считать неудовлетворительный уровень передачи знаний. Это часто происходит, если компания, расторгнувшая контракт по причине невыполнения ее требований, не может обеспечить наём осведомленных сотрудников из стана аутсорсера.

Другими преградами на пути успешного перехода к инсорсинговой модели считаются необходимость расширения внутренних возможностей, например по управлению поставками, и понимание, что реализация этого плана может повлечь за собой увеличение затрат, особенно на ранних стадиях перехода.

"Аутсорсинг до сих пор считается преобладающей моделью на рынке, — заключил Андерсон. — Но при этом наблюдается незначительный, но растущий обратный тренд в отдельных ситуациях и относительно исполнения конкретных функций. Компании, стремящиеся использовать инсорсинговую модель, должны отдавать себе отчет в том, что на этапе расторжения контракта могут возникнуть проблемы. Любые инициативы перехода на инсорсинг должны начинаться с составления подробного бизнес-плана и расчета затрат на переходный период".

НПП и НФАП...

◀ ПРОДОЛЖЕНИЕ СО С. 15

ектные и программные решения, а также конфигурации. Что касается зоны ответственности, то разработчикам типовых проектных решений для Минздрава позволено иметь "полуадминистративный" доступ к своему разделу, в котором хранится такое решение. Пользователям ФАП разрешено оставлять соответствующие комментарии, отзывы и т. п. с тем, чтобы потенциальные клиенты могли ознакомиться с проблемами внедрения и поддержки, узнать стоимость услуг и оценить конкурентное типовое проектное решение. Что касается СПО, то оно выложено в открытом доступе — это OpenOffice, MySpace, дистрибутивы Linux. Пользователю предоставляется виртуальная машина для сборки дистрибутива с автоматической проверкой на вирусы. Каждый файл сопровождается лицензией и электронной подписью человека, загрузившего его в ФАП, что обуславливает персональную ответственность за ПО.

Инфраструктура

При создании инфраструктуры НПП, считает Дмитрий Комиссаров, ни одно мероприятие более чем на 10% (по объемам работ) не выполнено, фактически сделаны только первые шаги в этом направлении. Задач, требующих решения, еще очень много. Сейчас НФАП включает прототипы ОС, системы сборки и т. д.

Для дальнейшего формирования и поддержки НФАП требуется выбрать оператора. "В качестве такового мы рекомендовали Минкомсвязи "Интеграл"", — рассказал г-н Комиссаров. Однако сейчас в качестве оператора в министерстве рассматриваются НИИ "Восход" и Ростелеком.

Следующий нерешенный вопрос — это регламенты. Их нужно разработать и внести на рассмотрение, под них нужно принять постановление Правительства. По его мнению, здесь работы еще года на полтора. Так, в НФАП должна быть закрытая часть: в ней хранится ПО под грифами ("секретно" и т. п.) или под соответствующей сертификацией, т. е. там много работы, за нее никто еще не брался. И здесь нужно получить мнения от ФСБ, ФСТЭК и других регуляторов.

Павел Фролов согласен с оценкой выполненного объема работ, которую дал г-н Комиссаров, но предлагает иметь в виду, что уже существуют продукты на базе СПО, внедренные в различных ведомствах страны. Эти продукты, по его мнению, уже можно включать в НПП в виде типовых проектных решений. Кроме того, у разработчиков СПО создана инфраструктура. В первую очередь имеются в виду разработчики ОС, у которых решены такие вопросы, как хранение пакетов ПО и их автоматизированная пересборка; в частности, компании РОСА и "Альт Линукс" имеют всю необходимую инфраструктуру. Таким образом, полагает он, в стране существуют как минимум три игрока, в числе которых РОСА и "Альт Линукс", которые могут закрыть потребности для НПП на уровне базового СПО, "а это уже немало, это уже шаг вперед, так как пять лет назад в этой области не было ни одного игрока, поскольку тогда были проблемы, требовавшие решения".

"Я не сомневаюсь, что когда государство вновь проявит интерес к НПП, эти имеющиеся наработки вместе помогут в части инфраструктуры совершить прыжок с 5 до 15—20% от уровня реализации программы", — сказал Павел Фролов.

В то же время некоторые эксперты дали более пессимистическую оценку, полагая, что хотя концепция инфраструктуры и проработана и имеются базовые ресурсы, но надо еще собрать работоспособную систему.

Президент РАСПО Юлия Овчинникова уверена: "В НПП заложены основы для создания ИТ-инфраструктуры в России и условия развития ПО, в том числе и СПО".

ПОДПИШИСЬ НА 2013 ГОД

СК ПРЕСС

PC WEEK RUSSIAN EDITION

Я подписываюсь

☐ на 6 месяцев и плачу за 17 журналов 1020 рублей (в т. ч. НДС 10%)

☐ на 12 месяцев и плачу за 35 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

Стоимость подписки:

На 6 месяцев (17 журналов) — 1020 рублей (в т. ч. НДС 10%)

На 12 месяцев (35 журналов) — 2100 рублей (в т. ч. НДС 10%)

Данное предложение на подписку и указанные цены действительны до 30.06.2013

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: podpiska@skpress.ru.

В случае если Вам не доставляют издания по подписке, сообщите об этом по e-mail: pretenzii@skpress.ru.