ГАЗЕТА ДЛЯ КОРПОРАТИВНЫХ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

PCWEEK UKRAINIAN EDITION

Pelican Publishing

КОМПЬЮТЕРНАЯ НЕДЕЛЯ PCWEEK.UA • 24 ФЕВРАЛЯ — 9 МАРТА • 2011 • №3 (03) • КИЕВ

HP поборется за сегмент Mission Critical

СЕРГЕЙ МИШКО

По признанию Сергея Сергеева, специалиста по бизнес-критичным системам HP, в денежном выражении глобальный рынок серверов на базе отличных от x86 архитектур продолжает сокращаться. Причин тому несколько: появление систем на высокопроизводительных 8-ядерных процессорах Intel Xeon, которые могут перебрать на себя выполнение части бизнес-критичных задач, низкая осведомленность специалистов о преимуществах тяжелых решений на базе семейства ОС Unix, активная маркетинговая политика Microsoft и VMware по продвижению программных инструментов для x86-архитектуры, наконец, избыточные запасы оборудования у многих заказчиков после кризиса. Очевидно, перечисленные причины и послужили поводом для компании HP в очередной раз напомнить о стратегии развития собственных бизнес-критичных решений.

СЕРВЕРЫ

Эрик Марторел: «За последние 18 месяцев сотни компаний отказались от бизнес-критичных систем IBM и Oracle в пользу HP»

Согласно приведенным данным IDC, за период с 2004 по 2010 гг. в регионе CEE (Central Eastern Europe) доля HP находилась в коридоре 35—55%, что соответствует монопольному положению лидера на рынке. В Украине за три квартала прошлого года доходы HP составили 5,65 млн долл. — это 43,8% от общего объема рынка. Сам по себе неплохой результат, но без итогов четвертого квартала он не позволяет ничего определенного сказать про успехи или неудачи компании в сравнении с 2009-м, как отмечает большинство экспертов, самым сложным для ИТ-индустрии годом. Между тем, в 2009 году доходы от продаж систем HP Integrity на базе Intel Itanium в Украине достигли 12,17 млн долл. при рыночной доле в 54%!

Повторить превосходный результат 2009 года (падение в сравнении с докризисным периодом составило всего чуть более 11%) в 2010 году HP едва ли удастся повторить даже в случае очень хороших результатов четвертого квартала. Кстати, их обещают обнародовать буквально на днях, но на момент подготовки материала они неизвестны. И причина здесь, похоже, не в просчетах менеджеров или в недостатках решений HP, сколько в продолжающемся сокращении сегмента бизнес-критичных систем в Украине (HP прогнозирует

ПРОДОЛЖЕНИЕ НА С. 6 ▶

Остатки харизмы Nokia ликвидированы соглашением с Microsoft

ЕЛЕНА ГОРЕТКИНА, ВЛАДИМИР МИТИН

Microsoft и Nokia заключили исторически важное соглашение, в результате которого Nokia, вложившая много сил и средств в разработку собственной ОС Symbian, будет выпускать смартфоны на базе некогда конкурирующей ОС Windows Phone. Остается только гадать, почему в качестве заменителя Symbian была выбрана не стремительно набирающая обороты Android (ряд экспертов не исключал и такой вариант развития событий), а пока не очень-то популярная ОС Microsoft. Некоторые эксперты предполагают, что Nokia просто не сумела договориться с Google.

БИЗНЕС

Стивен Элоп и Стив Балмер надеются, что сделка принесет миллиарды долларов. Свежо предание, да верится с трудом

Похоже, первопричиной такого решения стало неумение с умом потратить деньги, выделенные на НИОКР. По данным аналитической компании Bernstein Research, в минувшем году финский производитель потратил на НИОКР 3,9 млрд. долл., что почти в пять раз превышает смартфонные R&D-расходы Apple и почти в десять раз аналогичные расходы HTC (главного конкурента Nokia на рынке «неайфонных» коммуникаторов).

По мнению союзников, альянс сулит огромные преимущества. Так, глава Nokia Стивен Элоп считает, что сделка принесет миллиарды долларов. А Microsoft надеется укрепить положение на «горячем» рынке смартфонов, на котором сейчас доминируют Apple и производители устройств на базе Google Android, образуя двойку лидеров. Nokia и Microsoft собираются превратить эту двойку в тройку. Однако инвесторы и аналитики не разделяют такого оптимизма. После появления первых слухов об этом альянсе акции Nokia начали падать, и в результате за неделю их стоимость снизилась на 20%.

Неуверенность инвесторов вызвана несколькими причинами. Главная из них связана с тем, что в последнее время дела у Nokia идут неважно. Доля компании на рынке мобильных устройств сокращается уже в течение нескольких

ПРОДОЛЖЕНИЕ НА С. 6 ▶

В НОМЕРЕ:

Украинская власть посетила «Инком»

Премьер-министр Украины Николай Азаров и глава Государственного агентства по вопросам науки, инноваций и информации Владимир Семиноженко посетили компанию «Инком». В ходе официального полуторачасового визита высокие гости осмотрели производственный центр «Инком», познакомились с работой датацентра и ситуационного центра управления сетями компании «Датагруп», а также инновационных и учебных подразделений «Инком».

ИТ-СТРАТЕГИЯ

Во время визита высоким гостям показали инновационные системы отечественного производства.

Александр Федченко, президент компании «Инком», отметил: «Визит господина Азарова говорит, прежде всего, о том, что вопросы ИТ-отрасли являются для правительства Украины актуальными и своевременными. А состоявшийся диалог вселяет уверенность, что проблемы отрасли будут решаться на государственном уровне».

Александр Кардаков, председатель Наблюдательного совета компании «Октава Капитал», основатель компаний «Инком» и «Датагруп», представляя вниманию премьер-министра мощнейший узел, который управляет в круглосуточном режиме одной из крупнейших информационно-телекоммуникационных сетей Украины, акцентировал, что «дальнейшая судьба Украины зависит от того, как быстро мы сумеем перевести страну на инновационные рельсы. В этом вопросе важное значение играют внимание и поддержка со стороны государственных органов управления».

Во время визита премьер-министру и главе Госинформнауки были продемонстрированы инновационные системы и технологические новинки отечественного производства, среди которых компьютерная и серверная линейки Prime; разработанная специалистами «Инком» система видеонаблюдения с распознаванием номеров (для ГАИ) и фиксацией номеров для железнодорожных вагонов (для ЖД) и другие решения; спецтехника для выполнения задач технической защиты информации в сложных условиях эксплуатации, в том числе военного назначения, и другие решения.

Представляємо
нову серверну кімнату, повністю готову до експлуатації

Інтегрована система охолодження APC забезпечить найбільш економічно ефективну адаптацію вашої IT-кімнати відповідно до будь-яких майбутніх потреб

Блок кондиціювання рядного типу APC InRow забирає гаряче повітря безпосередньо з тильного боку серверних шаф, подаючи охолоджене повітря з фронтального боку шаф з IT-обладнанням.

Ваше серверне приміщення стало перешкодою на шляху запровадження нових технологій?

Консолідація, віртуалізація, конвергенція мереж, блейд-сервери — усі ці нові технології підвищують ефективність, скорочують витрати та дають змогу "отримувати кращий результат меншими зусиллями". Але вони також пов'язані з проблемами високої енергетичної щільності, охолодження та керування, які ніколи не бралися до уваги при проектуванні традиційних серверних залів. Ви покладаєтесь на власну інтуїцію, на можливості систем кондиціювання будівлі, впроваджуєте тимчасові рішення. А чи знаєте ви, як без зайвих витрат підвищити рівень надійності та ефективності управління в вашому серверному приміщенні?

APC by Schneider Electric пропонує комплексне рішення для серверних приміщень

Відтепер ви отримуєте всі необхідні системи електроживлення, охолодження, моніторингу та управління в одному інтегрованому рішенні, яке швидко та просто впроваджується в існуючому серверному приміщенні, не вимагаючи модернізації інженерних систем охолодження та електроживлення. Модульна конструкція з можливістю нарощування ресурсів у міру необхідності надає 100 % впевненість у тому, що ваш серверний зал ефективно працюватиме за будь-яких обставин.

Легко, економно та ефективно підготуйте вашу серверну кімнату для майбутніх завдань

APC позбавить вас клопоту пов'язаного з пошуком оптимальної конфігурації серверної кімнати. Автономні блоки охолодження InRow, монтажні шафи NetShelter з підтримкою високої енергетичної щільності і системи ізоляції повітряних коридорів APC можуть бути об'єднані для створення надійної екосистеми IT практично в будь-якому середовищі. Датчики моніторингу на рівні шафи, вбудовані у блок охолодження, автоматизовані елементи керування та інтегровані засоби програмного забезпечення створюють можливість отримання повного дистанційного контролю та цілковитого уявлення про стан усієї системи. Додайте систему безперебійного живлення (наприклад, найкращі у своєму класі ДБЖ Smart-UPS чи Symmetra), і ви отримаєте повнофункціональну систему для вирішення поточних та майбутніх завдань.

Якщо ви маєте окреме місце для IT-обладнання…

Отримайте готову систему охолодження для IT-обладнання високої щільності

Інтегрована система, що об'єднує блок прецизійного охолодження InRow SC, (охолоджуюча потужність до 7 кВт), монтажну шафу NetShelter SX та систему ізоляції повітряних коридорів Rack Air Containment зі спеціальною знижкою на обмежений період.

Якщо у вас немає відокремленого IT-простору…

Представляємо NetShelter CX: компактні серверні шафи з винятковою шумоізоляцією, пристосовані для відкритого офісного середовища.

У цих рішеннях компоненти електроживлення, вентиляції, охолодження та керування інтегровано в захищену, безшумну та охолоджену шафу, яка на вигляд не відрізняється від інших офісних меблів.

БЕЗКОШТОВНО завантажте інформаційні статті впродовж найближчих 30 днів і отримайте шанс ВИГРАТИ* моноблочний комп'ютер Lenovo з сенсорним екраном!

Завітайте на сайт www.apc.com/promo та введіть код 85798t

Тел.: +38 044 538-1478 • Факс: +38 044 538-1479

APC™ by Schneider Electric

APC by Schneider Electric, у Києві: 03057, Україна, Київ, вул. Металістів, 20 Т • Тел.: +38 044 538-1478, факс: +38 044 538-1479. Центр підтримки клієнтів: 0 800 502-7220, E-mail: apcukr@apc.com.

Зона .UA: полет успешный, но турбулентный

Олег Пилипенко

Глубина проникновения интернет-доступа в Украине в минувшем году превысила 33%, по итогам третьего квартала в стране насчитывалось около 13 миллионов регулярных пользователей Всемирной сети (по данным агентства InMind). В сравнении с 2009 годом это число выросло более чем в 1,5 раза: по состоянию на апрель позапрошлого года в стране насчитывалось всего 8 миллионов человек, регулярно бороздящих интернет-просторы. И все же 33% — это относительно немного в сравнении со странами Евросоюза, например, в Швеции уровень проникновения приближается к 85%.

ИНТЕРНЕТ

Минувший год был щедрым на довольно кардинальные события в развитии доменного пространства Украины. Во-первых, необычным явлением стала регистрация полукириллических доменов (IDN) в доменах COM.UA и KIEV.UA, начатая 19 октября 2010 года. Услуга довольно быстро обрела популярность, число делегированных IDN в com.ua и kiev.ua превысило 10 тысяч. При этом на улицах украинских городов уже можно видеть билборды с кириллизированными веб-адресами.

Во-вторых, компанией «Хостмастер» совместно с ICANN в Украине введен в действие локальный корневой сервер DNS, содержащий информацию о доменах верхнего уровня. Сервер является «зеркалом» одного из 13-ти корневых серверов ICANN, известного под названием «L-root».

Кроме того, с 15 июля 2010 года серверные кластеры ООО «Хостмастер», использующие технологию Anycast DNS, поддерживают адресацию IPv6, это новая версия протокола, которая создана в связи с предстоящим исчерпанием адресов IPv4. Она решает проблемы масштабирования и безопасности, свойственные предыдущей версии протокола.

На сегодняшний день услуги по регистрации кириллических доменов в Украине оказывают 48 компаний-регистраторов. Лидеры здесь те же, что и среди регистраторов традиционных доменных имен: это компании Imena.UA и «ДНС-Украина».

По словам Александра Ольшанского, президента компании Imena.UA, особых темпов роста в зоне украинского домена верхнего уровня .UA в 2010 г. не наблюдалось. Приблизительно так же можно оценить результаты развития в зонах второго уровня. Внедрение в 2010 году регистраций IDN-доменов в .UA на общий уровень развития также повлияли слабо. Их было зарегистрировано порядка 10 тысяч, что составило примерно 2% от украинской доменной зоны. Впрочем, потенциал роста у зоны .UA сегодня достаточно большой, отмечает Александр Ольшанский, однако для его реализации необходимо соблюдение некоторых условий.

Во-первых, следует упорядочить и сделать прозрачным порядок взаимодействия на всех уровнях доменной иерархии — регистратора, администратора и технического администратора. Обязательно должны быть разделены функции администратора и технического администратора: тот, кто исполняет правила, не должен их вырабатывать. «Ведь де-факто компания «Хостмастер» является сегодня техническим администратором, пытаясь в меру своих сил также выполнять функции администратора. Поскольку приходится совмещать обе функции, то это не всегда получается хорошо, страдает либо первая, либо вторая функция», — сетует А. Ольшанский.

Во-вторых — необходимо привести в порядок правила работы регистраторов, унифицировать их обязанности и ответственность. Следует понимать, что количество зарегистрированных доменов пропорционально доверию к институциональному устройству доменной зоны. А уровень этого доверия не в последнюю очередь зависит от их взаимодействия с регистратором. Очень важно, чтобы все регистраторы украинской доменной зоне использовали единые правила регистрации во всех публичных доменах. Поэтому услуга регистрации доменного имени в пределах страны должна быть универсальной.

В-третьих, нужно либерализовать правила регистрации в .UA, и, наконец, открыть зону. «Затянувшийся в Украине на 10 лет период приоритетной регистрации по торговым маркам — факт более, чем странный», — заключает А. Ольшанский.

Российский опыт показал, что регистрация кириллических доменов, в основном, оказалась скваттингом или же попытками от него защититься. О перспективе украинского кириллического домена говорить пока рано.

Что касается прогноза по развитию кириллических доменов в 2011 году и вопроса, стоит ли компании регистрировать домены как в латинице, так и в IDN, то российский опыт показал, что регистрация кириллических доменов в основном оказалась скваттингом или же попытками от него защититься. О перспективе украинского кириллического домена говорить пока рано. «Если же речь идет о полукириллических доменов в зоне .UA, то здесь я не вижу перспектив вообще. — говорит А. Ольшанский. — Однако регистрировать такие имена все же придется, поскольку так или иначе в процесс вмешиваются сквотеры, уводя трафик с «основного» домена. Но это вопрос скорее не к регистратору, а к специалисту по продвижению сайтов в интернете».

Касательно развития украинской доменной зоны в 2011 году, А. Ольшанский отметил прежде всего серьезное влияние на развитие украинской доменной зоны недавно принятого закона «О защите персональных данных». Причем, в силу своей нечеткой формулировки, создавшей неоднозначность в возможном истолковании, регистраторам придется «перестраховаться», изменить целый ряд процедур, которые опирались раньше на публичную доступность данных Whois. «Хочу подчеркнуть, что сама по себе информация в Whois персональными данными не является. Но из-за нечеткой формулировки в законе возникла возможность двойного толкования и как следствие — необходимость «закрыть» систему Whois. Таким образом, фактически была легализована услуга whois privacy, за которую наша компания боролась почти 5 лет. То есть, здесь мы получили неожиданную помощь. Теперь же эта услуга распространяется на всю страну, что тоже выглядит весьма странно», — резюмирует президент Imena.UA.

Кроме того, закон «О персональных данных» поднял очень важный вопрос — кто является владельцем той информации о клиенте, которая содержится в Whois, в базах данных регистраторов и администраторов доменов. На протяжении последних нескольких лет имели место попытки решить этот вопрос на юридическом уровне, но в этом году в силу своей актуальности он спровоцирует целый ряд изменений в процедурах управления доменами.

Свобода от догм и цен на ПО

Многие компании по-прежнему отдают предпочтение ПО с открытым исходным кодом (Open Source, OSS), что позволяет сократить затраты в области ИТ. Об этом сообщается в новом исследовании аналитической фирмы Gartner, в рамках которого с июля по август 2010 года был проведен опрос среди ИТ-руководителей 547 компаний из 11 стран.

АНАЛИТИКА

Свыше половины респондентов признались, что для важных и не очень задач используют открытый софт. 46% организаций работают с такими программами в особых проектах, 22% задействуют их во всех областях предприятия. Еще 21% ИТ-руководителей рассматривают возможность перейти на ПО с открытым кодом.

Помимо развития базовой инфраструктуры компании используют открытый софт для поддержки основной деятельности, включая управление данными и интеграцию, разработку приложений, совершенствование бизнес-процессов, безопасность, модернизацию ЦОД и виртуализацию — именно поэтому фирмы все больше уделяют внимание OSS, отметили в Gartner. С более глубоким пониманием и доступом к необходимым навыкам организации будут и впредь искать новое применение OSS. Хотя поиск открытых проектов для снижения расходов по-прежнему является основным фактором.

Наиболее популярным типом свободного ПО станет софт для управления серверами и БД. Уже сейчас в этих сферах свободный софт применяется в 52% случаев, а через год ожидается, что соответствующие доли рынка вырастут на 23% и 19% соответственно. Наименее популярным сегментом применения свободного ПО сейчас является электронное образование: на его долю приходится только 12%, но в следующем году ожидается рост до 32%.

По словам аналитиков, текущий уровень использования решений Open Source четко указывает на весомые перемены в ИТ-инфраструктуре компаний — ведь порядка 5 лет назад ПО с открытым кодом использовалось менее чем в 10% организаций. Оно за этот период времени в ИТ-среде росло примерно такими же темпами, какими проприетарное ПО теряло свою популярность.

«Конкурентные преимущества в области ИТ в последнее время играют все большую роль, и использование решений OSS может дать их компаниям. В частности, если компания может изменить код приложения, сделав его уникальным, она получает преимущество», — считают в Gartner.

Специалисты Gartner считают, что мир ожидает новая фаза развития Open Source. Подтверждением этого прогноза также являются данные исследовательской компании IDC, которая оценила, что к 2011 году мировой объем рынка Open Source достигнет показателя в 50 млрд долл.

5 заповедей по версии Gartner

В 2011 году, согласно прогнозам Gartner, доходы мирового рынка корпоративного ПО превысят 253 млрд долл., что на 7,5% больше, чем в 2010 году. Рыночное влияние SaaS, облачных услуг, ПО с открытым исходным кодом, индивидуализации и технологий Web 2.0 будут расширяться, в то время как развивающиеся страны, включая Бразилию, Россию, Индию и Китай (БРИК), проявят себя как двигатели роста и кардинальных инноваций.

АНАЛИТИКА

Gartner определила пять долгосрочных, всеобъемлющих и взаимозависимых тенденций, влияющих на корпоративное ПО:

Глобализация: включает консолидацию рынка и тенденции конвергенции технологий, а также связанных сообществ, слияний вендоров и поглощений. По мнению Gartner, в течение нескольких следующих лет сильно фрагментированные рынки ПО станут более структурированными и отмечены обширными сокращениями количества вендоров. Хотя предприятия конкурируют на мировом рынке, требования локализации — в том числе языков, культур и законов — должны будут поддерживаться.

Реализация: облачные вычисления, платформы в качестве службы PaaS и SaaS, в сочетании с широким распространением и мобильным доступом вызывают сомнения в вопросе закупок и поставок ПО организациям. Спрос на облачно-ориентированные решения будет расти на протяжении нескольких лет. Мобильные решения привели к появлению множества новых отраслевых рыночных инициатив, таких как мобильный банкинг, мобильная коммерция и удаленная диагностика в сфере здравоохранения.

Модернизация: в соответствии с тенденцией модернизации продолжают набирать обороты автоматизация и оптимизация бизнес- и рабочих процессов. Предприятия ожидают предоставления значительных ресурсов в 2011 году для обновления всех типов систем и ПО. Ключевым фактором модернизации является виртуализация.

Социализация: использование социальных сетей продолжает набирать обороты. В тенденции социализации, которая включает в себя персонализацию и совместную работу, Gartner прогнозирует, что рост внедрений унифицированных коммуникаций будет заметен в 2012 году, а вычисления местоположения и контекстно-зависимые получат большее развитие в 2013 году.

Вертикализация: Эта тенденция включает в себя цикл горизонтальных приложений, которые становятся все более заточенными для обслуживания конкретных отраслей промышленности. В развертывании новых программных решений общее для вендоров — изначально обеспечить обобщенную технологию, которая со временем может привести к более утонченно отраслевым и линейным бизнес-возможностям. Примерами являются бизнес-процессы обеспечения коммуникаций и приложения содержащие разнородный контент.

PCWEEK UKRAINIAN EDITION

СОДЕРЖАНИЕ

Топ-менеджеры ASUS рассказали о неттопах

Олег Пилипенко

Анжела Сю, региональный директор Asus по направлению ноутбуков и нетбуков, и Шарлотта Лю, продакт-менеджер Asus по направлению систем All-in-One и неттопов, во время своего визита в Киев рассказали о новых продуктах компании для потребительского и корпоративного рынков.

ПЕРСОНАЛЬНЫЕ КОМПЬЮТЕРЫ

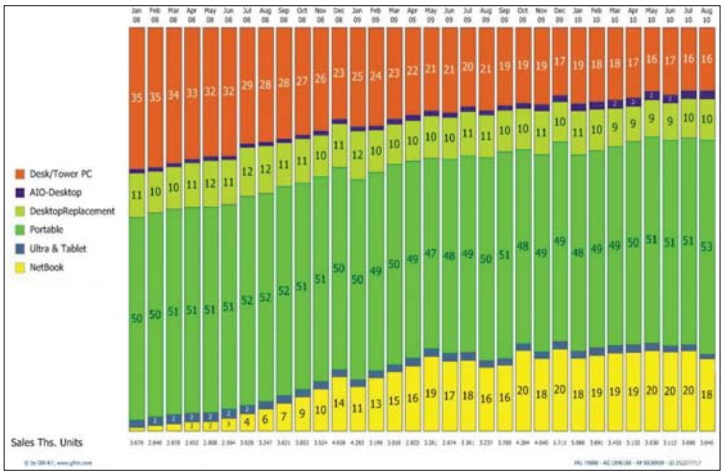
По мнению аналитиков, потребительский спрос на рынке настольных компьютеров все больше смещается в сторону неттопов и устройств класса All-in-One, при этом доля ПК с традиционным форм-фактором неуклонно снижается. Так, по данным Gartner, доля неттопов выросла с 5,4% в 2008 году до 6,5% в 3-м квартале 2010 года.

В то же время мировой спрос на продукты класса All-in-One (AIO) за последние три годы увеличился более чем в три раза. В 2010 их доля достигла 11—12% от общего объема проданных ПК. Наибольшим спросом AIO пользовались в Западной Европе (до 15%), а наименьшим — в странах СНГ (1%). Компания Asus вовремя уловила общемировую тенденцию и наладила производство неттопов под торговой маркой EeeBox, а также компьютеров All-in-One под маркой ET.

По словам Шарлотты Лю, среди основных преимуществ неттопов можно назвать очень низкое энергопотребление, всего лишь 15—30 Вт, небольшие размеры и бесшумность в работе. В 2011-м году компания готовит к выпуску продукты объемом всего 1 л и 1,5 л, которые можно будет смонтировать на задней панели монитора или под столом (с учетом тенденции минимизации электронных компонентов в скором будущем можно ожидать выпуска и поллитрового неттопа — прим. ред.).

В первом квартале 2011 года компания планирует выпустить новые модели на базе процессоров Intel Atom и чипсета nVidia ION, с оптическим приводом, портом USB 3.0 и ОС Windows 7 Premium на борту. Кстати, это будут самые миниатюрные устройства с оптическим приводом. Чипсет nVidia ION обеспечивает отличную производительность при воспроизведении full HD графики, что

ПРОДОЛЖЕНИЕ НА С. 6 ▶



Спрос на устройства класса All-in-One по регионам

АНОНСЫ

- **Тема номера PCWeek/UE №4 — Лучшие решения для офисной печати**
- **Интервью с начальником информационно-вычислительного центра Киевского национального университета им. Т. Шевченко Юрием Бойко**
- **Alpha Grissin Infotech — новый игрок на украинском рынке проектной дистрибуции**

Новости вашей компании, мнения о наших публикациях, приглашения на конференции и семинары, ваши пожелания высылайте по адресу:
press@skukraine.com

УПОМИНАНИЕ ФИРМ В НОМЕРЕ

EATON

Powering Business Worldwide

www.eaton.com/powerquality

Сервисные центры

Гарантийное и послегарантийное обслуживание оборудования Eaton на территории Украины осуществляется через сеть авторизированных сервисных центров.

Киев Мегатрейд-сервис +380 44 538 00 06
(Координатор сервисной сети)

Днепропетровск	Фирма «ВИСТ»	+380 44 4015544
Донецк	ООО «НПП АМИ»	+380 62 3450192
Житомир	СЭТ	+380 41 2418420
Запорожье	Рома-Сервис	+380 61 2125169
Ивано-Франковск	Технополис	+380 342 501222
Киев	DataLux Сервис	+380 44 4961790 (91,92)
Киев	ООО «БМС Сервис»	+380 44 4015544
Львов	Сервис компьютерной техники	+380 32 2440430
Одесса	Неоноджик	+380 48 7283728
Севастополь	Компасс-АйТи	+380 69 2452060
Сумы	НПФ Демекс Компьютер	+380 54 2601111
Харьков	Элсервис-М	+380 57 7141313
Черкассы	МегаСтайл	+380 47 2540150

Уменьшая занимаемое пространство, увеличиваем выходную мощность.

Если рабочее пространство шкафа ограничено, но требуется длительное время резервирования при значительной мощности потребления, – **Eaton** предлагает решение для защиты вашего ответственного оборудования. ИБП **Eaton 5130, 9130, 9135** и **9140** – часть серии **Powerware** с большой плотностью мощности (до 10 кВА) и широким диапазоном размеров.

Работая в режиме высокого КПД, эти ИБП потребляют значительно меньше энергии и менее требовательны к охлаждению.

МЕГАТРЕЙД
СПЕЦІАЛІЗОВАНИЙ ІТ-ДИСТРИБУТОР

Официальный дистрибутор в Украине
ул. Смоленская, 31-33, корп. 3, Киев 03005, Украина
т.: +380 44 538 00 06, ф.: +380 44 538 00 16
E-mail: office@megatrade.ua
www.megatrade.ua

Pelican Publishing PCWEEK UKRAINIAN EDITION

Учредитель «Пеликан Паблишинг»

Издатель ООО «СК Украина»

Директор
НАТАЛЬЯ ПРОЦЕНКО

Редакция

Редакционный директор
СЕРГЕЙ МИШКО

Главный редактор
ОЛЕГ ПИЛИПЕНКО

Над номером работали:

ВЛАДИМИР БОЙКО
ОЛЕГ ЕРМОЛЕНКО

Литературный редактор
ИРИНА МИЩЕНКО

Главный дизайнер
КСЕНИЯ БАСЕНКО

Тел./факс: (044) 361-70-57
E-mail: press@skukraine.com

Отдел рекламы

Менеджер по продажам
ВАЛЕРИЯ ДОНСКАЯ

Тел./факс: (044) 361-70-57
E-mail: advertisting@skukraine.com

Распространение

(044) 361-70-57

04050, Украина, Киев,
Гоголевская, 49, офис 30

PCWEEK/Ukrainian Edition. Газета печатается по лицензионному соглашению с компанией Ziff Davis Publishing Inc.

Газета зарегистрирована Государственным комитетом телевидения и радиовещания Украины.
Свидетельство о регистрации № 9892 от 27.05.05

Печать: ПрАТ «Издательство «Киевская Правда»
04136, г. Киев,
ул. М. Гречко, 13
тел./факс: (044) 422 57 75

PCWeek/UE выходит один раз в две недели. Распространяется по подписке.

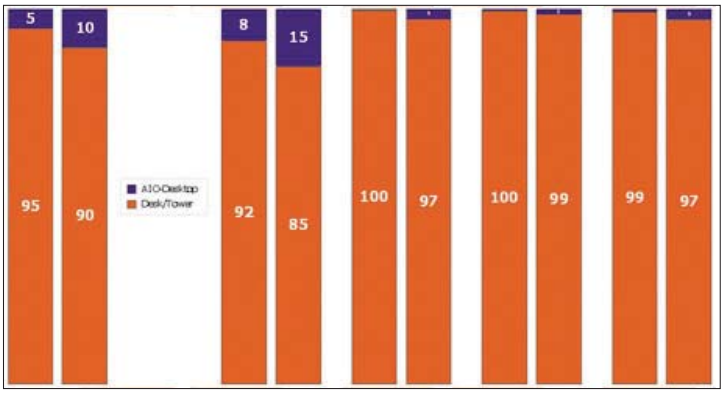
Тираж 10 000 экземпляров

Топ-менеджеры...

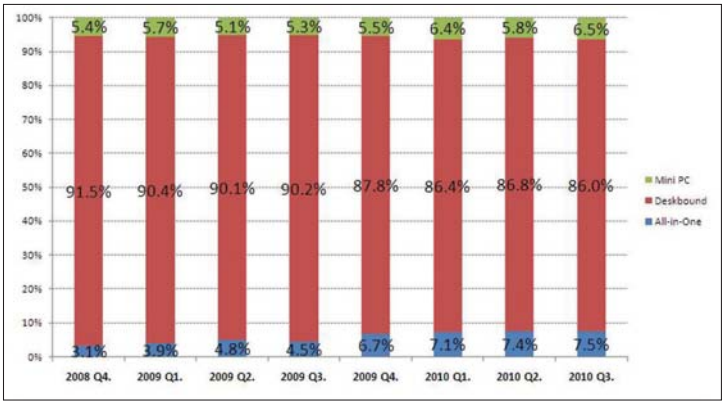
◀ ПРОДОЛЖЕНИЕ СО С. 4

позволяет использовать устройство в качестве мультимедиа-центра. Во-втором квартале намечается выход однолитрового неттопа на базе AMD Brazos E350, также с портом USB 3.0 и Win 7 Premium на борту. Устройство потребляет на 70% меньше электроэнергии, чем стандартный настольный ПК. Некоторые продукты, помимо портов USB 2.0 и 3.0, также оснащены устройством для считывания SD-карт и портом eSata.

В категории AIO компания Asus выпускает продукты трех типов: 16-дюймовые POS-терминалы для корпоративного рынка, компьютеры для ежедневной работы с диагональю экрана 20" и 21,5", а также устройства класса Entertainment с самым большим дисплеем 23.6" и 27". Компьютеры поставляются как с сенсорным экраном, так и с обычным, с установленным ТВ-тюнером и без него. В качестве вычислительной платформы используются процессоры Intel Core i3/i5. Технические характеристики All-in-One от Asus достаточно внушительные: до 8НБ ОЗУ, до 1 ТБ жесткий диск. Во-втором квартале 2011 года планируется миграция на платформу Sandybridge. Посредством HDMI-порта к компьютеру можно подключить различные мультимедиа-устройства, такие как фото и видеокамера, DVD-плеер и т. д. Комбинация двух скоростных интерфейсов — USB 3.0 и HDMI — делают All-in-One очень удобными для подключения мобильных устройств.



Спрос на устройства класса All-in-One по регионам



Соотношение продаж неттопов, стандартных ПК и AIO на мировом рынке. Источник: Gartner

Остатки харизмы...

◀ ПРОДОЛЖЕНИЕ СО С. 1

кварталов. Инвесторы сомневаются, что союз с Microsoft исправит положение Nokia. Хотя компания остается лидером рынка мобильных телефонов, она постепенно уступает позиции конкурентам, таким как Apple и производители Android-смартфонов.

Некоторые аналитики находят союз Nokia с Microsoft весьма рискованным. Ведь Microsoft пока так и не преуспела на мобильном рынке, хотя представила Windows Phone 7 еще в прошлом году. Поэтому участникам альянса нужно будет приложить максимум усилий, чтобы догнать Apple и Google, и действовать очень быстро и без сбоев. Однако наблюдатели сомневаются, что это им удастся, поскольку обе компании не славились быстротой реакции. К тому же никаких конкретных планов они пока не представили. Глава Microsoft Стив Балмер лишь выразил уверенность, что вместе союзники будут двигаться вперед быстрее, чем раньше.

НОВОСТИ

ВНЕДРЕНИЯ

МАУ на продуктах KOSS

Компания «Лаборатория Касперского» сообщает о поставке авиакомпании Международные авиалинии Украины программного комплекса для централизованной защиты рабочих станций, файловых серверов и мобильных устройств — Kaspersky Business Space Security. Поставку осуществил партнер «Лаборатории Касперского», компания «Объединение ЮГ».

«За последние 7 лет наша компания значительно выросла: увеличился штат сотрудников, возросли объемы пассажирских перевозок, повысились в том числе и требования к обеспечению безопасности информационных активов компании. И это неудивительно. Ежедневно МАУ обрабатывает тысячи файлов, которые содержат информацию о полетах, стыковках и пассажирах.

HP поборется...

◀ ПРОДОЛЖЕНИЕ СО С. 1

его объем в 2010 году на уровне 18 млн долл. против 22,55 млн долл. в 2009-м) и активизации конкурентов. Последнее обстоятельство как раз хорошо объясняет открытое сравнение на проходившей пресс-конференции представителями HP собственных решений с предложениями IBM и Oracle. По словам Сергея Сергеева, в денежном выражении мировой рынок мэйнфреймов сейчас демонстрирует рост. Как хорошо известно, эта вотчина принадлежит IBM.

Эрик Марторел, директор по продажам бизнес-критичных серверных решений HP в регионе EMEA, рекомендует больше обращать внимания не на результаты синтетических тестов, а на предпочтения реальных заказчиков. По результатам проведенного в 2009 году опроса Latest Gabriel Consulting Group системы HP под управлением ОС HP-UX обгоняют ближайших конкурентов по показателям производительности, управляемости, качества, доступности и надежности. Часть презентации г-на Марторела была посвящена миграции на HP-UX с платформ IBM и Oracle. Основным недостатком первых в HP считают низкую производительность на операциях ввода-вывода (она особенно важна, в частности, для систем core banking и биллинга), вторых — ограниченный роадмап серверов Sun SPARC Enterprise M-серии и сопутствующие с этим риски.

В прошлом году HP впервые ввела понятие отказоустойчивой конвергентной ИТ-инфраструктуры для решения бизнес-критичных задач, которая включает сетевое оборудование, серверы, СХД, ПО и набор сервисов по интеграции и запуску этих систем. Ильдар Ахметов, менеджер по бизнес-критичным серверным решениям HP в странах СНГ, отмечает четыре ее основных преимущества.

1. Упрощение и унификация ИТ за счет применения различных бизнес-критичных серверов из единого модельного ряда HP — Superdome2, лезвий Integrity и Integrity NonStop BladeSystem, способную объединять до 4080 нод.
2. Принцип отказоустойчивости от процессора до системы в целом гарантирует минимальное запланированное и незапланированное время простоя.
3. Динамическая оптимизация дает возможность оценивать доступные ресурсы и перераспределять в зависимости от нужд бизнеса.
4. Защита инвестиций и стабильность предполагает 10 лет поддержки для Superdome2, бинарную совместимость с последними поколениями продуктов и открытый роадмап с долговременными обязательствами.

Ильдар Ахметов рассчитывает на хорошие итоги продаж бизнес-критичных систем HP в четвертом квартале, но точных цифр пока не называет

HP BladeSystem Matrix под управлением HP-UX стала первой бизнес-критичной платформой компании для развертывания конвергентной инфраструктуры. Решение «все в одном» призвано существенно ускорить внедрение сложных информационно-вычислительных сред и запуск на их основе ИТ-сервисов. В зависимости от сложности задачи весь процесс отнимает от часа до двух суток. На сайте HP можно найти несколько десятков шаблонов для наиболее распространенных корпоративных приложений Microsoft, Oracle, SAP, SAS и других. BladeSystem Matrix включает серверы управления Integrity или ProLiant, блейд-шасси и серверы для них, СХД EVA StorageWorks EVA4400 или LeftHand, ПО BladeSystem Matrix Infrastructure Operating Environment. Предусмотрен starter kit, который позволяет заказчикам постепенно докупать необходимое аппаратное и программное обеспечение.

КОМПЛЕКСНІ РІШЕННЯ для побудови ЦЕНТРІВ ОБРОБКИ ДАНИХ

Компанія «МЕГАТРЕЙД»

є офіційним дистрибутором в Україні провідних світових IT-виробників:

- **Телекомунікаційні шафи:**
  Conteg
  Schroff
  Panduit
- **Системи безперевного електроживлення:**
  Eaton
  Delta

- **Активне мережне обладнання:**
  Cisco
  Alcatel-Lucent
  Aten
  RAD
- **Системи охолодження та вентиляції:**
  Stulz

- **Системи резервного електроживлення:**
  Europower
  Gesan
  Inmesol
- **Серверне обладнання та системи збереження даних:**
  IBM
  Cisco

- **Кабельні системи та аксесуари:**
  AMP Netconnect
  Panduit
- **Програмне забезпечення:**
  Microsoft
  Oracle
  Parallels

З повним переліком IT-виробників, офіційним дистрибутором яких є компанія «МЕГАТРЕЙД», Ви можете ознайомитися на сайті www.megatrade.ua

МЕГАТРЕЙД
СПЕЦІАЛІЗОВАНИЙ IT-ДИСТРИБУТОР

Найбільший український спеціалізований IT-дистрибутор

Вул. Смоленська, 31-33, корп. 3, Київ, 03005, Україна
т.: +380 44 538 00 06, ф.: +380 44 538 00 16
E-mail: office@megatrade.ua
www.megatrade.ua

ИНТЕРВЬЮ С ИТ-ДИРЕКТОРОМ

Швейцарские качества Сбербанка России в Украине

СЕРГЕЙ МИШКО

Сергей Иванович Адаменко, заместитель председателя правления ПАО «Дочерний банк Сбербанка России в Украине» (ДБСР), принимал участие в рамках темы номера PCWeek/UE №2 от 10 февраля. С тех пор ассоциация украинских банков (АУБ) успела обновить показатели деятельности финансовых учреждений — за месяц ДБСР продвинулся вверх по списку сразу на несколько пунктов. По состоянию на 1 января 2011 года банк, чья история в Украине берет свое начало с приобретения в 2007 году Сбербанком России небольшого ЗАО «Банк НРБ», занимает 21-е место по размеру капитала (1,53 млрд грн) и объемам активов (9,92 млрд грн).

ИНТЕРВЬЮ

PCWeek/UE: Сергей Иванович, в рейтинге АУБ ваш банк постепенно отвоевывает все более высокие строчки. Как вы можете охарактеризовать текущее положение дел в банке?

СЕРГЕЙ АДАМЕНКО: Сбербанк можно отнести к категории банков, которые по сегодняшнему состоянию рынка развиваются быстро. Не агрессивно, но динамично. В течение ближайших 3—4 лет мы сохраним те же темпы роста, что и сейчас. Вы это сможете оценить как по количеству отделений, так и по качеству услуг и перечню банковских продуктов.

Сейчас мы имеем небольшой и достаточно плоский продуктовый ряд. Но мы не торопимся предлагать некондиционные продукты, ведь нет ничего хуже, чем вызвать недовольство потребителя. Продать это второй раз будет очень тяжело. Если услуга целесообразна, будем над ней работать, и предложим ее клиентам только когда доведем до совершенства.

PCWeek/UE: Можно сказать, что украинская «дочка» Сбербанка России занимает особое место на рынке финансовых услуг. Еще вчера небольшой и малоизвестный в нашей стране банк сейчас очень быстро растет и активно наращивает свое присутствие. Как это соотносится с принятой стратегией развития ИТ-инфраструктуры?

С.А.: Размерность банка, скорее, является показателем масштаба проблем, с которыми ему приходится сталкиваться. Я бы сказал, что для большинства крупных банков новые технологические инновации менее доступны. По разным причинам. Часто тяжелое наследие и наслоение разных технологических платформ не позволяют применить новое решение по определению.

В этом плане у нас есть некоторое преимущество. Когда мы подходили к конструированию банка, год или полтора мы боролись с той организацией, которую купил Сбер (НРБ — прим. ред.). Наследие оказалось, возможно, не фатальным, но, тем не менее, оно доставляло достаточно неудобств. Поэтому речь зашла не о расчистке, а о создании новой платформы — сохранять было нечего. Именно небольшой размер банка позволил рискнуть и начать строить новую платформу. Причем не в течение 3—5 лет или 10 лет, как у большого банка, а за полтора-два года.

То есть ты никак не модернизируешь маленькую убогую систему, а рядом строишь новую. Потом просто переходишь на нее и дальше уже начинаешь расти с учетом новой платформы. В нашем случае это стало возможным в разумные сроки, а размер инвестиций не оказался фатальным для материнской компании. Без серьезного инвестора готового предоставить финансовые и временные ресурсы, привлечь достаточно умных людей, небольшой банк не сумеет осуществить проект подобного рода. Но если правильно сформированное ядро уже есть, расти вместе с ним несложно, подключая к нему все новые отделения.

Технологическое наследие больших банков формировалось 10—15 лет назад. По современным меркам это очень много. Даже на уровне обычных гаджетов мы не успеваем угнаться за технологиями — каждый год выходит новый iPhone, новый iPad, новые программы. Я поражен, ты заходишь на App Store, и если год назад там было пару тысяч приложений, то сегодня только в одном разделе, например, «Финансы», их больше тысячи. Тысячи программ, которые даже мельком просмотреть и оценить тяжело! Но каждая предлагает пользователю некоторые дополнительные возможности.

Например, мне не составляет труда, разговаривая с вами, ответить на вопрос, что будет с золотом. Очень удобная программка Wall Tracker, iPhone и высокоскоростной Wi-Fi-доступ в интернет позволяют мне узнать динамику изменения цен на золото за интересующий период всего за 10 секунд! То же самое касается стоимости серебра или нефти. Иметь оперативный доступ к информации подобного рода очень важно для финансистов. Она помогает принять правильное решение при формировании мультивалютной корзины для VIP-клиентов, которые преследуют цель извлечения максимальной прибыли от размещения активов в банке.

PCWeek/UE: Судя по динамике роста ДБСР, постепенно он тоже перейдет в разряд крупных банков. Не получится ли так, что новые технологии, заложенные в ядро ИТ-инфраструктуры сейчас, по мере развития банка начнут устаревать, и вы столкнетесь с проблемами, свойственным большим финансовым учреждениям?

С.А.: Стать большими мы планируем через три-четыре года, когда у нас будет не 80 отделений, а 300 или 350. То, что мы создаем сегодня, существенно снизит или даже сведет на нет последствия через каких-нибудь 5—7 лет. Мы построили однотипную среду. Ядро корпоративной сети и все сопутствующее оборудование, включая Wi-Fi-точки, — от Cisco Systems, все сервера, которые стоят у нас внизу в ЦОД (ЦОД ДБСР расположен в здании главного офиса на ул. Владимирской в Киеве — прим. ред.) — только IBM, СУБД — только Oracle. Каждая из перечисленных компаний принадлежит к числу лидеров в своем сегменте рынка. Все это стандарты Сбербанка России.

Многие крупные банки сегодня пытаются бороться со следствием, но это невозможно. Когда сменялись ИТ-директора, руководители отделов, все подчинялось сиюминутной выгоде. Но когда кинулись через 10 лет, чтобы исправить ситуацию, поняли, что нужно еще 10 лет. Необходимость поддержки разноформатной ИТ-инфраструктуры влечет за собой огромные финансовые потери, необходимость привлечения существенных человеческих ресурсов, риски, наконец.

PCWeek/UE: За многолетнюю историю существования вашей материнской компании наверняка приходилось сталкиваться с описанными сложностями?

С.А.: И приходится сейчас. Получается, мы учимся не только на чужих, но и на собственных ошибках. На то человеку и даны мозги, чтобы компилировать удачный опыт и отбрасывать неудачный. У каждого из нас есть неудачный опыт, но это не повод его масштабировать.

PCWeek/UE: Какие задачи стоят перед ИТ-подразделением банка в обозримой перспективе?

С.А.: Наш банк преследует стратегические цели, которые абсолютно корреспондируются с целями материнской структуры. Они состоят, прежде всего, в том, что мы идем к созданию виртуальных универсальных рабочих мест, которые базируются исключительно на веб-технологии, с последующим переходом к облачным вычислениям. Мы строим только онлайновые интерфейсы, офлайновые используются в исключительных случаях, например, при выгрузке данных в хранилище. Для организации онлайнового взаимодействия используем интеграционные продукты компании IBM.

Сергей Адаменко

Перед нами стоит задача по созданию индустриального ландшафта, базирующегося на высокопроизводительных системах от лучших производителей в мире, который позволит обеспечить необходимые темпы роста и нагрузку, многократно превышающую нынешнюю. В 2011 году мы закончим базовый этап внедрения системы взаимоотношения с клиентами CRM Siebel, которую рассматриваем в качестве фронт-офисного решения. Она будет тесно интегрирована с телекоммуникационным оборудованием компании Cisco, с почтовыми клиентами Microsoft, с системами хранения и обработки данных, ERP-системой и т.д.

До конца года мы планируем построить еще один ЦОД (второй по счету — прим. ред.), который будет, минимум, в три раза больше предыдущего.

PCWeek/UE: Вы заметили, что стратегические цели ДБСР в полной мере корреспондируются с целями материнской компании. Другими словами, Сбербанк России попытается портировать свою бизнес-модель на украинский рынок?

С.А.: Около десятка лет назад западные банки стремились портировать сюда свою модель, но она не ложилась. Модель поведения человека во Франции, Германии или Италии совершенно несопоставима с моделью поведения человека в Украине. У нас другая цена денег, другие потребности, мы иначе относимся к банкам. Не значит, что радикально иначе, но это порой существенно.

Несмотря на свой почтенный возраст, Сбербанк постоянно умнеет и становится лучше, адаптируется к существующим реалиям. Мы уходим от интеграции ИТ-систем к бизнес-интеграции, которая не предусматривает выравнивание продуктовой линейки. Да, у нас одинаковые платформы, например, CRM Siebel, но это не означает, что на их основе реализованы одинаковые модели. Другими словами, войдя в систему здесь, клиент сможет получить необходимые ему услуги на всех территориях, где есть Сбербанк. Их качество не будет отличаться. Но это не означает равенство кредитных ставок, ставок по депозитам, равенство продуктового ряда. Подобного рода интеграция только губительна для бизнеса.

PCWeek/UE: АБС какого разработчика применяется в вашем банке? Насколько ее возможности вас устраивают?

С.А.: Мы используем АБС Б2 компании CS. У нас задействовано много продуктов этого разработчика, в принципе, могу сказать, что на сегодняшний день они удовлетворяют требованиям банка. Что будет завтра? Время покажет.

PCWeek/UE: Вы придерживаетесь идеи централизации ИТ, когда в отделениях все управляется из центра?

С.А.: Не только придерживаемся, но так и делаем. Такой подход позволяет обеспечить необходимое качество услуг для клиентов и приемлемый уровень издержек. Вся ответственность возложена на главный офис, и мы определяем каким образом предоставлять сервисы на местах.

PCWeek/UE: При реализации проектов вы получаете поддержку со стороны материнской компании? Если да, в чем она выражается? Возможно, таким образом ДБСР получает определенные преференции над другими банками в Украине.

С.А.: Знаете, самое худшее, когда компания развивается на преференциях. Наш банк не просит преференций, они нам не нужны. Если ведем какой-либо проект, нас поддерживают все ресурсы Сбербанка России — технические, материальные, интеллектуальные. Однако это не означает, что нас автоматически заливают деньгами, ДБСР получает поддержку в рамках потребностей.

Зато если посмотреть на структуру акционерного капитала, бренд Сбербанка России стоит очень много. Думаю, она будет стоить еще больше, больше, чем Microsoft или Intel — вопрос только времени. Мы с вами очень много платим, покупая, скажем, часы Patek Pilippe, Vacheron Constantin, Breguet. Это хорошие часы, но как минимум, 50% их стоимости обусловлены многими десятками лет существования мануфактуры. Надписи «Сбербанк России» в этом году исполняется 170 лет. Поэтому обслуживаться в Сбербанке России сопоставимо с приобретением часов перечисленных брендов — дорого и очень позитивно для ценителей. Не каждый человек носит часы этих марок, но те, кто носят, почему-то считают нужным заплатить за них отнюдь немаленькие суммы.

PCWeek/UE: Вы хотите сказать, что ДБСР не планирует выходить на массовый рынок? Все-таки часы перечисленных марок далеко не все могут себе позволить.

С.А.: Согласен. Продолжая образное сравнение, можно сказать, что большинство людей мечтает иметь эти часы, правда? Но путь к ним лежит через Tissot, Swatch и т. д. Представьте, Сбербанк России — держатель всех перечисленных брендов. А значит для менее взыскательных клиентов мы тоже предложим услуги, соответствующие их потребностям. Но это будут услуги от одного поставщика, который владеет и более дорогими брендами уровня Patek Pilippe или Breguet.

УСПЕШНЫЙ БИЗНЕС – ЗАЩИЩЕННЫЙ БИЗНЕС

KASPERSKY lab

Ведите бизнес успешно и абсолютно спокойно под защитой «Лаборатории Касперского»

Мы предлагаем:

- простые и эффективные решения для защиты ваших информационных ресурсов
- совместимость с любой компьютерной инфраструктурой
- быстрый и профессиональный сервис с учетом особенностей вашего бизнеса

Подробнее: www.kaspersky.ru
или по тел. +380 44 495 26 05

Показательный пример построения ЦОД

СЕРГЕЙ МИШКО

ПРОЕКТЫ

Непростое решение о начале строительства ЦОД руководству «Кредобанка» пришлось принимать в самом начале кризиса, когда для большинства банков вопрос стоял о выживании, не говоря уже об инвестициях в ИТ. Наличие мощного инвестора в лице польской PKO BP Group (ее активы составляют примерно треть от совокупного объема всех отечественных банков) помогло претворить смелые планы в жизнь — уже несколько месяцев объект находится в эксплуатации. Эдуард Савушкин, вице-президент компании «Инком», чей львовский филиал выступил интегратором проекта, считает его уникальным для Украины. В то время как большинство ЦОД в нашей стране вынужденно подгоняют под готовые требования заказчика, в случае с «Кредобанком» внедрение начиналось, как это и положено, с консалтинга и предпроектного аудита.

Внедрение сетевой платформы Cisco Nexus 7000 в «Кредобанке» — первое на территории стран СНГ

Одной из предпосылок построения ЦОД в «Кредобанке» стала необходимость более качественного управления ресурсами и консолидации вычислительных мощностей. Содержать в каждом из нескольких десятков отделений выделенный сервер с набором всех сопутствующих лицензий на ПО оказывалось неоправданно дорого. Внедрение новых финансовых продуктов в соответствии с динамично меняющейся рыночной конъюнктурой и переход на европейские стандарты качества обслуживания клиентов требовал от банка наличия современной ИТ-инфраструктуры.

Как известно, у каждой медали есть две стороны. Затишье в бизнесе, вызванное разразившимся финансовым кризисом, в «Кредобанке» использовали для кардинального переформатирования накопившегося с момента основания банка в 1990 году ИТ-хозяйства. Местом строительства ЦОД выбрали индустриальное здание во Львове площадью 100 кв. м, которое в настоящий момент находится в собственности банка. Кстати, по словам председателя правления «Кредобанка» Ивана Феськива, на территории Львова охотно размещают свои ЦОД даже киевские банки — средоточие в этом приграничном регионе специализирующихся на разработке ПО компаний и квалифицированных ИТ-специалистов.

Проект построения ЦОД в «Кредобанке» стартовал в 2009 году. Предварительно специалисты «Инкома» в ходе проведенного аудита разработали концепцию внедрения, на этапе проектирования собрали все необходимые статистические данные о работе систем заказчика и тенденциях роста объемов данных и вычислений и в итоге выполнили расчет необходимых подсистем. Представители сформированной совместной рабочей группы из сотрудников ИТ-департамента банка и компаний Cisco Systems, IBM и «Инком» провели моделирование и тестирование систем, чтобы убедиться в их полной пригодности для оптимального решения стоящих перед бизнесом перспективных задач.

«Нам несколько раз приходилось менять решение, последние полгода работали вовсе без выходных», — признается Игорь Гентош, начальник управления системной интеграции «Кредобанка», и тем не менее, не скрывает своего удовлетворения от реализации проекта. Гордиться и в самом деле есть чем: за 4,5 месяца удалось построить ЦОД, соответствующий всем требованиям НБУ и стандарту TIA 942 с уровнем надежности TIER III (регламентирует максимально допустимое время простоя — 1,6 ч/год). Объект рассчитан на размещение 1 600 юнитов с техническим оборудованием.

Электроснабжение

В здание от трансформаторной подстанции заведены 2 электрических ввода с AVR (Automatic Voltage Regulation) и максимальной нагрузкой 1 МВт — они обеспечивают электроснабжение не только ЦОД, но и расположенных по соседству потребителей.

Гарантированное электроснабжение

У банка есть собственная ДГУ Gesan мощностью 860 кВА — этого достаточно для обеспечения бесперебойного электроснабжения основных потребителей в течение 4 часов. В щитовой за пределами серверного помещения ЦОД расположены два ИБП EATON Powerware мощностью 275 кВА (по признанию заказчика, аналог APC оказался слишком дорогим). Кстати, во время посещения ЦОД произошло внеплановое отключение энергии, и журналисты стали свидетелями аварийного запуска дизель-генератора. Организаторы клятвенно заверяют, что подобные перебои происходят достаточно часто и намеренно никто не собирался устраивать «живую» демонстрацию запуска системы резервного питания. Находясь в Украине, несложно поверить в такие истории.

Телекоммуникации

Объект подключен к двум независимым оптическим каналам связи, идущих из различных канализаций. Нужно заметить, что все помещения «Кредобанка» во Львове соединены друг с другом оптическими линиями, общая протяженность которых достигает 60 км. В распоряжении каждого отделения банка есть канал с пропускной способностью 2 Мбит/с — он позволяет решать задачи централизации, начатой в середине 2010 года.

Помещение для ЦОД

Согласно требованиям НБУ все оборудование ЦОД находится в экранированном помещении. Высота фальшпола составляет 40 см, внутри находятся шланги с хладагентом жидкостной системы охлаждения. В соответствии с требованиями НБУ по ТЗИ в ЦОД построена система автоматического пожаротушения и прописан детальный

Эдуард Савушкин: «Из всех задач проекта построения ЦОД технически наиболее сложной является миграция существующих приложений и баз данных. Успешный результат нашей работы — это результат команды специалистов интегратора, заказчика и вендоров»

план мероприятий при пожаре для персонала заказчика. В серверном помещении используется условно безопасный для человека газ R125, в помещении с ДГУ — порошок. Внутри ЦОД осуществляется мониторинг физических параметров внешней среды и состояния оборудования APC InfraStruXure: влажности, качества электроснабжения, температурных режимов.

Шкафы

Плотность энергопотребления составляет 6 кВА на стойку при расчетном значении 8 кВА, максимальная мощность оборудования в серверной может достигать 240 кВА. В ЦОД применяются шкафы APC, Panduit и IBM. Последние легко узнать по характерному пьедесталу для смещения центра тяжести и улучшения устойчивости конструкции при неполном заполнении оборудованием. В настоящий момент в помещении находится 18 шкафов, в перспективе их число вырастет до 38.

Слева на фото баллон с газом системы пожаротушения, хорошо заметно экранирование стен здания, справа в рядах шкафов выделяются системы внутреннего охлаждения APC InRow и шкафы IBM — единственные с пьедесталами для смещения центра тяжести

В банке не исключают возможности передачи части инфраструктурных мощностей ЦОД в аренду третьим организациям.

Система охлаждения

Для отвода тепла от стоек внедрена технология холодных и горячих коридоров с внутренним охлаждением APC InRow и установлены два чиллера Emerson Network Power Liebert HPC с четырьмя компрессорами в каждом. Поддержка технологии Free Cooling дает возможность нагнетать холодный воздух с улицы в зимнее время года и тем самым экономить электроэнергию и ресурс агрегатов. Холодильные машины работают попеременно с суточным интервалом, при этом одна из них находится в резерве. Они запитаны напрямую от ДГУ, тогда как насосная группа — от ИБП. Емкости бака с охлаждающей жидкостью достаточно для поддержания в серверном помещении надлежащей температуры в течение 15-20 мин даже при полностью обесточенных чиллерах, далее градиент роста температуры может достигать 1°С/мин, что соответствует нештатной аварийной ситуации.

Сетевая инфраструктура

В ЦОД построена СКС с применением решений Panduit. Все информационные кабели находятся в лотках, расположенных в верхней части здания. Особого внимания заслуживает ядро сети, в основе которого лежит масштабируемая модульная платформа Cisco Nexus 7000, разработанная

Два чиллера Emerson Liebert HPC с поддержкой технологии Free Cooling работают попеременно с суточным интервалом

специально для нужд ЦОД. Она вмещает 512 портов 10 GbE, поддерживает будущие технологии 40/100 GbE и обеспечивает емкость коммутации до 15 Тбит/с на одном шасси. Это первая в отрасли платформа с унифицированной коммутационной матрицей, избавляющая от необходимости строить две отдельные сети — IP и FC. По словам Александра Масло, технического руководителя представительства Cisco в Украине, речь идет о первом внедрении Nexus 7000 в масштабах СНГ.

ПРОДОЛЖЕНИЕ НА С. 24 ▶

ДОСЬЕ

Самый польский украинский банк

По данным АУБ (ассоциации украинских банков) состоянием на 1 января 2011 года ПАО «Кредобанк» с центральным офисом во Львове занимает 35-е место по размеру капитала (766 млн грн) и объемам активов (4,45 млрд грн). В соответствии с классификацией НБУ он относится ко II группе — «Крупные банки». Региональная сеть «Кредобанка» включает около 140 филиалов и отделений и 370 собственных банкоматов практически по всей Украине. Клиентская база насчитывает более 32 тыс. юридических лиц и предпринимателей и около 320 тыс. физических лиц. Стратегическим акционером «Кредобанка» (99,6% акций) является крупнейший польский банк PKO BP SA.

Унікальний досвід наших професіоналів у створенні хмарних інфраструктур дозволить вам гарантовано вирішити такі задачі, як

- Консолідація та віртуалізація обчислювальних ресурсів
- Забезпечення вимог Business Continuity та Disaster Recovery Planning
- Катастрофостійкість інфраструктури та IT-сервісів
- Міграція IT-сервісів до Хмарної моделі
- Міграція центрів обробки даних

denovo
Надихаючись Майбутнім

vmware PARTNER
ENTERPRISE SOLUTION PROVIDER

Звертайтеся за додатковою інформацією за телефоном
+380 44 200 9339
e-mail: forinfo@de-novo.biz
www.de-novo.biz

ИНФРАСТРУКТУРА

EMC УНИФИЦИРУЕТ СВОЙ MID-RANGE

ЛЕВ ЛЕВИН

Корпорация EMC представила по обе стороны Атлантики свое новое семейство модульных дисковых массивов среднего класса (mid-range) VNX, которые заменят две прежние линейки ее систем хранения — Clariion CX и Celerra, рассчитанные соответственно на использование в сетях хранения SAN на основе интерфейса Fibre Channel и в качестве специализированного файлового сервера NAS, к которому компьютеры подключаются по IP-протоколу через стандартную локальную сеть Ethernet. На уровне «железа» Celerra отличалась от Clariion CX только управляющими модулями, которые реализовывали функции NAS, поэтому вполне логичным шагом выглядит объединение обеих линеек в единую серию VNX, поддерживающую как SAN, так и NAS (с помощью управляющих лезвий). EMC позиционирует свою новую серию mid-range как унифицированные системы хранения Unified Storage, фактически повторяя тот подход, который уже восемь лет предлагает компания NetApp, реализовавшая в своих NAS-системах FAS поддержку технологий SAN. Судя по отчетам IDC, идея Unified Storage в версии NetApp оказалась востребованной рынком, и последние кварталы этот вендор постоянно увеличивает свою долю и уже вышел на третье место в мире, в то время как такие традиционные конкуренты EMC, как HP и IBM, заняты интеграцией в линейку своих систем хранения продуктов недавно приобретенных фирм 3Par и XIV. NetApp сегодня для EMC стала наиболее опасным конкурентом.

СИСТЕМЫ ХРАНЕНИЯ

Модуль контроллеров массива VNX5100

Пат Гелсингер, руководитель отделения продуктов для информационной инфраструктуры EMC, представляет массив для малого и среднего бизнеса VNXe

Линейка VNX состоит из пяти моделей (см. табл. 1). Как утверждает EMC, за счет использования в контроллере дисковых массивов новейших многоядерных процессоров Intel Xeon 5600 и новой версии ПО автоматического перемещения данных между разными уровнями хранения FAST по производительности VNX троекратно превосходит Clariion CX и Celerra. Правда, пока не ясно, есть ли в VNX какие-нибудь принципиальные технологические новшества по сравнению с Clariion CX, кроме поддержки NAS и замены интерфейса Fibre Channel на SAS во внутренней архитектуре массива.

Вместе с mid-range корпорация обновила и свой портфель систем хранения начального уровня, заменив Clariion AX на две модели VNXe (табл. 2), ориентированные на рынок малого и среднего бизнеса. Как утверждают руководители корпорации, системы VNXe можно будет приобрести менее чем за 10 тыс. долл., т. е. они обойдутся покупателем дешевле, чем аналогичные массивы от Dell, IBM и HP, а также NetApp. До сих пор доля EMC в секторе систем хранения начального класса была существенно ниже, чем в секторе mid-range и high-end, из-за того, что эти системы часто покупаются вместе с серверами, и поэтому Clariion AX было трудно конкурировать с дисковыми массивами от серверных вендоров (правда, одно время эти массивы по OEM-соглашениями поставляли Dell и Fujitsu Siemens Computers, но эти компании затем заменили их на собственные системы хранения). При продвижении VNXe основная ставка делается на простоту установки и обслуживания этого массива (впрочем, большинство систем хранения начального уровня также рекламируются как продукты, для работы с которыми не требуется специального обучения) и на существенное увеличение числа авторизованных реселлеров EMC, которые получат право на продажи VNXe.

Dell, которая ранее продавала предыдущие поколения Clariion и Celerra, намерена включить в свою продуктовую линейку только VNX. Fujitsu пока не делала вообще никаких заявлений на этот счет. Оба этих вендора в последнее время пытаются выйти из тени EMC на рынке систем хранения: Fujitsu стала активно продвигать разработанные в Японии дисковые массивы Eternus, а Dell в конце прошлого года приобрела производителя дисковых массивов для SAN компанию Compellent. Как заявил председатель правления и исполнительный директор EMC, его корпорация теперь рассматривает партнерские отношения с Dell не как стратегические, а только как тактические.

Таблица 1. Модельный ряд EMC VNX

Модель	VNX5100	VNX5300	VNX5500	VNX5700	VNX7500
Максимальное число дисков	75	125	250	500	1000
Тип дисков	SAS, Nearline SAS, Flash				
Число слотов для плат ввода/вывода	0	4—8	4—13	6—18	8—42
Функции NAS					
Управляющие модули X-Blade	Нет	1 или 2	1, или 2, или 3	2, или 3, или 4	От 2 до 8
Оперативная память одного X-Blade, Гб	Нет	6	12	12	24
Протоколы доступа к файлам	—	NFS, CIFS, MPFS, pNFS			
Функции SAN					
Контроллеры массива	2	2	2	2	2
Оперативная память контроллера, Гб	4	8	12	18	24
Поддерживаемые протоколы	Fibre Channel	Fibre Channel, iSCSI, Fibre Channel over Ethernet			

Таблица 2. Модельный ряд EMC VNXe

Модель	VNXe3100	VNXe3300
Минимальное число дисков	6	7
Максимальное число дисков	96	120
Тип дисков	SAS, Nearline SAS	SAS, Nearline SAS, Flash
Число слотов для плат ввода/вывода	2	4
Функции NAS		
Протоколы доступа к файлам	NFS, CIFS	
Функции SAN		
Управляющие модули X-Blade	Интегрированные	
Контроллеры массива	1 или 2	2
Оперативная память контроллера, Гб	4	12
Протоколы	iSCSI	

ВЫБИРАЕМ НАСТОЛЬНЫЕ СИСТЕМЫ ХРАНЕНИЯ

П. ДЖ. КОННОЛИ

Настольные устройства хранения — это простое решение, если вам необходимо работать с большим объемом данных, не умещающимся в компьютере. В отличие от меньших по размеру, более портативных корпусов для дисков такие устройства не предназначены для ношения в портфеле. Зато их можно подключать к сети и использовать в качестве общего ресурса рабочей группы. В зависимости от количества физических дисководов их можно сконфигурировать для поддержки различных уровней RAID, обеспечив дополнительную защиту данных. Ниже перечисляются восемь факторов, которые лаборатория eWeek Labs рекомендует вам учитывать при покупке настольной системы хранения.

1. Подключение

Конечно, наилучшим вариантом будет сетевое подключение с поддержкой протокола Gigabit Ethernet. Но почти столь же часто используется непосредственное подключение к нескольким внешним устройствам хранения. Поддержка USB 2.0 подразумевается в любом случае, и я не могу представить себе устройство, в котором она отсутствует. В ближайшие месяцы станет полезной поддержка USB 3.0. Неплохо иметь и такой интерфейс, как eSATA, но по непонятным нам причинам на портативных устройствах он не привился. Всегда считался важным порт FireWire, но в связи с повсеместным использованием USB 2.0 он теряет свое значение. Мне хотелось бы также, чтобы устройства можно было подключать к шине iSCSI для использования в кластеризованных или виртуализированных средах.

2. Объем

Чем больше, тем лучше. Для рабочих групп становится все более обычным делом иметь несколько терабайтов данных, хранящихся на компьютерах и различных внешних устройствах. При покупке всегда предусматривайте вдвое больший объем, чем считаете необходимым, поскольку данные неизбежно разрастаются, заполняя все доступное пространство.

3. Избыточность

Поддержка RAID уровней 5 и 6 гораздо предпочтительнее, чем JBOD. RAID 6 значительно менее известен, чем RAID 5, который сохраняет целостность данных в случае отказа одного из входящих в массив физических дисков. Он обеспечивает двойную защиту, сохраняя данные даже при выходе из строя двух дисков. Если ограничиться просто набором дисков, это позволит максимально использовать их объем, но не спасет вас в аварийной ситуации.

4. Безопасность

Даже если устройством будет пользоваться лишь один человек, все равно следует применять шифрование, коль на устройстве могут храниться какие-то конфиденциальные сведения. А если пользователей несколько, значение защиты возрастает экспоненциально. Так что выясните, может ли нечестный сотрудник, особенно если он пользуется доверием и обладает соответствующими полномочиями, получить доступ к данным, в которых у него нет необходимости.

5. Управляемость

Насколько просто управлять устройством? Можно ли управлять им дистанционно без ущерба для безопасности? Используются ли по умолчанию или можно ли легко задействовать такие протоколы, как SSH (Secure Shell) и SFTP (SSH File Transfer Protocol)?

6. Защита окружающей среды

Шумные вентиляторы и дисководы могут сделать соседство даже с самым привлекательным настольным устройством хранения совершенно невыносимым. Можно ли через интерфейс управления задать пороговые значения скорости вращения вентилятора? Можно ли снизить энергопотребление устройства посредством выведения его из «спящего» состояния подачей сигнала через локальную сеть (Wake-on-LAN) или составления расписания раскручивания и остановки диска? Насколько просто добавить поддержку ИБП?

7. Встроенные приложения

Даются ли рекомендации по выбору онлайновых сервисов резервного копирования или привязка к ним? Если да, то насколько удачно это реализовано? Может ли устройство хранения стать чем-то большим, чем корпусом, в котором вращается носитель информации? Нет ли возможности превратить его в носитель сервисов внутренней сети? А если да, то насколько просто управлять ими?

8. Гарантия и техническая поддержка

Если потребуется заменить дисковод, легко ли будет найти запасные части? Обеспечивает ли производитель замену на следующий рабочий день? Можно ли использовать другие дисководы, когда официально одобренные компоненты будут уже недоступны?

Grandstream
Innovative IP Voice & Video

Узнай, что на самом деле происходит в твоё отсутствие.

GXV3662
Антивандальная купольная IP-камера высокого разрешения (720P). Камера работает в двух режимах: день/ночь, поддерживает связь через SIP, возможность двусторонней связи.

GXV3611
Стационарная IP-камера для использования во внутренних помещёниях. Встроенный микрофон, громкоговоритель и детектор дыма обеспечивают высочайшийуровень безопасности.

GXV3615 Cube IP Camera
Профессиональная IP-камера в кубическом корпусе. Встроенный потоковый видеосервер позволяет вести видеонаблюдение десяти сотрудникам одновременно.

Оборудование для IP-видеонаблюдения Grandstream позволяет наблюдать происходящее, находясь в любой точке земного шара, используя мобильный телефон или видеофон.

TELCO
Innovative Telecommunications

Дистрибьютор в Украине

Телефон: +380 (44) 406-56-06
Факс: +380 (44) 406-57-47
www.telco.ua

2011-Й — ГОД ОЖИВЛЕНИЯ И НОВАТОРСТВА

ЕЛЕНА ГОРЕТКИНА

Трансформация ИТ-отрасли давно является основной темой ежегодных прогнозов ведущих аналитических компаний. За последнее время появилась целая волна новаторских технологий — облачные услуги, мобильные вычисления, социальные сети... По прогнозу аналитиков, в 2011 году они обретут зрелость и начнут завоевывать место в качестве массовых (mainstream) платформ. В результате главными направлениями ИТ-отрасли будут развитие традиционных технологий и освоение новаторских подходов, которые не только станут основой для создания новых рынков, но и, вероятно, приведут к перестановке сил на компьютерном Олимпе. Смена платформ будет сопровождаться подъемом ИТ-рынка и постепенным возвращением к докризисному уровню.

Оживление ИТ-рынка

В области ИТ наметился подъем. По прогнозу IDC, в 2011-м расходы на информационные технологии вырастут по сравнению с 2010-м на 5,7% и достигнут 1,6 трлн. долл. Темп роста будет несколько ниже, чем в прошлом году, когда рынок вырос на 6,4%. Но тогда этот результат был достигнут после спада на 3,7%, вызванного кризисом, и оказался даже гораздо лучше сделанного ранее прогноза.

Рассматривая распределение рынка по сегментам, IDC отмечает отличие нынешнего года от предыдущего. Так, темп роста расходов на оборудование составит 7,8%, что ниже, чем в 2010-м (13%); при этом основными двигателями станут конвергированные мобильные устройства, сетевое оборудование и ПК. Однако затраты на ПО и услуги будут расти быстрее прошлогодних. Ожидается, что сегмент ПО вырастет на 5,3% (рост в 2010-м — 3,9%), а услуг — на 3,6% (в 2010-м — 0,9%). Увеличится спрос на аутсорсинг — рост достигнет 4%.

Положительный прогноз предлагает и компания Gartner: в 2011-м рынок вырастет на 5,1% и достигнет 3,6 трлн. долл. (в эту оценку включены не только ИТ, но и коммуникационные технологии). Но Gartner, как и IDC, отмечает, что в нынешнем году темп роста будет несколько ниже прошлогоднего, который, по ее данным, составил 5,4%.

Наиболее активно, по мнению Gartner, будет расти сегмент телекоммуникационного оборудования (см. таблицу). Ожидается значительное оживление спроса на мобильные устройства, причем в развитых странах основными катализаторами подъема станут смартфоны, а в развивающихся — недорогие устройства без торговой марки (white box).

Хотя IDC и Gartner позитивно оценивают перспективы ИТ-рынка, они предупреждают о возможных рисках, связанных с неустойчивым состоянием экономики США (высокий уровень безработицы и новый спад на рынке недвижимости) и Западной Европы (задолженность отдельных стран и курс правительств на режим строгой экономии). К тому же в 2011-м будет ощущаться влияние новаторских технологий и моделей оплаты — спрос на облачные услуги, виртуализацию и мобильные устройства положительно отразится на одних сегментах ИТ-рынка и отрицательно — на других. Тем не менее ИТ-рынок будет расти, хотя и медленнее, чем до кризиса, но быстрее мировой экономики в целом.

Как и в прошлом году, главными катализаторами подъема будут развивающиеся регионы. По прогнозу IDC, на долю Центральной и Восточной Европы, Латинской Америки, Азии (кроме Японии) и Африки придется 27% мирового ИТ-рынка, в абсолютных цифрах — 440 млрд. долл., что на 10,4% больше, чем в 2010-м. Доминирующее положение здесь займут Бразилия, Россия, Индия и Китай (БРИК): их доля в ИТ-расходах развивающихся стран составит 44% — на 14,4% больше, чем в 2010-м. При этом больше половины придется на Китай, который, как предполагается, по объему ИТ-рынка в 2013-м обгонит Японию.

IDC рекомендует поставщикам ИТ-продуктов обратить пристальное внимание на развивающиеся регионы, особенно на страны БРИК, чтобы воспользоваться открывающимися там перспективами.

Надвигаются облака

По мнению IDC, облачные услуги станут основой для роста ИТ-рынка в ближайшие 20 лет и причиной его трансформации с точки зрения продуктов и бизнес-моделей.

В 2010-м в этой области произошел существенный сдвиг: все ведущие игроки включили облачные технологии в свои стратегии, продуктовые планы, предложения и маркетинг. Как считают аналитики, это приведет к значительному подъему спроса на облачные вычисления. Ожидается, что в 2011-м затраты на услуги общедоступных облаков вырастут на 30%, до 29 млрд. долл., а в 2014-м — до 55 млрд.

Поставщики постараются расширить свои облачные платформы за счет покупки разработчиков подходящих решений, и ожидают в 2011-м новую волну слияний и поглощений, а также партнерских сделок

Подъем произойдет и в сегменте частных облаков — на их долю придется 13 млрд. долл. Отставание аналитики объясняют тем, что предложения в этой области появились на несколько лет позднее, чем услуги общедоступных облаков. Однако интерес заказчиков обеспечит здесь более быстрый темп роста — 26% в год. Но аналитики считают, что пик спроса на частные облака придется на 2015-й, а потом подъем замедлится, так как в области общедоступных облаков появятся новые предложения, которые привлекут внимание заказчиков.

Радужный облачный прогноз предлагает и Gartner, отмечая, что в 2011-м вендоры будут продвигать пакеты решений для реализации частных облаков, которые включают технологии (ПО, оборудование) и методики (передовые методы внедрения и использования). Многие игроки будут также предлагать услуги по удаленному управлению облачным сервисом.

Как полагают в IDC, к концу 2011-го около 15% доходов ИТ-отрасли и более 30% роста будет приходиться на долю общедоступных и частных облаков. Поскольку облака становятся горячим направлением ИТ-рынка, возникает вопрос: чья платформа будет доминировать в этой области? В качестве главных претендентов IDC называет Amazon, Google, IBM, Microsoft, salesforce.com, Oracle, VMware и некоторые телекоммуникационные компании. Выиграет тот игрок, которому удастся привлечь к своей облачной платформе самую большую и сильную экосистему разработчиков решений. Ставки в этой игре высоки. Ведь победитель станет «следующей Microsoft» и займет на рынке облаков такое же доминирующее положение, какое софтверный гигант имеет в области Windows-приложений.

Исходя из такого развития событий аналитики считают, что поставщики постараются расширить свои облачные платформы за счет покупки разработчиков подходящих решений, и ожидают в 2011-м новую волну слияний и поглощений, а также партнерских сделок.

Вторая волна поглощений намечается в области управления гибридными структурами, которые включают облака (частные и общедоступные) и традиционные корпоративные системы. По мнению IDC, в этой области усилится конкуренция между поставщиками традиционных продуктов управления (CA, Citrix, Compuware, HP, IBM, Microsoft, Symantec, VMware и др.), новыми игроками на этом поле (Cisco и Oracle) и сервисными компаниями (Accenture, CSC, HCL, Infosys, PwC и т. д.), причем последние будут играть роль брокеров облачных услуг. Чтобы укрепить положение, игроки будут скупать разработчиков средств развертывания облаков и управления ими.

Рост популярности облаков подстегнет рынок облачных услуг, и в результате у провайдеров вырастет спрос на оборудование. По прогнозу IDC, в 2011-м на долю поставщиков облачных услуг придется 12% продаж серверов и систем хранения, а к 2014-му — 20%. Кроме того, ожидается, что предприятия станут использовать в своих будущих корпоративных системах все больше технологий, разработанных для провайдеров облачных услуг (массовое масштабирование, оптимизация нагрузки, автоматическое управление и облачный подход). Поэтому аналитики рекомендуют ИТ-вендорам уделять больше внимания облачным провайдерам.

Нарастает мобильность

Вторая причина трансформации ИТ-рынка связана со стремительным ростом числа мобильных устройств и приложений. Так, в 2011-м к интернету будут обращаться более 2 млрд. человек, причем более половины из них с помощью мобильников, в основном смартфонов (пять лет назад таких мобильных пользователей было в десять раз меньше). По прогнозу IDC, в 2011-м будет продано 330 млн. смартфонов — на 24% больше, чем в 2010-м. В результате в ближайшие полтора года по количеству выпущенных устройств мобильники (смартфоны и планшеты) впервые за историю ИТ-рынка обойдут персональные компьютеры.

Вендоры не оставляют без внимания такое развитие событий. В связи с этим IDC полагает, что традиционные игроки рынка ПК, такие как Microsoft и Lenovo, постараются усилить позиции в мобильном сегменте за счет покупки компаний, специализирующихся в этой области, например Motorola и RIM.

Наступление мобильных устройств отмечает и Gartner. По ее оценке, в 2011-м во всем мире будет использоваться 1 млрд. ПК и 5 млрд. мобильных телефонов. Исходя из дальнейшего роста популярности мобильников аналитики прогнозируют, что к 2020-му рынок беспроводных продуктов достигнет 1 млрд. долл.

Росту рынка смартфонов будет способствовать резкое увеличение спроса в развивающихся странах, особенно в Индии и Китае, на недорогие модели на базе ОС Android, число которых постоянно растет. Это может отрицательно отразиться на поставщиках дорогих смартфонов (например, Apple).

Продолжится победное шествие планшетов во главе с Apple iPad. По прогнозу IDC, в 2011-м будет продано 42 млн. планшетов (гораздо больше, чем нетбуков), и в течение следующих четырех лет объем продаж будет ежегодно расти на 50%. В этом году Apple сохранит ведущие позиции, но усиление конкуренции со стороны планшетов на базе ОС Android разработки Dell, HP, Samsung и других компаний приведет в 2012—2013 гг. к сокращению доли iPad.

Обострится конкуренция и в области платформ для мобильных приложений. Ставки в этой игре высоки. Ведь аналитики ожидают в 2011-м бурного всплеска активности в сегменте мобильных приложений. В течение этого года будет загружено 25 млрд. приложений (в 2010-м — 10 млрд.) на сумму свыше 12 млрд. долл. (в 2010-м — 5 млрд. долл.). В области мобильных платформ основными претендентами на корону являются Apple и Google, а главными каналами продаж — онлайновые магазины Apple App Store и Android Market. И хотя пока лидерство останется за первой площадкой, вторая обгонит ее по темпу роста из-за стремительного увеличения числа мобильных устройств на базе Android.

Поставщики традиционного софта, естественно, не желают оставаться в стороне от этого феномена. По мнению IDC, следует ожидать распространения модели онлайновой продажи приложений и в мире ПК. Ведущие позиции аналитики отводят Microsoft и ее будущему магазину Windows App Store, который, как предполагается, откроется в этом году.

Инновации в широкополосных сетях

В связи с распространением мобильных и облачных технологий растет спрос на услуги широкополосной связи. Как уже отмечалось, в 2011-м число пользователей интернета, по прогнозу IDC, достигнет 2 млрд., а в

Распределение ИКТ-расходов в 2011 г.

Сегмент ИТ-рынка	2010 г.		2011 г.	
	Расходы, млрд. долл.	Рост,%	Расходы, млрд. долл.	Рост,%
Компьютерное оборудование	364,1	8,9	391,3	7,5
Корпоративное ПО	235,9	6,1	253,7	7,5
ИТ-услуги	782,0	2,5	817,9	4,6
Телекоммуникационное оборудование	426,6	14,0	465,4	9,1
Телекоммуникационные услуги	1593,0	3,9	1647,4	3,4
Всего	3401,6	5,4	3575,8	5,1

Источник: Gartner.

2016-м приблизится к трём. Многие из них активно применяют приложения, требующие высокой пропускной способности, такие как онлайновое видео, IP-телефония, загрузка музыкальных файлов.

Это стимулирует расширение рынка широкополосного доступа. Так, по оценке компании Instat, в последние годы число абонентов широкополосных услуг ежегодно росло на 25% и в 2010-м достигло 763 млн. человек.

Но такой бурный рост оказывает огромное давление на операторов проводных и беспроводных сетей, которым приходится активно заниматься оптимизацией нагрузки, повышением производительности и внедрением новаторских технологий.

Так, в прошлом году большое внимание привлекала технология 4G. Однако, по мнению IDC, рекламного шума было больше, чем результатов. В 2011-м ситуация немного улучшится, но лишь один из ста выпущенных карманных устройств будет поддерживать 4G. Сдерживать распространение 4G будут также ограниченный территориальный охват и проблемы с роумингом. Оживление на этом рынке наступит не раньше 2012—2013 гг.

В области проводной связи ожидается повышение внимания к технологии Ethernet Exchange, позволяющей передавать трафик между локальными сетями разных операторов. В 2011-м, по всей вероятности, стремительно увеличится объем предлагаемых услуг. Распространение этой технологии подстегнет внедрение широкополосной связи во многих отраслях, например в финансовой и здравоохранительной, а также будет стимулировать развитие экосистем провайдеров облачных услуг, мультимедийного цифрового контента и мобильных приложений.

Социальные сети набирают силу

В связи с ростом популярности социальных технологий среди предприятий IDC прогнозирует стремительный подъем в этой области — спрос на платформы для социальных сетей будет ежегодно увеличиваться на 38% в течение ближайших пяти лет.

По оценке Gartner, в 2010-м объем рынка корпоративного социального ПО вырос на 14,9% — до 644,4 млн. долл., а в 2011-м увеличится на 15,7%, до 769,2 млн. долл. Этот софт поддерживает блоги, сообщества, дискуссионные форумы, социальные закладки и вики. По мере повышения зрелости социальных технологий предприятия интегрируют их в приложения, направленные на решение задач бизнеса, такие как продвижение продукции. маркетинг и взаимодействие с потребителями. По прогнозу Gartner, к 2014-му более 20% сотрудников будет использовать для коммуникации социальные сети вместо электронной почты.

В 2011-м в связи с тенденцией превращения социальных сетей в массовую технологию ожидаются расширение их применения среди средних и малых предприятий и консолидация поставщиков ПО для этой области.

За последнее время число компаний, продвигающих социальное ПО, значительно выросло, превысив сотню. Однако, как предполагают в IDC, вскоре это количество уменьшится, так как их скупят ведущие игроки — Oracle, SAP, Microsoft, HP, Cisco и IBM, чтобы выйти на перспективный рынок или укрепить на нем свои позиции. Кроме того, крупные поставщики социального софта будут поглощать нишевых разработчиков для расширения присутствия на рынке. В результате, по мнению аналитиков, в 2011-м будет куплено примерно 30% таких компаний.

Поскольку даже в США лишь половина из предприятий среднего и малого бизнеса (СМБ) имеет собственный веб-сайт, они будут активно применять социальные сети, чтобы бесплатно воспользоваться возможностями интернета для привлечения и удержания клиентов. Как полагает IDC, к концу 2011-го более 40% СМБ-компаний будет использовать социальные сети для продвижения товаров и услуг.

Цифровая вселенная расширяется

По прогнозу IDC, в 2011-м объем цифровой информации вырастет на 27% и достигнет 1,8 зеттабайт, а к 2015-му — превысит 7 зеттабайт. Главным двигателем станет цифровой контент — видео, телевидение, изображения и копирование информации.

Главной новинкой 2011-го станет переход новаторских технологий от опытно-экспериментальной фазы к этапу массового внедрения в индустрии ИТ и других отраслях.

В связи с таким экспоненциальным ростом возникает необходимость в управлении огромным объёмом неструктурированных данных и их анализе. Рост популярности облачных технологий приведет к тому, что значительная доля таких данных будет храниться в средах, включающих частные и общедоступные облака, а также в традиционных корпоративных системах, к которым можно обращаться с помощью самых разных устройств. Ни один поставщик не имеет средств для управления всей этой инфраструктурой, но многие хотят занять здесь ведущее положение. Поэтому IDC ожидает волну слияний и поглощений, в ходе которой Cisco, Dell, EMC, HP, IBM, Microsoft и Oracle будут покупать компании, специализирующиеся в области управления информацией. В качестве кандидатов аналитики называют Informatica, Pervasive Software, Autonomy, Open Text, Harmonic и другие.

Огромные объемы информации нужно не только хранить, но и эффективно использовать. Однако сейчас изменения в бизнесе происходят так быстро, что старая модель хранения данных для последующего анализа уже не работает. В IDC полагают, что в этом году новые и традиционные игроки выпустят средства аналитики в реальном времени, а потом перенесут их в облака, чтобы расширить пользовательскую базу.

Грядущие перемены в бизнес-аналитике прогнозирует и Gartner. В связи с ростом вычислительной мощности компьютеров и мобильных устройств, а также с увеличением пропускной способности сетей связи меняется подход предприятий к принятию решений. Для предсказания будущего развития событий они хотят вместо анализа данных за прошедший период выполнять моделирование текущей информации в реальном времени. Это потребует существенных перемен в имеющейся инфраструктуре бизнес-аналитики, но позволит предприятиям улучшить результаты деятельности и повысить вероятность успеха.

«Интеллектуализация» отраслей ускоряется

По мнению IDC, распространение новых платформ — мобильных, облачных, социальных и мультимедийных — позволит ИТ-поставщикам расширить спектр отраслевых решений и экспертных знаний, чтобы помочь предприятиям более активно использовать интеллектуальные возможности информационных технологий. Аналитики выделили четыре отрасли, в которых такая трансформация происходит особенно активно.

В розничной торговле все шире применяются мобильные и социальные технологии. По оценке организации National Retail Federation, во время сезона предпраздничных продаж в США почти 30% покупок (на сумму 447 млрд. долл.) совершались с помощью мобильных устройств. Люди использовали их для поиска товаров и услуг, сравнения цен и выполнения оплаты. Число мобильных покупателей растет. Опрос IDC показал, что в этом году 40% потребителей (гораздо больше, чем год назад) планируют применять мобильники для шопинга. Внедрение социальных технологий также стоит у ритейлеров на повестке дня. По данным этого же опроса, более половины респондентов полагаются на советы друзей при совершении покупок, при этом четверть из них выясняют их мнения через социальные сети.

Финансовые организации также не остаются в стороне от мобильных веяний и начинают внедрять поддержку мобильных платежей. В США операторы беспроводных сетей, платежных средств и ИТ-компании (Google и Apple) собираются уже в этом году запустить ряд систем мобильных платежей с поддержкой технологии NFC (Near Field Communication). Аналитики полагают, что в 2011-м эти системы будут работать независимо друг от друга, но потом начнут сливаться для расширения охвата.

Мобильные технологии находят применение и в здравоохранении. В этом году 14% населения США (порядка 31 млн. человек) будет использовать мобильные медицинские приложения. Согласно опросу IDC, более 90% пациентов имеют сотовые телефоны или смартфоны. Поставщики ИТ-решений для здравоохранения стараются использовать данное обстоятельство, разрабатывая соответствующие приложения. Этому способствует появление медицинских приборов с поддержкой беспроводной технологии Bluetooth, таких как глюкометры, измерители давления и веса, с помощью которых люди могут загружать свои показатели в мобильные приложения, анализировать и отправлять врачам.

В энергетике продолжится внедрение технологии Smart Grid, направленной на применение ИТ в целях экономии электроэнергии. По мнению IDC, инвестиции в Smart Grid подстегнет выпуск первых электромобилей, подзаряжаемых от сети (Plug-in electric vehicle, PEV). По прогнозу, в 2015-м в мире будет использоваться более 2,7 млн. таких машин, а в 2020-м — 7,7 млн. Для их подзарядки потребуются специальные станции, что откроет новое поле деятельности для независимых провайдеров услуг.

Грядут перемены

Как подчеркивает в заключение IDC, главной новинкой 2011-го станет переход новаторских технологий от опытно-экспериментальной фазы к этапу массового внедрения в индустрии ИТ и других отраслях. При этом они будут интегрироваться друг с другом, например облачные технологии с мобильными, мобильные — с социальными сетями, а социальные сети — с хранилищами данных и бизнес-аналитикой в реальном времени, что позволит пользователям получить от них большую отдачу.

Новаторские технологии станут растущей частью ИТ-рынка, что приведет к его реструктуризации, поскольку игроки будут развивать и интегрировать эти новинки, покупать их поставщиков. Одновременно они будут менять продуктовые предложения, целевые клиентские сегменты, партнерские стратегии и бизнес-модели. Поэтому при составлении планов на ближайшее время компании должны учесть, что им придется конкурировать на обновленном ИТ-рынке, и помочь заказчикам в создании «интеллектуальной» экономики на базе мобильных, виртуальных и социальных платформ.

НОВОСТИ

БИЗНЕС

McAfee стала дочерней компанией Intel

На днях корпорация Intel объявила о закрытии сделки по приобретению McAfee. Антивирусный производитель продолжит разрабатывать и продавать продукты и услуги в сфере информационной безопасности под собственным брендом. Первые плоды стратегического партнерства Intel и McAfee ожидаются на рынке в течение этого года: компании собираются предложить решения для защиты совершенно нового уровня.

В Intel и McAfee уверены, что принятый подход к защите информации не в состоянии противостоять вирусам на миллиардах интернет-устройств (ПК, смартфоны, телевизоры, планшеты, бортовые системы автомобилей, медицинское оборудование и банкоматы). С ростом киберугроз для обеспечения безопасного выхода в интернет недостаточно существующих технологий. Необходим новый подход, который вместе с программным обеспечением и сопутствующими услугами включает и аппаратные решения. Компании постараются сделать так, чтобы пользователи компьютеров и средств связи находились в большей безопасности.

БЕЗОПАСНОСТЬ

Oracle выпустила брандмауэр для баз данных

Корпорация Oracle анонсировала программный межсетевой защитный экран Oracle Database Firewall. Продукт формирует защитный периметр вокруг баз данных, помогая предотвращать атаки типа SQL Injection и несанкционированные попытки доступа к конфиденциальной информации.

Благодаря технологии, анализирующей синтаксис кода SQL, Oracle Database Firewall проверяет SQL-запросы, посланные базе данных, и в соответствии с предварительно установленными правилами определяет, пропустить, предупредить об опасности, блокировать или заменить эти SQL-запросы. Конфигурируемые опции мониторинга SQL-запросов включают:

- «Белый список» санкционированных SQL-запросов, которые межсетевой экран будет пропускать к базе данных, блокируя все прочие;
- «Черный список» несанкционированных SQL-запросов, которые будут всегда блокироваться;
- Исключения, предлагающие гибкие возможности корректировки применяемых политик безопасности;
- Правила, использующие такие атрибуты, как время, IP-адрес, название приложения, имя пользователя и категорию SQL-запроса.

Malware as a Service (MaaS)

Появление преконфигугированных наборов инструментов для осуществления веб-атак, готового к использованию вредоносного ПО и проч., которые можно приобрести в «черных» App Store.

Алексей Лукацкий, Cisco

В ежегодном отчете по безопасности Cisco еще за позапрошлый год (Cisco 2009 Annual Security Report) мы отметили это явление как одну из набирающих силу тенденций, а первые факты использования технологии «киберпреступление как услуга» нашим специалистам стали известны еще в начале 2000-х годов. С точки зрения защиты, ничего нового использовать не надо — просто необходимо эффективно использовать уже существующие технологии и продукты, правильно настраивать их и своевременно обновлять.

Демьяненко, ESET

Данная услуга на форумах разработчиков вредоносного ПО присутствует уже давно наравне с заказными вирусами, бот-нет сетями и т.д. При этом авторы подобных сервисов предоставляют определенную гарантию, что в случае обнаружения вредоносного ПО антивирусными продуктами, будет выпущена новая версия. На сегодняшний день над модификациями вирусов трудятся организованные группы программистов, которые, естественно, зарабатывают на этом деньги и продают это как «услугу».

Кирилл Керценбаум, IBM

Действительно, данная тенденция набирает обороты последние 2-3 года: разработка вредоносного ПО становится такой же простой и удобной, как это в свое время случилось с разработкой легальных приложений после появления систем объектно-ориентированного программирования. Основной опасностью в данном случае является то, что, во-первых, скорость модификации разнообразного вредоносного кода увеличивается в разы, и обычные сигнатурные методы защиты становятся малоэффективны. Во-вторых, возникает опасность того, что разработка и распространение вредоносных файлов будет вестись сотрудниками самих компаний внутри защищаемого периметра. Таким образом, можно порекомендовать использовать технологии с механизмами проактивной и эвристической защиты, а также инструменты, которые позволяют анализировать и то, что происходит внутри защищаемого периметра, а не только защищаться от атак извне. Например, такими характеристиками обладают современные системы класса Network Intrusion Prevention System (NIPS).

Сергей Маковец, ISSP

Наличие спецсредств для атак на веб-ресурсы у киберпреступников было всегда, ведь черный рынок давно работает. Появление «черных» AppStore вряд ли приведет к увеличению числа атак. Продажа готовых бот-сетей для совершения DDos-атак осуществляется повсеместно. А целевые атаки на определенные сервисы в платежных системах очень сильно зависят от используемой предприятием платформы и, соответственно, такой «инструментарий» используется далеко не повсеместно.

Средства для защиты от веб-атак на сегодняшний день стандартны и входят либо в функционал систем предотвращения вторжений (IPS), либо представляют собой специализированный класс устройств — WAF (Web Application Firewall). ISSP предлагает высокопроизводительные интеллектуальные системы предотвращения сетевых атак от компании Sourcefire и WAF от Breach Security.

Олег Головенко, Symantec

Популярность таких инструментов отрицать сложно. Бизнес «черных» App Store растет: с недавних пор наборы инструментов для веб-атак значительно упростились и теперь стали доступны не только обремененным техническими знаниями «специалистам», но и обычным пользователям. Это ПО позволяет злоумышленникам с легкостью запускать множество содержащихся в комплекте угроз для компьютерных систем. Более того, оно позволяет автоматизировать проведение атак и настраивать действие вредоносных программ таким образом, чтобы избегать их обнаружения.

Один из самых популярных комплектов — Zeus — представляет большую опасность для малого бизнеса. Его основная задача состоит в хищении банковских данных. К сожалению, малые предприятия устанавливают меньше барьеров для защиты своих финансовых транзакций, что делает их уязвимыми и привлекательными для Zeus и мошенников.

Прибыльность таких атак налицо: в сентябре 2010 года в США арестовали группу киберпреступников, которые подозреваются в хищении более $70 миллионов с помощью комплекта Zeus с банковских электронных и торговых счетов, произведенных на протяжении 18 месяцев.

Широкая популярность и спрос спровоцировали рост цен на комплекты для проведения киберататк. В 2006 г. популярный комплект WebAttacker продавался на черном рынке за $15. В 2010 г. ZeuS 2.0 рекламируется по цене почти $8 000.

Недавно корпорация Symantec проводила исследование инструментов для кибер-атак и вредоносных сайтов и зарегистрировала более 310 000 уникальных доменных имен, на которых размещены вредоносные данные. В среднем, Symantec ежемесячно регистрирует более 4,4 миллиона вредоносных веб-страниц.

Денис Безкоровайный, Trend Micro

Явление Malware as a Service уже сейчас вовсю активно, так что было бы ошибкой называть это трендом 2011 года. На криминальном рынке давно доступны конструкторы фишинг-сайтов, троян-киты и остальные наборы инструментов, которыми может пользоваться даже малоподготовленный начинающий киберпреступник. Таким образом, порог вхождения в этот «бизнес» непрерывно снижается, что влечет за собой увеличение количества образцов вредоносного ПО, которое может атаковать бизнес и домашних пользователей. С ростом количества «уникальных» вирусов, которые с функциональной точки зрения являются лишь модификациями, а с точки зрения детектирования антивирусными средствами кажутся абсолютно новыми, требующими новых сигнатур, возрастет потребность бизнеса в новых, не привязанных к сигнатурам, методах обнаружения и блокирования вредоносного ПО. Например, TrendMicro во всех своих продуктах использует репутационный подход на основе системы SmartProtectionNetwork, позволяющий блокировать заражение вредоносным ПО без использования сигнатур, что очень ускоряет блокировку новых и только что созданных модификаций вредоносного ПО.

Дмитрий Петращук, ООО «БМС Консалтинг»

Данная тенденция действительно имеет место. Рынок вредоносного ПО начал формироваться достаточно давно, и на сегодняшний день торговля вирусами и троянскими программами получила очень широкое развитие. Причем объем данного рынка не намного меньше, а по некоторым оценкам, превышает объем рынка средств антивирусной защиты.

Как всякий бизнес, разработка злонамеренного ПО, для того чтобы быть выгодной, должна постоянно предлагать новые продукты, с большими возможностями. Фактически, мы в виде MaaS наблюдаем развитие нескольких ключевых тенденций.

1. Разделение труда — сегодня разработчики вирусов не занимаются их распространением.

Активно работает схема: «Вирусописатель — Продавец — Владелец ботнета — Пользователь-мошенник — Жертва».

Сравните со схемой продажи легального ПО: «Разработчик — Дистрибутор — Магазин — Покупатель»

2. Появление полностью коммерчески ориентированных вирусов, примером которого стал печально известный Zeus.

3. Повышение конкуренции между владельцами бот-сетей, приводящее к настоящим конкурентным войнам, как с подходами к ценообразованию, так и с использованием в программном коде троянских программ элементов, деактивирующих конкурентов.

На этом рынке преконфигурированные наборы инструментов для осуществления веб-атак являются только одним из продуктов, доступных массовому «пользователю».

ПРОДОЛЖЕНИЕ НА С. 19 ▶

ТОП-10 трендов

Аналитики компании WatchGuard Technologies, известного разработчика решений в области информационной безопасности, в конце минувшего года обозначили Топ-10 трендов в области ИТ-безопасности на текущий год. По мнению Эрика Ааристада, вице-президента WatchGuard Technologies, «… 2011-й будет непростым годом для сетевой безопасности, поскольку криминалитет и хакеры перенесут угрозы на новый уровень».

Но сбудутся ли прогнозы аналитиков WatchGuard? По каждому из обозначенных трендов мы попросили специалистов в области ИТ предоставить свои комментарии, а также дать рекомендации ИТ-службам компаний каким образом и с помощью каких решений лучше встретить угрозы 2011 во всеоружии.

Владимир Тихонов, руководитель службы консалтинга «Лаборатории Касперского» в Восточной Европе

Кирилл Керценбаум, представитель по продажам направления IBM Security компании IBM в России и СНГ

Дмитрий Петращук, директор департамента консалтинга в области информационной безопасности ООО «БМС Консалтинг»

Оврашко Андрей, консультант службы телекоммуникационных технологий и информационной безопасности ООО «БМС консалтинг»

Алексей Вагин, ведущий консультант службы телекомуникационных технологий и информационной безопасности ООО «БМС консалтинг»

Павел Демьяненко, руководитель технической поддержки фирмы ESET в Украине

Василий Задворный, начальник отдела ИТ-консалтинга компании «Инком»

Андрей Кузьменко, коммерческий директор компании headtechnology UA

Александр Чубарук, региональный представитель Check Point в Украине

Алексей Лукацкий, менеджер по развитию бизнеса Cisco в Украине

Олег Головенко, технический специалист Symantec

Александр Хомутов, директор компании «ИТ Лэнд»

Сергей Маковец, директор по технологиям, компания ISSP

Денис Безкоровайный, технический консультант Trend Micro в Росси и СНГ

Бизнес-аналитика (появление новых источников информации)

На сегодняшний день при внедрении решений по контролю за безопасностью большинство организаций больше фокусируются на функциях защиты и предотвращения, чем выявления и анализа. В 2011 году приоритеты изменятся. Это означает, что несмотря на все предпринимаемые усилия, вероятность проникновения вредоносного ПО в корпоративную сеть возрастет и выявление и анализ угроз начинают играть первостепенную роль.

Алексей Лукацкий, Cisco

Да, это так, хотя специалистам по безопасности будет непросто выкроить время в своем насыщенном графике для анализа текущей ситуации и тенденций. Специально для этого мы не только запустили бесплатный интернет-ресурс Cisco Security Intelligence Operations (Cisco SIO), на котором можно постоянно получать доступ к информации о текущих Интернет-угрозах, новостях о ИБ, блогах по безопасности, аналитике, статистике, различных Web-инструментах, видео, новостям, бюллетеням по уязвимостям и т.д. Аналогичная информация может быть получена и через специальное бесплатное приложение для iPhone, которое разработала Cisco и которое можно скачать в Apple AppStore.

Кирилл Керценбаум, IBM

Я не готов согласиться с данным тезисом на 100%: данная тенденция также существует на протяжении последних 3-4 лет. Подтверждением этому может служить уже достаточно широкое предложение на рынке так называемых систем Security Event and Information Management (SEIM), на базе которых строятся Security Operation Center (SOC), основным предназначением которых и является анализ и мониторинг систем безопасности для превентивной реакции на разнообразные атаки и нарушения политик безопасности. 2011 год же можно, наверное, считать тем сроком, когда подобные системы начнут проникать в компании среднего и малого бизнеса, пока же это было в основном прерогативой крупных корпоративных заказчиков.

Сергей Маковец, ISSP

Внедрение любых систем информационной безопасности не имеет смысла без полноценного анализа ИТ-активов в организации. Только полноценное и осмысленное внедрение СУИБ (Системы Управления Информационной Безопасностью) позволит создать управляемую инфраструктуру, основанную на анализе рисков и анализе уязвимостей ИТ-активов. СУИБ — это в первую очередь анализ рисков, создание процедур, написание положений политики безопасности и инструкций по эксплуатации информационной инфраструктуры, основанных на требованиях к СУИБ, это и обучение сотрудников, и только потом — внедрение определенных механизмов контроля, основанных на технических средствах.

Денис Безкоровайный, Trend Micro

Задачи выявления вредоносного ПО в корпоративных сетях будут стоять острее в 2011 году, что связано с ростом количества модификаций вредоносного ПО и ослаблением традиционной защиты. Компаниям следует обратить внимание не просто на средства выявления аномалий, а на продукты, сочетающие в себе комплексные механизмы выявления, анализа и блокировки вредоносного ПО. В качестве примера такого продукта можно привести Trend Micro Threat Management Services — это решение может выявлять новые угрозы на основе анализа трафика в корпоративной сети и выявления аномалий и характерных шаблонов поведения, определять источник заражения и пр.

Дмитрий Петрущук, ООО «БМС Консалтинг»

Развитие мобильных технологий, облачных сервисов, повышение динамичности и гибкости бизнес-процессов приводит к тому, что современные корпоративные сети уже не имеют защищенного периметра, — это понятие все больше «размывается». Количество каналов проникновения вредоносного ПО растет экспоненциально. Офицеры по информационной безопасности и администраторы ИТ-систем уже не в состоянии с необходимой скоростью отслеживать все возможные слабые места в защите системы и адекватно внедрять контроли и меры предотвращения угроз.

Информационная безопасность предприятия — это организационный процесс, в который вовлекаются самые разные люди, технологии, решения и функции защиты. И для того, чтобы такой процесс был эффективным он должен включать все формы деятельности по планированию, выявлению и анализу угроз, оценке рисков, выбору и внедрению защитных мер, мониторингу, инцидент-менеджменту, аудиту и планированию последующих превентивных и корректирующих мероприятий.

Александр Хомутов, «ИТ Лэнд»

Что касается конкретных мер, которые могут быть предприняты для защиты Вашей корпоративной инфраструктуры, то, как указывают эксперты WatchGuard, в первую очередь необходимо уделять большее внимание выявлению угроз и аналитическим технологиям. Все более популярными будут технологии, которые улучшают «просматриваемость» сети, помогают идентифицировать угрозы, которые уже присутствуют в ней, сопоставлять все аспекты сетевой атаки и проводить программно-техническую экспертизу. За примерами таких технологий и продуктов далеко ходить не надо — так же компания WatchGuard предлагает целый ряд решений, которые помогут Вам в этих задачах. Стоит обратить внимание в первую очередь на две линейки ее продуктов — устройства для универсальной защиты XTM и XCS, предназначенные для защиты веб-контента и электронной почты.

Владимир Тихонов, «Лаборатория Касперского»

Наиболее правильным является применять комплексно функции выявления-защиты и защиты-предотвращения. Эффективная защита строится следующим образом. Во-первых, проводится информационный аудит на предприятии, во-вторых, выявление несовместимостей или лазеек, через которые могут проникнуть в сеть. После проведения комплексного анализа разрабатывается необходимая структура защиты сети от вирусов и утечки информации. После установки защиты ведется постоянный анализ атак на защищаемую сеть. Таким образом, мы получаем наиболее глубокую информацию для дальнейшей модернизации защиты.

DLP для защиты интеллектуальной собственности

Предполагается, что правительства многих стран на законодательном уровне обяжут компании внедрять более изощренные технологии защиты для исключения возможности неправомерного использования конфиденциальной информации.

Алексей Лукацкий, Cisco

История с WikiLeaks действительно подхлестнула интерес к тематике контроля утечек информации. Однако эксперты компании Cisco, которая и сама является разработчиком DLP-технологий, давно заметили, что попытка подменить техническими средствами задачу работы с людьми к добру не приведет. Утечка конфиденциальной информации — это всегда проблема человеческого фактора, и если человек хочет унести информацию, он ее унесет. Как показывает статистика, существующие DLP-решения ориентированы, в первую очередь, на предотвращение случайных утечек.

Кирилл Керценбаум, IBM

Разговоры о том, чтобы обязать на законодательном уровне компании защищаться от утечек конфиденциальной информации, ведутся достаточно давно, но пока никаких успехов в этом направлении нет даже в странах Европейского Союза. Наиболее строго эти процессы регламентируют в США, в Европе и России действуют определенные правила в отношении сохранности персональных данных, но до тотального внедрения DLP-технологий еще далеко, в первую очередь, это связано с их дороговизной и сложностью.

Сергей Маковец, ISSP

Система DLP позволяет предотвратить неконтролируемые утечки любой информации. По статистике компании Websense, до 85% всех утечек происходит непреднамеренно, другими словами по ошибке. Законодательные инициативы могут стать драйвером развития рынка DLP-систем, если будет правильно сформулировано, что же такое «неправомерное использование конфиденциальной информации». Пока это регулируется внутренними документами компаний и часто вступает в противоречие с Конституцией Украины.

Олег Головенко, Symantec

Согласно результатам недавно проведенного нами исследования, степени защищенности объектов критической инфраструктуры в РФ, российские предприятия рассчитывают, скорее, на свои силы, чем на государственные программы по защите объектов критической инфраструктуры. Отношение предприятий к этим программам скептическое — об этом заявили 35% респондентов. Тем не менее, российские объекты критической инфраструктуры, хоть и в меньшей степени, чем в среднем по миру, но готовы сотрудничать с государством — большинство компаний высказалось по этому поводу нейтрально либо положительно.

Дмитрий Петрущук, ООО «БМС Консалтинг»

С данным утверждением сложно согласиться. Я считаю маловероятной ситуацию, когда правительство обяжет бизнес внедрять конкретную технологию. Да, возможно усиление требований по защите персональных данных, но требования законов, стандартов и правительственных указов в демократических государствах всегда учитывает интересы всех сторон — и граждан, и бизнеса. Примеры принятия решений, которые для защиты прав граждан существенно урезают права и возможности коммерческих компаний в США и Европе, на сегодняшний день отсутствуют.

Василий Задворный, «Инком»

Думаю, не стоит повторно напоминать про разнообразные скандалы, связанные с утечкой конфиденциальных данных, в том числе, и по вине государственных учреждений, которыми был богат прошедший год. Поэтому определенная реакция на защиту данных на уровне государств и межгосударственных организаций определенно будет. Правда, стоит заметить, что работа по регламентации защиты информации и требований к реализации такой деятельности ведется давно. И в данном случае стоит говорить, скорее, про ее новый виток, спровоцированный известными скандалами.

Что касается Украины, прошедший год обогатил список законов и нормативов, касающихся ИБ сразу на два пункта. Во-первых, НБУ опубликовал стандарт ИБ в банках на основании международных стандартов серии ISO. Во-вторых, с 1 января вступил в силу Закон о защите персональных данных. Оставим пока за скобками качество и проработанность данных документов — это предмет исследования, а не комментария. Однако само появление данных документов подтверждает усиление роли государства в сфере управления ИБ.

НОВОСТИ

ВНЕДРЕНИЯ

Многоуровневая система управления данными для «Укртелеком»

Украинский системный интегратор «ЭС ЭНД ТИ УКРАИНА» завершил первый этап проекта реализации архитектуры многоуровневой системы резервного копирования, восстановления и архивирования данных для ОАО «Укртелеком». Основной целью проекта стало обеспечение процесса стандартизации и консолидации бизнес-систем при постоянном росте числа абонентов и услуг оператора. В частности, необходимо было решить задачи: обеспечения гарантированного времени восстановления автоматизированной системы биллинга и ее данных, а также обеспечивающих ИТ-сервисов; уменьшения объема хранящихся резервных копий и совокупной стоимости владения комплексов хранения данных; повышения надежности создания и хранения резервных копий.

В результате проекта заказчик получил прогнозируемое время восстановления для критичных бизнес-систем, а также был существенно уменьшен объем резервных копий за счет технологии дедубликации. Разработаны стандартизованная и формализованная стратегия резервного копирования, а также формализованный план резервного копирования.

Объемы вредоносного ПО «из коробки» продолжат расти

Если раньше предполагалось, что приобретая ноутбук, устройство для хранения данных или даже фоторамку, пользователь получает заведомо свободное от вредоносного ПО аппаратное обеспечение. Но времена изменились! В 2010 году были зафиксированы случаи распространения продуктов известных производителей, инфицированных вредоносным ПО. Более того, однажды такие продукты даже распространялись прямо во время известных конференций по безопасности.

Алексей Лукацкий, Cisco

В этом нет ничего удивительного. Любое доверие — это всегда палка о двух концах. С одной стороны, оно облегчает многие аспекты нашей жизни, а с другой привносит в нее новые угрозы. Нам приходилось сталкиваться со случаями заражения веб-сайтов разработчиков систем ИБ, распространения вредоносного ПО через их системы рассылок и т.д. И это гораздо более серьезная угроза, так как интернет-технологии получают все большее распространение в мире.

Кирилл Керценбаум, IBM

Наверное, можно согласиться, что случаи регистрации заражения «из коробки» продолжат расти, но считать это большой угрозой и устоявшейся тенденцией нельзя. Такие случаи, скорее, характеризуют просчеты в технологическом цикле компаний-производителей, чем преднамеренные действия хакеров, ведь монетизации данного вида угроз добиться на данный момент практически невозможно.

Олег Головенко, Symantec

Нам известны подобные случаи. Хотя по большей части эти инциденты вызваны «человеческим фактором», что еще раз доказывает — в области ИБ самым слабым звеном остается человек.

Дмитрий Петрущук, ООО «БМС Консалтинг»

Не могу согласиться с данным утверждением. Говорить о каком либо росте объема «коробочного» вредоносного ПО не позволяет спорадичность данного явления. Наша компания фиксировала еще в 2002 году случаи поставки в Украину компьютерной техники с «встроенным» злонамеренным кодом, что подтверждалось проверкой популярными на тот момент антивирусными приложениями. Чаще всего проблема заключалась не в мифических «хакерах», проникших в сеть завода по изготовлению винчестеров в Тайване, а в ошибках алгоритмов антивирусов.

Роль Facebook и других социальных медиа в распространении угроз возрастет

Можно провести аналогию с вложениями электронной почты — в свое время они представляли серьезную угрозу для бизнеса. Теперь их заменили ссылки на социальные сети. Сейчас веб выступает источником большинства атак, и в этом контексте Facebook представляет собой ощутимую угрозу.

Алексей Лукацкий, Cisco

Соглашаясь с названной тенденцией, я бы все-таки скорректировал ее в части упомянутого источника угрозы. Facebook, MySpace и подобные им социальные сети пока не получили на постсоветском пространстве ощутимого преимущества по сравнению с «родными» объединяющими людей ресурсами — «ВКонтакте», «Одноклассники», «В кругу друзей» и т.д.

Кирилл Керценбаум, IBM

В данном случае не стоит особо акцентировать внимание именно на угрозах, исходящих от Facebook. Все, что касается социальных ресурсов, будь то Facebook, Twitter, LinkedIn, «ВКонтакте» и проч. несут в себе как огромный новый инструментарий личного и делового общения, так и отличную платформу для вирусописателей. Количество угроз на базе принципов социальной инженерии на протяжении последних 5 лет было стабильно высоким. В основном мы встречались с ними в почтовом и интернет-трафике, теперь же они все активнее распространяются в новых медиа и социальных ресурсах. Что касается рекомендаций, то здесь мы можем говорить об использовании систем защиты проактивного характера и анализа трафика (IPS), а также при наличии возможности с точки зрения характера ведения бизнеса — ограничения или запрета доступа пользователей к определенным ресурсам.

Сергей Маковец, ISSP

Повсеместное распространение технологии Web 2.0 и социальных сетей, действительно, представляет угрозу для современного бизнеса. Нерегламентированное использование социальных медиа приводит к атакам вида XSS, распространению malware, утечкам конфиденциальной информации и, как минимум, к нецелевому использованию каналов связи.

Олег Головенко, Symantec

Да, действительно, известны случаи, когда приложения Facebook пересылали конфиденциальную информацию о пользователе сторонним источникам. Ситуацию осложняет то, что многие социальные сетевые сервисы используются предприятиями и организациями для повышения уровня коммуникаций и продуктивности среди сотрудников. И хотя социальные сети будут продолжать изменять формат сотрудничества коллег в 2011 году, ИТ-организациям придется научиться защищать внутреннюю информацию от этих приложений и управлять ими. Технологии защиты от подобных угроз сейчас уже существуют.

Алексей Вагин, ООО «БМС консалтинг»

Несомненно, количество пользователей социальных сетей стремительно увеличивается. Например, Facebook заявляет о достижении планки в более чем 500 миллионов человек! Большинство из них пользуются услугами социальных сетей непосредственно со своего рабочего места, подвергая опасности, прежде всего, корпоративные активы. Более того, социальные сети — не единственные популярные интернет-приложения. К ним можно также отнести и коммуникационные приложения, и обмен видеопотоками, блоги, игры и т.д. Эти приложения используются как в рабочих целях, так и для персональных нужд. И если в первом случае компаниям необходимо заботиться только о безопасности контента (как с точки зрения наличия в нем вредоносного ПО, так и конфиденциальной информации), то во втором случае возникает проблема нерационального использования рабочего времени.

Василий Задворный, «Инком»

Думаю, что тут украинский тренд вполне совпадает с мировым. Уровень проникновения социальных сетей у нас достаточно высок. А вот уровень культуры их использования не на высоте. Данное замечание касается не только социальных сетей, но и компьютерных технологий вообще. Рядовые пользователи в подавляющем большинстве просто не знают о существовании целого ряда угроз ИБ, черпая основные знания о предмете в основном из голливудских фильмов. Кроме того, ситуация усугубляется значительным распространением приложений, использующихся в социальных сетях.

Владимир Тихонов, «Лаборатория Касперского»

В настоящее время доступ к социальным сетям полностью блокируют лишь четверть компаний. Многие признают, что корпоративное присутствие на таком сервисе помогает развитию бизнеса. Но в то же время, количество спама, которое попадает к пользователю через социальные сети растет из года в год. Самым опасным из четырех популярных социальных ресурсов (Facebook, Twitter, MySpace и LinkedIn) стал Facebook.

ВКРАТЦЕ

ПО

Oracle переносит Open Office в облака

Корпорация Oracle представила два полных пакета офисных программ — Open Office 3.3 и Oracle Cloud Office. В их основе кодовая база перешедшего под контроль корпорации открытого проекта OpenOffice.org, однако впервые Oracle наряду с локальной версией офисного пакета Open Office предлагает его облачную редакцию. По словам вендора, оба пакета базируются на открытых стандартах и способны исполняться на персональных компьютерах, Web-клиентах и мобильных устройствах. Сделав этот шаг, Oracle вступает в конкуренцию с такими офисными решениями, как Google Docs и Microsoft Docs.com

В состав обоих пакетов, основанных на формате Open Document Format (ODF) и обеспечивающих совместимость с различными версиями Microsoft Office, входят приложения для создания текстовых документов, таблиц, презентаций, баз данных и графических изображений. Указанный комплекс офисных приложений работает на платформах Windows, Mac, Linux, в Web-браузерах и на смартфонах (в частности, на iPhone). Oracle Cloud Office 1.0 позиционируется как пакет программ для Web и мобильных пользователей, позволяющий множеству сотрудников совместно работать над документами в стиле Web 2.0 и иметь мобильный доступ к нужным документам. Из пресс-релиза вендора не ясно, обладают ли облачная и мобильная версии офисного пакета всей функциональностью традиционного локального решения Open Office.

Oracle Open Office 3.3 включает новые расширения для приложений Oracle Business Intelligence, Oracle E-Business Suite и Microsoft Sharepoint, что делает интеграцию с отдельными видами корпоративного ПО более быстрой и не требующей дополнительных настроек. Утверждается, что стоимость лицензии Oracle Open Office 3.3 почти в пять раз ниже стоимости Microsoft Office. По данным ZDNet, корпоративная лицензия обойдется заказчикам (организации, в которых больше 100 пользователей) в 90 долл., а стандартная — в 49,95 долл. Первая способна работать на всех упомянутых платформах, поддерживает 17 языков, включает ряд инструментальных средств и коннекторов к внешним приложениям. Вторая развертывается только на одной платформе и поддерживает единственный язык. В отличие от аналогичных пакетов ряда конкурентов бесплатные лицензии для частных пользователей не предусмотрены. Не обнародованы пока и условия, на которых заказчикам и партнерам будут предоставляться такие облачные офисные программные сервисы.

С. С.

НОВОСТИ

BICS заключила 10-летний контракт с компанией «ИнфопульсУкраина»

«Инфопульс» подписал контракт с компанией «BICS», котораявходит в состав BelgacomGroup и являетсяведущиммеждународным провайдером голосовойпочты, роуминга, связи и мобильныхфинансовых услуг. Ориентированный на построениедолгосрочногосотрудничества, контракт потребуетпродления только в конце 2020 года. Согласно генеральному соглашению, «Инфопульс» будетпредоставлятькомпании «BICS» различныеИТ-услуги, в том числеподдержку приложений BICS, разработку на .NET и Java платформах, а такжепроведение ITT тестирования.

«С Инфопульсомбылподписан контракт, так как он победилв конкурентном тендере. Решающими фактором для выбораИнфопульсадолгосрочныстратегическим партнером по ИТ аутсорсингу стали отличноекачество ИТ услуг, высокаяквалификация IT специалистов, быстраяреакция и гибкость по отношениюк выполнению наших требований.

«Взломанный автомобиль»

Хакеры постоянно находятся в поиске новых способов проникновения в вычислительные устройства. По мере проникновения высокотехнологичной электроники в автомобили перед злоумышленниками открываются новые возможности. Это тем более опасно, если учесть, что таким образом они смогут нанести даже физический вред человеку.

Алексей Лукацкий, Cisco

Да это действительно так, но я не могу согласиться с тем, что это тенденция 2011 года, особенно в Украине, России, Белоруссии и т.д. Как с точки зрения отсутствия собственных разработок в этих областях, так и с точки зрения пока невысокого уровня технологического развития республик бывшего СССР.

Что касается международного опыта, то как участник международной организации по стандартизации ISO, могу сказать, что работа в этом направлении ведется и уже давно. Например, в подкомитете №3 технического комитета по стандартизации №22 «Электрическое и электронное оборудование», а также в ТК 204 «Интеллектуальные транспортные системы». В качестве примера их работы назову только два документа — в 2001 году был разработан специальный стандарт ISO 15031-7:2001 «Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 7: Data link security», а в 2008 — ISO 24534-5:2008 «Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles — Part 5: Secure communications using symmetrical techniques», посвященные теме безопасности.

Кирилл Керценбаум, IBM

Давно стало очевидно, что по мере все большего проникновения компьютерных технологий в нашу жизнь, так же глубоко начнут проникать туда и компьютерные вирусы. Но при этом нужно помнить, что основная задача современного вредоносного кода, закладываемая его разработчиками, — это извлечение прибыли путем сбора или хищения личной информации, статистики, слежения и др., а вот нанесение повреждений как компьютерным системам, так и их пользователям, к счастью, пока на повестке дня не стоит.

Сергей Маковец, ISSP

Считаю, что угрозы хакеров для автомобильной промышленности сильно завышены. Больший урон любому объекту, управляемому АСУ, могут принести ошибки в программном коде. Пресловутый человеческий фактор был и будет главным источником уязвимостей и сбоев в работе любого компьютеризированного средства, возможно, даже систем наведения.

Денис Безкоровайный, Trend Micro

На данный момент распространению вредоносного ПО в автомобилях мешает специфичное и нетиражируемое системное ПО, устанавливаемое в транспортные средства. Но уже есть тенденции к унификации части автомобильного ПО, что в свою очередь увеличит риск распространения вредоносного ПО. Правда, пока не ясно как именно злоумышленники смогут монетизировать «взломанный» автомобиль, ведь известно, что жажда наживы является основной движущей силой киберпреступников. Так что эксперименты со «взламыванием» автомобилей, скорее всего, останутся уделом любителей и не станут массовой проблемой, по крайней мере, в 2011 году.

Владимир Тихонов, «Лаборатория Касперского»

Современный уровень развития ИТ-технологий позволяет через интернет запросить у своей кофе-машины чашечку кофе и через пару минут подойти и забрать готовый продукт. Теоретически, даже кофеварка может быть заражена вирусами. Все устройства с ПО и возможностью связи с сетью являются потенциальной целью вирусов.

Изменение понятия «периметра сети»

Корпоративные сети становятся все более мобильными, а значит, устройствам из их состава требуется защита и за пределами традиционного периметра. Очевидно, это приведет к перераспределению акцентов, компании начнут уделять все больше внимания защите их основного актива — данных и, как следствие, ЦОД.

Александр Чубарук, Check Point

Вопросы информационной безопасности продолжают оставаться краеугольным камнем модели публичного облака. Именно сомнения в безопасности бизнес-приложений и данных при передаче их третьим лицам (провайдерам публичных облачных сервисов) сдерживают большинство предприятий от перехода (полного либо частичного) в облака.

Кирилл Керценбаум, IBM

Это явление не станет тенденцией 2011 года, такая характеристика является данностью уже фактически с момента появления ноутбуков, смартфонов и удаленного доступа к почте, что произошло как минимум лет 5 назад. Сейчас основное давление на осовремененное «понятие периметра сети» осуществляет нарастающая популярность SaaS (Soft-as-a-Service) услуг, а также аренда ЦОДов, а не построения своего собственного. Поэтому мы все больше переходим от защиты, основанной на географической или физической границе, к защите непосредственно данных в зависимости от их разнообразных характеристик.

Алексей Вагин, ООО «БМС консалтинг»

Проблема трансформирования периметра сети от граничных межсетевых экранов, разделяющих локальную вычислительную сеть от сетей интернет до уровня персонального компьютера (ноутбука, КПК) сотрудника компании — не нова. По опыту «БМС Консалтинг» могу сказать, что довольно много компаний, содержащих в своем штате мобильных сотрудников, уже ощутили это на себе. В случае, когда к информационной безопасности подходили комплексно, такая трансформация не вызывала особых проблем. К сожалению, таких примеров немного.

Действуя по принципу «делай как все», администраторы безопасности не задумываются об угрозах, применимых непосредственно к их предприятию. Только за прошлый год по причине недостаточной защиты (или ее полного отсутствия) рабочих мест сотрудников (включая мобильных) компаниям был нанесен ущерб, который исчисляется миллиардами долларов. Причин этому может быть множество, и все их можно распределить по следующим группам:

- проникновение вредоносного программного обеспечения в корпоративную сеть;
- перехват конфиденциальной информации при использовании незащищенного удаленного доступа к корпоративным ресурсам;
- потеря (кража) компьютеров/ноутбуков и съемных носителей информации.

Для защиты от таких угроз возможно применение различного рода агентов безопасности:

- персональный брандмауэр;
- персональный IPS;
- антивирус;
- система контроля запуска приложений;
- система контроля портов ввода/вывода;
- контроль доступа к WEB-ресурсам;
- шифрование дисков;
- шифрование съемных носителей;
- клиент удаленного доступа.

Владимир Тихонов, «Лаборатория Касперского»

Понятие защиты «периметра сети» изменилось с появлением большого количества мобильных устройств в корпоративной сети, таких как ноутбуки, мобильные телефоны и коммуникаторы. В концепции Kaspersky Open Space Security уже учтена возможность попадания вируса не только снаружи, но и изнутри сети. Благодаря линейке решений Kaspersky Open Space Security сеть защищена системно, а значит, все ее элементы находятся под контролем и не смогут распространять вирусы изнутри.

НОВОСТИ

БЕЗОПАСНОСТЬ

Никогда не доверяйте содержимому SMS-спама

Новое исследование Spam Reporting Service, проведенное ассоциацией GSM, показало, что почти две трети (70%) всех спамовых SMS-сообщений, поступающих абонентам, представляют собой угрозу мошенничества. Данные собирались с марта по декабрь 2010 г. при содействии таких операторов, как AT&T, Bell Mobility, KT, Korean Internet & Security Agency (KISA), SFR, Sprint и Vodafone.

Анализ данных показал, что спам был обнаружен во всех сетях всех перечисленных операторов, причем его уровень был выше ожидаемого. Выявленные атаки использовали сложную модификацию сообщений и передачу малого количества сообщений с одного телефонного номера, чтобы усложнить и затянуть на как можно дольше определение источника спама. Методы генерации спама отличались в зависимости от региона мира, поэтому задача совместной борьбы с этим явлением еще более усложнилась.

Хотя примерно одна десятая часть идентифицированного злонамеренного спама выглядела вполне содержательной, большинство сообщений было направлено на получение выгоды их отправителем, а 70% — явно имели признаки атаки на финансовые сервисы.

Аналитики разделили SMS-угрозы на две категории: фишинг (сбор финансовой информации) и социальное мошенничество (просьба занять деньги или сделать ставку в игре). Оказалось, что в Азии основное количество вредоносных SMS связано с социальным мошенничеством. В Европе примерно четверть атак связано с мошенническими лотереями, просьбами о деньгах и страховыми сервисами, причем каждое пятое сообщение выглядело вполне невинно. В Северной Америке огромная часть спама являлась просьбами ссудить деньгами.

Malware...

◀ ПРОДОЛЖЕНИЕ СО С. 16

Похоже, что в будущем нас ждут новые еще более масштабные атаки, более агрессивные бот-сети, и не за горами активный переход разработчиков вредоносного ПО на «облачные» технологии.

Александр Хомутов, «ИТ Лэнд»

Нельзя не согласиться с аналитиками WatchGuard в том, что распространение «вредоносного ПО как услуги» (MaaS) может стать одной из самых серьезных угроз наступившего года. По мере того, как хакерство становится все более организованным и все более попадает под криминальный контроль, хакерский «андеграунд» начинает имитировать коммерческие рынки, в результате чего на черном рынке появляются готовые «киты взломщика». Сейчас на хакерских сайтах и форумах можно купить комплекты для веб атаки, готовые к использованию ботнеты и вредоносное ПО. Согласно прогнозу WatchGuard, в 2011 году криминальный андерграунд сделает еще один шаг вперед, создав удобные интернет-магазины вредоносного ПО. Это означает, что «скрипт кидди» (неграмотные молодые взломщики) смогут запросто развертывать свои бот-сети.

Конечно, борьба с такого рода опасностями не относится к компетенции ИТ-служб и специалистов по безопасности отдельных компаний. Ею должны заниматься соответствующие структуры на государственном и международном уровнях, то же самое можно сказать об эскалации кибервойн.

Владимир Тихонов, «Лаборатория Касперского»

Уже прошло то время, когда вирусы создавали студенты ради банального развлечения. На сегодняшний день вредоносное ПО пишется, по большей части, «на продажу», либо для достижения финансовых целей группы разработчиков. Таким образом, вирусы превратились в готовый инструмент, который могут использовать не только специалисты кибер-технологий, но и рядовые пользователи. Это стало уже трендом в последние годы.

Вырастет количество VoIP-атак

Атаки на VoIP-серверы сравнятся по популярности с атаками на почтовые серверы. Отчасти это связано с наличием в открытом доступе инструментов для их осуществления, например, SIPVicious.

Алексей Лукацкий, Cisco

Компания Cisco и наши заказчики очень редко сталкиваются (и вряд ли число столкновений вырастет в будущем) с этой угрозой. Видимо причина в том, что безопасность — это неотъемлемая часть всех наших технологий — от систем хранения данных и оборудования для домашних сетей до беспроводных решений и систем TelePresence.

Павел Демьяненко, ESET

Не уверен, что сравнятся в этом году, поскольку в Украине использование VoIP-телефонии пока еще не настолько популярно, но я думаю, что это ожидает нас достаточно в скором будущем.

Кирилл Керценбаум, IBM

Атаки на VoIP-серверы вряд ли будут столь популярны как, например, атаки на различные веб-ресурсы. Здесь мы можем говорить в первую очередь об атаках класса DoS и DDos, служащие основным инструментов нечестной конкуренции, но при этом нужно понимать что VoIP-серверы не получил и такого широкого распространения, как почтовые или веб-серверы, которые как минимум по одному а то и больше имеет каждая компания. Угрозы для VoIP скорее будут больше концентрироваться в части эксплуатации этих каналов передачи информации для транспортировки вредоносного трафика, а также для получения доступа к той легитимной информации, которая по ним передается.

Оврашко Андрей, ООО «БМС консалтинг»

За последнее 10 лет наблюдается интенсификация влияния коммуникаций на рынок. Это непременно сказывается на нашем образе жизни. Все большую популярность набирают голосовые сервисы и средства их интеграции с инфраструктурой компаний. Тем не менее, кроме удобства это непременно несет и угрозы. Одним из наиболее распространенных протоколов VoIP является SIP, который, помимо преимуществ, имеет ряд недостатков, связанных с безопасностью. Гибкость и расширяемость протокола с одной стороны, с другой стороны является его уязвимым местом, позволяя злоумышленникам эффективно разрабатывать эксплойты сервисов, использующих SIP. По опыту проектов «БМС Консалтинг» скажу, что были замечены случаи «угона» SIP-серверов небольших компаний. Такие серверы, как правило, использовались для звонков за рубеж либо как площадки для атак более крупных целей.

Сергей Маковец, ISSP

Технология VoIP распространена повсеместно. Она однозначно удобна и имеет большую гибкость. Не удивительно, если число VoIP-атак будет расти экспоненциально.

APT (Advanced Persistent Threats) — аббревиатура, которую предстоит выучить

Единого определения видов угроз, которые подпадают под APT пока не существует, но это не меняет сути — отдельный класс представляющих особенно высокий уровень опасности угроз, атак, способов инфицирования и техник распространения вредоносного ПО уже нельзя игнорировать. Угрозы класса APT могут подолгу скрываться в сети жертвы, очищать информацию в журналах и иметь очень изощренные цели.

Павел Демьяненко, ESET

Я бы отнес к этому виду угроз те разновидности нетривиального вредоносного ПО, над созданием которого трудятся организованные группы программистов. Как правило, они ежедневно выпускают новую модификацию угрозы, избегая обнаружения антивирусными программами. В данном случае борьба напоминает игру в «кошки-мышки», когда вирусные лаборатории трудятся над выпуском сигнатур с наиболее вероятными модификациями угрозы, а пользователи страдают от вредоносных действий программы.

Андрей Кузьменко, headtechnology UA

Для борьбы с громадным количеством угроз, в том числе и APT, организации покупают множество различных решений — IPS, firewalls, Vulnerability Scanners и т.д. Но эти системы уже не в состоянии обеспечить комплексную защиту. В очень многих случаях компаниям не хватает просто видимости того, что происходит в их сети.

Кирилл Керценбаум, IBM

Уже сейчас примерно 80% угроз являются угрозами типа APT и, как уже отмечалось выше, с подобными угрозами уже практически невозможно бороться стандартными методами: ни сигнатурный анализ, ни стандартная эвристика не может увидеть подобные «плохие» программы-хамелеоны, всячески демонстрирующие средствам защиты свои положительные характеристики. Как мы знаем, уже даже наличие цифровой подписи (вирус Stuxnet, к примеру, ее содержал) не может являться гарантией легитимности того или иного файла. К сожалению, по-прежнему не существует инструментов, которые могут на 100% гарантировать защиту от угроз класса APT, однако при комплексном подходе к организации системы защиты, базирующейся на различных взаимоисключающих и взаимодополняющих технологиях, грамотных политиках информационной безопасности и повышения грамотности пользователей ПК, риски от подобных угроз можно свести к минимуму.

Сергей Маковец, ISSP

APT является очень опасным видом угроз, особенно ввиду того, что к этому типу угроз относятся blended «смешанные» или low and slow «вялотекущие» атаки. Большинство таких атак невозможно отследить в сетевом трафике или обнаружить определенной сигнатурой в базе антивируса или правилом системы IPS. Такие атаки могут проводиться достаточно продолжительное время, иметь определенный алгоритм или шаблон поведения и обнаруживаться анализом системных событий и событий аудита. APT характеризуются повышением полномочий, внедрением шпионского ПО и, как правило, зачисткой следов присутствия в журналах регистрации.

Олег Головенко, Symantec

Целевые атаки с использованием угроз класса APT, которые произошли в 2009 году, часто мелькали в заголовках газет в начале 2010. Наиболее заметным из них был троян Hydraq (a.k.a., Aurora).

Как правило, этот тип атаки начинается с разведки, которая может включать в себя изучение общедоступной информации о компании и ее сотрудниках, например, из социальных сетей. Затем эта информация используется для создания специальных узконаправленных фишинговых сообщений электронной почты, нацеленных на компанию или конкретных сотрудников. Успешная атака может предоставить злоумышленнику доступ к сети предприятия.

В случае атаки Hydraq, для установки трояна эксплуатировалась ранее неизвестная уязвимость в Internet Explorer, а также закрытая уязвимость в Adobe Reader и Adobe Flash Player. После завершения установки злоумышленники могли выполнять различные действия на зараженном компьютере, в том числе предоставляя полный удаленный доступ.

Обычно, когда такие атаки проводятся в отношении отдельных лиц, вся нужная информация сразу собирается и злоумышленники переходят к следующей цели. Однако, APT-атаки предназначены для того, чтобы оставаться незамеченными в информационных системах предприятия для сбора информации в течение длительных периодов.

Дмитрий Петращук, ООО «БМС Консалтинг»

Определение аббревиатуры APT в данном вопросе не совсем корректно. Данное буквосочетание используется для описания техник сетевых атак и взлома, которые давно известны и сами по себе серьезной опасности не представляют, но, использованные совместно в течение продолжительного времени и направленные против одной жертвы, данные атаки способны привести к проникновению в практически любую сеть.

Давайте рассмотрим следующую аналогию: «Уже привычное дело, если у кого-то в общественном транспорте украли из пальто мобильный телефон. Это серьезная проблема для пострадавшего и неприятный случай как таковой. Представим же, что все карманники города договариваются целенаправленно и постоянно обчищать карманы некоего Иванова Ивана Ивановича, когда он утром едет на работу…». Вот этим Иваном Ивановичем и становятся компании-жертвы атак класса APT.

Следует понимать, что заказчиком такой атаки, как правило, может быть только организация уровня правительства государства или крупной международной компании, так как для проведения целенаправленной APT-атаки необходимо серьезное финансирование, а значит, предполагается серьезная выгода для атакующего.

Для того чтобы определить, является ли ваша компания потенциальной жертвой APT-атаки можно воспользоваться рекомендациями CEO компании «Imperva», Амичая Шулмана, и ответить на следующие вопросы.

- Ваш веб-сайт размещен на домене .mil или .gov?
- Ваша организация обеспечивает защиту государства?
- Ваша компания поддерживает национальную инфраструктуру (электроэнергия, транспорт, связь, ресурсы)?
- В вашей сети хранится персональная информация, которая может заинтересовать правительства других государств, например, членов оппозиции китайского правительства?

В результате вы сможете убедиться, что на самом деле не так много существует в мире компаний, которым необходимо серьезно опасаться атак класса Advanced Persistent Threats.

НОВОСТИ

Cisco анонсировала приложение Jabber для унифицированных коммуникаций

На проходившей в Орландо (штат Флорида) выставке Enterprise Connect 2011 компания Cisco анонсировала приложение Cisco Jabber для унифицированных коммуникаций. Оно поддерживает функции учета присутствия, мгновенных сообщений, передачи голоса, видео и голосовых сообщений, совместной работы и конференц-связи на обычных компьютерах, компьютерах с ОС Mac OS, планшетных системах и смартфонах. Cisco Jabber помогает корпоративным пользователям осуществлять несложный и безопасный, с точки зрения доступа к информации, поиск нужных людей, выяснять, доступны ли они для связи, и если да, то на каких устройствах, а также вести совместную работу, выбирая тот или иной метод либо устройство по своему усмотрению.

Приложение Cisco Jabber (будет доступно пользователям Mac-компьютеров с лета 2011 года) создает унифицированный клиентский интерфейс, размещаемый либо на клиентском компьютере, либо в сетевом облаке. Он дает пользователю возможность легко и беспрепятственно переходить от мгновенных сообщений к голосовой и видеосвязи и буквально на лету запускать функции совместной работы. Кроме того, пользователи получат мгновенный доступ к необходимым функциям как в офисе, так и за его пределами.

Приложение Cisco Jabber доступно уже сегодня или станет доступным в будущем для платформ Windows, iPhone, iPad, Nokia, Android и BlackBerry. Помимо этого, Jabber интегрируется с оконечными видеоустройствами Cisco Unified IP Phone, Cisco Web Ex Meeting Center и CiscoTele Presence. Поддержка различных платформ в любом месте, наиболее удобном для пользователя, делает совместную работу более быстрой и эффективной. Кроме того, скоряются процессы принятия решений и меж корпоративного сотрудничества, повышается производительность труда.

Приложение Cisco Jabber основано на технологи Jabber Inc. Cisco приобрела эту компанию в 2008 году. Функции Cisco Jabber совместимы с решением Cisco Unified Communications Manager (версия 6.1.4 и выше).

Защита в трех измерениях

Доход компании Check Point Software Technologies, специализирующейся на разработке систем безопасности для интернета, в 2010 финансовом году впервые превысил $1 млрд. Успешные финансовые результаты были обусловлены повышенным спросом на ее продукты сетевой защиты. Некоторое время назад разработчик представил концепцию ИТ-безопасности 3D Security, которая определяет безопасность как бизнес-процесс, объединяющий политики, персонал и выполнение требований. В рамках этой концепции в середине февраля был анонсирован принципиально новый продукт Check Point R75. О последних решениях компании и планах экспансии на украинском рынке мы говорили с Александром Чубаруком, менеджером по продажам в Украине.

ИНТЕРВЬЮ

PCWeek/UE: Александр, вы работаете в компании Check Point с июня прошлого года. По вашим ощущениям, насколько украинский рынок «созрел» к внедрению более комплексных и продвинутых в сравнении с обычными антивирусами решений по информационных безопасности?

АЛЕКСАНДР ЧУБАРУК: Уровень зрелости зависит от типа бизнеса. Например, наши традиционные заказчики из банковского сегмента и телеком-сектора «созрели» уже давно. У этих компаний имеется понимание правильной методологии комплексной системы информационной безопасности, есть выделенные департаменты ИБ, которые предметно занимаются данной тематикой. С моей точки зрения, государственный сектор также созрел к подобным комплексным решениям, но там своя специфика.

Кроме того, существуют определенные внешние драйверы. В банковской сфере, например, это PCI DSS и другие отраслевые стандарты, требующие внедрения комплексных встроенных систем ИБ. То же самое касается и телекоммуникационного сектора. Во многих странах, в том числе и в нашей стране, принят закон о защите персональных данных. Это внешние факторы, которые не просто стимулируют, а требуют у компании, обладающей определенными данными, наличия адекватных систем их защиты.

По моим ощущениям в последнее время в корпоративном секторе Украины наблюдается интерес к тому, как правильно строить системы ИБ. То есть, вместо лоскутного подхода, обеспечивающего определенную степень защиты с помощью антивируса или файрвола, компании подходят с методологической точки зрения с намерением правильно пройти все этапы.

PCWeek/UE: В представленной вами концепции 3D Security безопасность определяется как трехмерный бизнес-процесс, объединяющий политики безопасности, людей (в основном персонал компании, но не только) и выполнение требований. Однако пользователи всегда были слабым звеном в ИБ, а социальная инженерия неизменно будет главной угрозой для безопасности. Почему же речь об 3D Security зашла только сейчас?

А.Ч.: Начнем с того, что все традиционные системы, скажем так, вчерашнего дня, предполагали реализацию определенной политики безопасности. Например, межсетевой экран реализовывал политику безопасности защиты периметра сети, определял, к каким интернет-ресурсам пользователи могут иметь доступ через этот защитный экран, и какие сервисы компании видны снаружи, из интернета. Основная сложность заключается в том, каким образом происходит идентификация пользователей, которые, как было отмечено, являются основным слабым звеном.

Так вот сложность в том, что они идентифицировались по IP-адресу, причем многие компании применяют такой метод до сих пор. Предполагалось, что у пользователя есть свой компьютер с закрепленным за ним IP-адресом, и если мы пишем политику ИБ для данного IP-адреса, то она действует для сотрудника, который работает за данным компьютером.

Сегодняшние системы построения инфраструктуры организации предполагают, что пользователь может работать с любого компьютера, с любого устройства. При этом IP-адреса на разных устройствах также будут различными.

Кроме того, сегодня во многих организациях используются системы DHCP, и не факт, что один и тот же компьютер пользователя будет получать один и тот же IP-адрес. Какую методику применяют в этом случае для файрвола? Пишут политику для целого набора IP-адресов, однако в такой политике невозможно выделить конкретных пользователей. Например, если правило разрешает доступ к какому-либо интернет-ресурсу, то разрешает всем. Ведь с помощью традиционных технологий нельзя реализовать гранулированную политику вплоть до конкретного пользователя.

Иными словами, нет средств, которые будут отслеживать, что один и тот же пользователь получает доступ с разных устройств — например, с десктопа и с мобильного устройства. Такое развитие инфраструктуры стало возможным сегодня и в ответ Check Point предлагает концепцию и механизмы построения политики и системы информационной безопасности в соответствии с требованиями сегодняшнего дня.

PCWeek/UE: Каким образом реализуется гранулированная политика безопасности сегодня?

А.Ч.: Для этого система должна отслеживать и ассоциировать с одним и тем же пользователем несколько IP-адресов. Нашей компанией был разработан механизм, который позволяет интегрировать интернет-шлюз с Active Directory. Когда пользователь пытается получить доступ к внешним ресурсам, то шлюз, через который производится подключение, с помощью механизма идентификации определяет, что в данный момент подсоединяется, например, Александр Чубарук и выбирает политику доступа к внешним ресурсам, которая прописана именно для конкретного пользователя, а не для IP-адреса. И если я завтра зайду с другого компьютера и с другим IP-адресом, он все равно определит, что это Александр Чубарук и применит политику, созданную для данного пользователя.

PCWeek/UE: Насколько сложен процесс внедрения продукта R-75? Ведь это не обычная утилита, которую пользователь может самостоятельно установить, не прибегая к помощи специалистов или консультантов вендора?

А.Ч.: На самом деле, возможен и такой вариант. Продукты Check Point всегда славились дружественным интерфейсом и этим подкупали администраторов безопасности. Все действия и настройки производятся через графический интерфейс и, соответственно, те средства управления, которые предоставляет Check Point посредством GUI плюс руководство по настройке позволяют запустить систему со стандартными настройками самостоятельно. Системные интеграторы же работают в основном на сложных технологических проектах, которые предполагают серьезный сетевой ландшафт или распределенную систему.

PCWeek/UE: Насколько прост процесс добавления программных блейдов, которые входят в состав R75?

А.Ч.: Все производится по аналогии с аппаратным блейд-сервером: если нужно нарастить функционал, добавляется новое лезвие в шасси. Например, на

Александр Чубарук

шлюзе заказчика изначально активированы два блейда — файрвол и VPN, а пользователь хочет добавить еще один — IPS. Во-первых, ему необходимо купить подписку на новый модуль. Во-вторых, для активации функционала достаточно установить отметку «√» в перечне того ПО, которое работает на шлюзе. Соответственно, новый блейд активируется и начинает работать. Все программные блейды поставляются со стандартными политиками безопасности.

PCWeek/UE: Check Point выпускает аппаратные и программные решения. В каких случаях компания-заказчик должна выбирать ПО, а в каких — аппаратные устройства?

А.Ч.: Традиционно, Check Point являлся производителем ПО, и весь функционал шлюза безопасности сети предоставлялся в программном варианте. В последние несколько лет в портфеле Check Point появились и аппаратные устройства. В чем их основное преимущество? Если в процессе эксплуатации возникают какие-то ошибки, исключен вариант обращения заказчика к нескольким службам технической поддержки.

Если же в компании заказчика применяется программное решение, установленное на сервере какого-либо производителя, и происходит сбой, очень важно вначале идентифицировать, что было причиной сбоя: ПО или само оборудование. В случае использования комплексного «железного» решения такой вариант исключен: заказчик имеет единую точку входа в службу техподдержки Check Point, которая решает все проблемы.

PCWeek/UE: Какова ценовая политика на аппаратное обеспечение и ПО?

А.Ч.: Программное обеспечение дешевле, но стоимость технической поддержки чуть дороже за счет того, что приходится иногда решать вопросы на уровне «железо-софт». Если брать аппаратное решение, то само устройство изначально чуть дороже, но поддержка на него дешевле.

PCWeek/UE: Какими критериями следует руководствоваться заказчику при выборе аппаратного или программного продукта?

А.Ч.: Если заказчик хочет сэкономить на начальных инвестициях и у него уже имеется сервер, то ему дешевле взять программный продукт. Если же он планирует систему с нуля, имеет смысл рассмотреть приобретение аппаратного решения.

PCWeek/UE: Сколько стоит внедрить Check Point, назовите диапазон цен?

А.Ч.: От нескольких сотен долларов до миллиона, все зависит от масштаба ИТ-инфраструктуры. Есть решения для SMB-сектора, например, Safe@Office, которые продаются и в Украине, их стоимость начинается с $500-600. И есть крупные проекты, в которых общая инсталлированная база переваливает за миллион: это внедрения в крупнейших украинских банках и телекоммуникационных компаниях.

PCWeek/UE: Можете рассказать о планах Check Point в Украине на ближайшее время?

А.Ч.: В 2011 году мы хотим вывести на рынок качественно новые виды сервиса и поддержки, иными словами, приблизить тот сервис, который получают в Украине наши заказчики, к европейской модели. Имеются в виду как сроки подмены аппаратного обеспечения, так и время реагирования на проблемы заказчиков.

Также в планах дальнейшее развитие партнерской сети и повышение квалификации существующих партнеров. Развитие офиса Check Point, скорее всего, будет зависеть от многих факторов — в том числе и от достижения плановых показателей продаж.

НОВОСТИ

БЕЗОПАСНОСТЬ

IPS-система с пропускной способностью 20 Гбит/с

На конференции по информационной безопасности RSA Conference корпорация IBM представила высокопроизводительное устройство для обеспечения сетевой безопасности.

Система IBM Network Intrusion Protection System (IPS) GX7800 предоставляет организациям возможность защищать свои данные и инфраструктуру от неавторизованного доступа и атак без ущерба для производительности и готовности важнейших бизнес-приложений.

В частности, это устройство:

- работает с пропускной способностью около 20 Гигабит в секунду (Гбит/с);
- предоставляет организациям полный комплекс средств обеспечения безопасности — таких как защита веб-приложений — без снижения пропускной способности сети;
- распространяет средства обеспечения безопасности на облачные среды для защиты данных;
- использует результаты исследований службы IBM X-Force, помогая компаниям заблаговременно защищаться от угроз.

Новое устройство позволяет развернуть средства обеспечения безопасности в базовой сети, где производительность и готовность особенно важны. Эти средства включают, помимо всех ключевых функций традиционных систем IPS, такие возможности, как защита web-приложений, предотвращение потерь данных и технология Virtual Patch, и все они могут выполняться одновременно для повышения уровней безопасности. Например, благодаря интеграции с решением IBM Rational AppScan, новая версия системы может автоматически создавать специальные политики безопасности для защиты web-приложений, исходя из уязвимостей, выявленных с использованием AppScan.

Безопасность облачных инфраструктур: развенчиваем мифы

ЕВГЕНИЙ ЖИЛЯКОВ, ИНСТРУКТОР CISCO КОМПАНИИ NOVAX

Многие противники перехода к облачным сервисам мотивируют свою позицию тем , что «это небезопасно». Встречный аргумент достаточно прост — ничто не безопасно. Если компания хочет экономить деньги за счет использования облака, то ей придется глубоко проанализировать существующую политику безопасности, чтобы определить какая часть ответственности ложится на плечи провайдера и какие механизмы будут регулировать взаимодействие двух организаций по части защиты информации. Разумеется, это непросто, и в процессе доработки политики компанию ожидает ряд трудностей. Тем же компаниям, в которых политика безопасности отсутствует как таковая, переживать вообще нечего — для них процесс перехода пройдет незаметно.

ОБЗОРЫ

«Облако» сейчас является центральной темой обсуждений в сфере ИТ. И те, кто все еще скептически утверждает, что переход к облачным решениям необязателен и большинство украинских компаний в нем не нуждаются, должны вспомнить судьбу таких «новинок» как IP-телефония, конвергенция и виртуализация. Со временем все больше ИТ-ресурсов будут перемещены в облако. Следовательно, подразделения, ответственные за безопасность, должны уже сейчас модифицировать корпоративную политику для будущей поддержки подобных решений.

Прежде всего, определим что именно мы будем называть «облачным решением». Это модель построения ИТ-инфраструктуры, при которой ресурсы, необходимые для работы бизнес-приложения, частично или полностью выносятся на сторону провайдера*. На схеме 1 показаны варианты облачных сервисов — SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service). В каждой из реализаций, области ниже пунктирной линии находятся в распоряжении и под ответственностью провайдера, за элементы выше линии несет ответственность заказчик.

Кроме того, решение может отличаться по физическому размещению ресурсов, по принадлежности прав поддержки и по тому, кто является заказчиком сервиса. Данные критерии в совокупности определяют четыре основные класса облачных решений: публичные, частные, партнерские и гибридные. На схеме 2 изображена суть этих решений.

Из-за огромного количества вариантов размещения, владения, управления, использования инфраструктуры облака, а также из-за разнообразия типов услуг (IaaS, PaaS, SaaS) универсальный способ обеспечения безопасности не представляется возможным. Это правда и неправда одновременно. Отсутствие единого рецепта действительно имеет место, но это не означает, что с задачей справиться нельзя.

С операционной точки зрения, безопасность как сервис можно представить в виде набора решений, используемых в компании, таких как IPS или программный антивирус. При выносе определенных ресурсов в облако следует соотнести их с общим набором механизмов, отвечающих за их защиту, и искать пути утверждения зон ответственности за работу механизмов защиты в SLA. В зависимости от типа сервиса (IaaS, PaaS, SaaS) количество этих механизмов будет разным. Схема 3 показывает простой способ поиска незакрытых областей в системе безопасности для различных типов сервиса. В идеале именно эти области должны закрываться провайдером или совместно при помощи существующих или созданных инструментов.

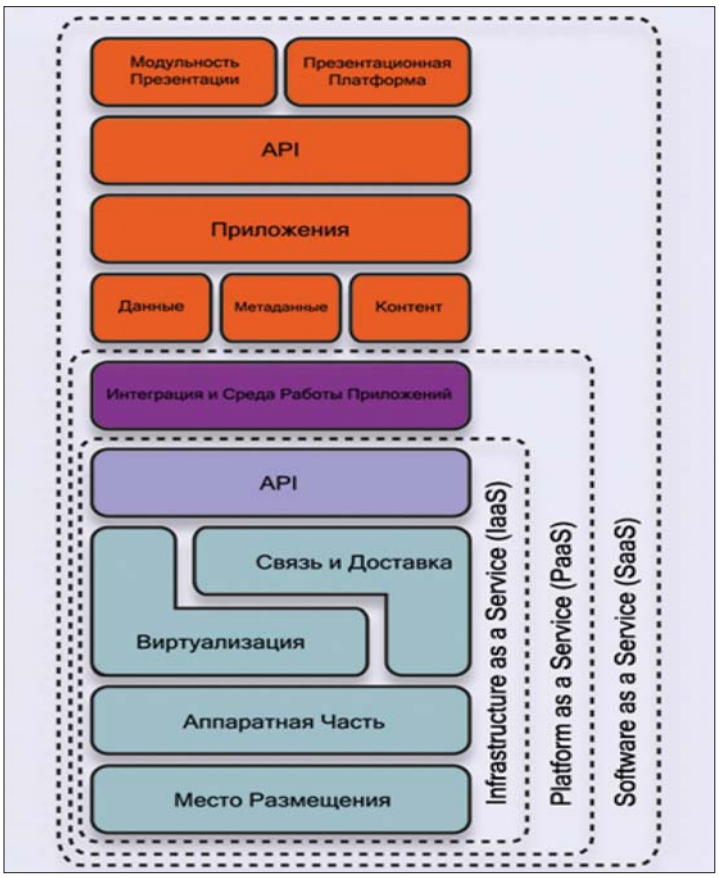


Схема 1. Эталонная модель облачных сервисов

	Инфраструктурой Управляет	Инфраструктура Принадлежит	Инфраструктура Расположена	Инфраструктурой Пользуется
Публичное	Провайдер	Провайдер	Вне организации	Не Имеет Доверия
Частное / Партнерское	Организация ИЛИ Провайдер	Организация ИЛИ Провайдер	Внутри Организации ИЛИ Вне Организации	Имеет Доверие
Гибридное	Организация и Провайдер	Организация и Провайдер	Внутри Организации и Вне Организации	Имеет Доверие / Не Имеет Доверия

Схема 2. Варианты реализации облачных услуг

Схема 3 может быть использована как общее руководство по этапам ревизии и корректировки политики безопасности. Сам же процесс содержит множество нюансов и деталей, которые тщательно и доступно изложены в руководстве от CSA (http://cloudsecurityalliance.org/csaguide.pdf). Вопросы, которым авторы документа советуют уделить внимание, условно поделены на две группы: управление и операции.

К вопросам управления относятся управление рисками, аудит, соответствие нормам, управление жизненным циклом информаци, мобильность сервиса и совместимость с инфраструктурой других вендоров. К операционным вопросам относятся обеспечение непрерывности бизнеса, возобновление бизнеса после бедствия, поддержка дата-центра, работа с инцидентами, безопасность приложений, шифрование и управление ключами, идентификация и управление доступом, виртуализация ресурсов.

Общая рекомендация носит, скорее, административный характер: расходы, необходимые на модификацию систем безопасности в связи с миграцией, должны/могут быть компенсированы за счет финансовой выгоды, полученной от миграции. Защита делегируемой инфраструктуры в том виде, в котором она была прописала в политике у заказчика, должна быть транслирована на сторону провайдера и принята провайдером как обязательная к выполнению в полном, частичном или скорректированном виде. Кроме того, заказчик должен ознакомиться с политикой провайдера и проанализировать ее на предмет адекватности и соответствия принятым в компании стандартам и нормам.

Отдел информационной безопасности заказчика обязательно должен принимать участие в формировании SLA, если это возможно. В рамках этого участия важно установить метрики и индикаторы, по которым будет производиться мониторинг качества работы систем защиты. Эти критерии должны быть оговорены и утверждены в SLA до миграции.

Очень скользким местом является такой элемент политики, как оценка рисков. Поскольку действие происходит на территории поставщика, проводить игрушечные атаки с целью выявления дыр в безопасности нельзя. Кроме того, провайдеры для реализации своих услуг часто пользуются услугами сторонних организаций. Некоторые провайдеры предоставляют альтернативные способы тестирования систем защиты, но это скорее редкие случаи, а не тенденция. В процессе созревания рынка ожидается появление большего количества провайдеров, понимающих важность этого элемента для повышения доверия со стороны заказчиков.

План восстановления бизнеса после бедствия должен обязательно включать сценарии потери сервиса от провайдера или потери провайдером сервиса от стороннего поставщика. Процесс восстановления необходимо скоординировать с провайдером и, при возможности, протестировать.

Важным является и вопрос ответственности сторон в случае аудита систем безопасности. Такой аудит может проводиться в случае инцидента нарушения целостности или конфиденциальности пользовательских данных. Разделение ответственности должно быть оговорено и утверждено в соответствии с существующим разделом прав и обязательств по применению инструментов безопасности.

*Провайдер может быть внешним (сервис-провайдер, к примеру, Amazon) или внутренним (облако обслуживает нужды различных департаментов, изолируя их рабочие среды друг от друга)

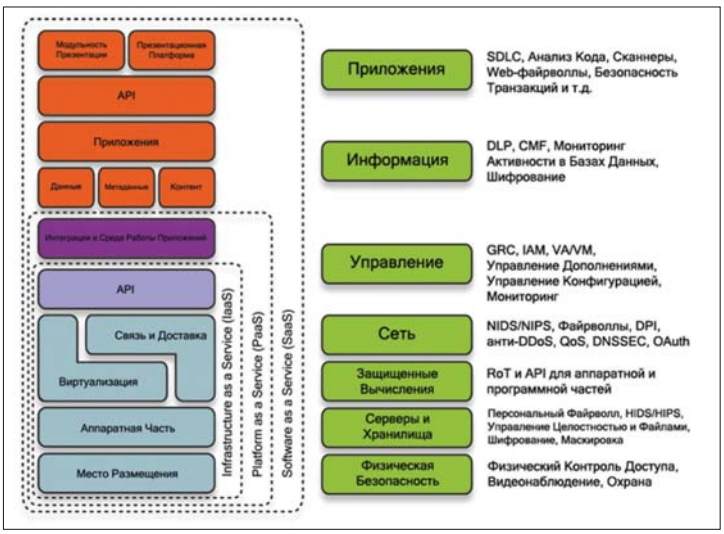


Схема 3. Поиск незакрытых областей в системе безопасности

Веб за стеной огня

АЛЕКСАНДР ХОМУТОВ,
ДИРЕКТОР «ИТ ЛЭНД»

БЕЗОПАСНОСТЬ

Интернет уже давно вошёл в нашу жизнь, и теперь мы напрямую связываем бизнес с электронной почтой, корпоративными веб-порталами, ERP- и CRM-системами. Сегодня практически каждый банк имеет систему интернет-банкинга, позволяющую пользователям работать со своим расчётным счётом из любой точки мира.

Очень часто в компаниях с территориально распределённой структурой понятие периметра сети размывается. Ресурсы, с которыми работают сотрудники и партнёры, зачастую могут находиться вне организации, и доступ к ним обычно осуществляется через веб-браузер. Корпоративное ПО нередко пишут внешние разработчики, которые не всегда уделяют должное внимание безопасности кода.

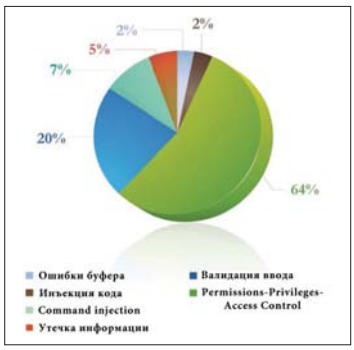


Рис. 3. Наиболее распространенные типы уязвимостей прочих веб-приложений. По данным отчета Cenzic за первое полугодие 2010 года

Согласно отчету компании Cenzic за первое полугодие 2010 года, более 90% коммерческих веб-приложений подвержены риску утечек и раскрытия информации, 80% имеют уязвимости авторизации и аутентификации, а уязвимостям в управлении сессиями и межсайтового скриптинга подвержены 68% веб-приложений. Скорее всего, в Украине этот процент ещё больше, так как зачастую мы доверяем создание приложений студентам либо программистам, которые имеют очень расплывчатые понятия о безопасности кода. Даже если приложение разрабатывалось серьезной компанией, вы всё равно не застрахованы от данных проблем.

Такие классические средства защиты, как межсетевые экраны и системы IPS, не обеспечивают нужного уровня безопасности для веб-приложений, поскольку большинство межсетевых экранов работают на 4-м уровне модели OSI, а сигнатурные базы IPS направлены на предотвращение, в первую очередь, сетевых атак. Использование приложений с технологиями Java, Flash, ActiveX и SQL-запросов, делает применение классических средств защиты малоэффективными. Наиболее распространенными типами атак на веб-приложения являются межсайтовый скриптинг (Cross Site Scripting, XSS) и внедрение SQL-кода (SQL injection), распространены также атаки типа отказ в обслуживании DoS и DDoS. Обычно основная задача атакующего — это внедрение на ресурс вредоносного ПО либо полное разрушение веб-ресурса путём уничтожения базы данных.

Для обеспечения безопасности веб-ресурсов используются специализированные межсетевые экраны — Web Application Firewall (WAF). Используя WAF совместно с системами IPS можно создать мощный рубеж защиты от многочисленных атак. Системы IPS обнаруживают на сетевом уровне такие атаки, как сканирование портов, CGI-атаки и направленные на протоколы атаки. Они сравнивают пакеты с известными сигнатурами атак и принимают решение запретить либо пропустить пакет. Однако системы IPS не имеют представления об уровне Web Application, а именно о структуре данных, запросах и кодировании (в случае SSL). Такой подход не в состоянии предотвратить множество атак либо ложных срабатываний в зависимости от настройки IPS. В отличие от IPS, система WAF понимает конструкцию данных веб-трафика и отслеживает состояние приложений и клиентских сессий.

Кроме использования WAF, необходимо систематически проверять веб-ресурсы специализированными сканерами безопасности с целью выявления таких проблем ресурса, от которых не способен защитить WAF. К их числу относятся, к примеру, слабые пароли. Для определения уязвимых мест веб-приложений и серверов служат такие продукты как Acunetix Web Security Scanner. Это решение способно, в частности, определять уязвимости SQL Injection и XSS и содержит целый набор таких утилит как сканнер диапазонов ip-адресов на открытые порты, редактор передаваемых HTTP-заголовков, сниффер (анализатор трафика). Именно использования WAF и систематическое сканирование позволит обеспечить должный уровень безопасности веб-приложений в организации.

С автором материала можно связаться по адресу: support@itland.com.ua

Рис. 1. Процент коммерческих веб-приложений, имеющих те или иные уязвимости. По данным отчета Cenzic за первое полугодие 2010 года

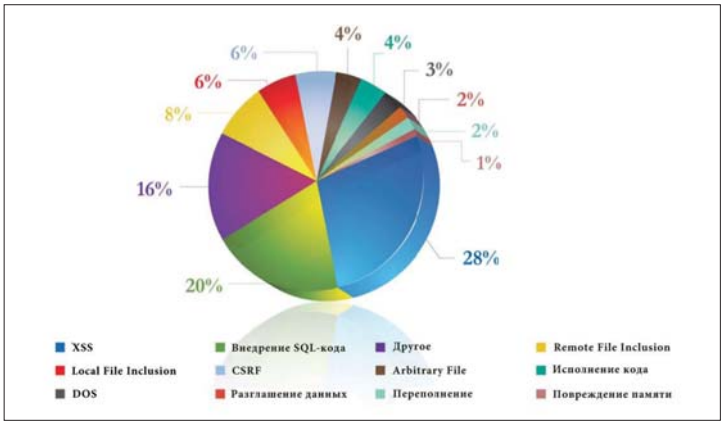
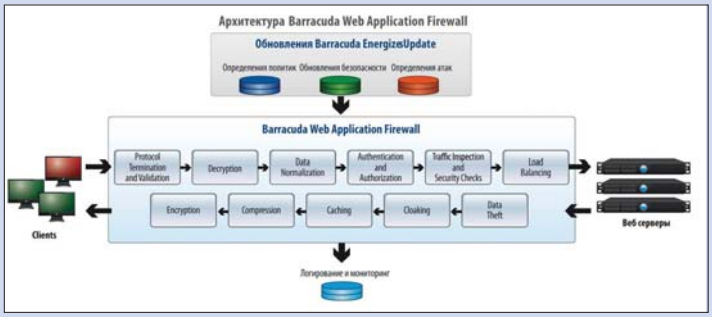


Рис. 2. Наиболее распространенные типы уязвимостей коммерческих веб-приложений. По данным отчета Cenzic за первое полугодие 2010 года

Основными разработчиками аппаратных систем WAF являются компании Barracuda Networks, Breach Security, F5 и Imperva. Эти системы поставляются в виде шлюза безопасности и могут устанавливаться в сети в режиме In-Line Mode либо Sniffer и не требуют внесения изменений в существующую инфраструктуру сети.

Одним из наиболее распространенных WAF является Barracuda Web Application Firewall от компании Barracuda Networks. Это устройство защищает веб-приложения и сервисы, а также позволяет увеличить производительность и масштабируемость приложений. Barracuda Web Application Firewall работает на 7-м уровне модели OSI и предотвращает атаки XSS, SQL-инъекции и межсайтовую подделку запросов (CSRF). Использование данных устройств позволит в безопасном режиме эксплуатировать корпоративные веб-ресурсы, а встроенная балансировка нагрузки — распределить запросы пользователей на несколько серверов. Балансировка нагрузки — важный параметр системы, особенно при отражении незначительных DDoS-атак.



Архитектура Barracuda Web Application Firewall

Таблица 1. Сравнение возможностей IPS и WAF

Возможности	IPS	WAF
Защита от межсайтового скриптинга и внедрения SQL-кода (XSS, SQL)	Ограничено	+
Защита от подделки межсайтовых запросов (CSRF)	—	+
Нормализация зашифрованного трафика	—	+
Инспекция HTTPS-трафика	—	+
Защита от перехвата сессий	—	+
Предотвращение перехода по директориям и захвата браузера	—	+
Предотвращение кражи данных и клоакинга	—	+
Защита от полного перебора	—	+
Защита веб-сервисов	—	+
Защита от загрузки вредоносного ПО и вирусов	—	+
Защита от DoS на уровне приложений	—	+
Защита ограничения скорости	—	+
Проксирование трафика	—	+
Журналирование доступа приложений и запись аудита пользователей	—	+

НОВОСТИ

В Украине стартовали продажи планшета ViewPad 10

Корпорация ViewSonic объявила о начале продаж планшетного компьютера ViewPad 10 в Украине. Профессиональный планшет ViewSonic ViewPad 10 оснащен экраном с диагональю 10,1", процессором Intel Atom N455 с тактовой частотой 1,66 ГГц, 1 ГБ оперативной памяти и встроенным твердотельным накопителем емкостью 16 ГБ. Дисковое пространство можно расширить благодаря наличию кард-ридера Micro SD и двух портов USB 2.0. Сенсорный емкостный экран с разрешением 1024x600, яркостью 220 кд/м2 и контрастностью 700:1 отлично подходит как для работы, так и для развлечений — игр и просмотра видео, также ViewPad 10 можно подключить к внешнему монитору или телевизору благодаря наличию порта mini VGA.

Использование аппаратной платформы Intel Atom позволяет ему работать под управлением как Google Android 1.6, так и Microsoft Windows 7 Home Premium. Кроме того, возможна установка еще одной мобильной ОС — MeeGo.

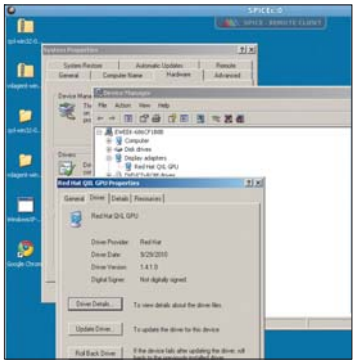
FEDORA 14 С ОБНОВЛЁННЫМИ ИНСТРУМЕНТАМИ РАЗРАБОТЧИКА

ДЖЕЙСОН БРУКС

Вышел новейший релиз Fedora 14, быстро развиваемого силами сообщества программистов варианта дистрибутива Red Hat Linux. Как обычно, он включает набор обновленных приложений с открытым исходным кодом. Особый акцент сделан на получивших дальнейшее развитие инструментах разработчика, таких как новейшие версии интегрированных сред разработки Eclipse и NetBeans. Что касается новых функций, то в Fedora 14 их немного, особенно если сравнивать с последней версией главного конкурента Fedora — Ubuntu.

ОБЗОРЫ

Больше всего привлекло мое внимание в Fedora 14 добавление программных пакетов для поддержки протокола



Протокол удаленного доступа к рабочему столу Red Hat Spice наконец-то реализован в Fedora, хотя и с некоторыми ограничениями

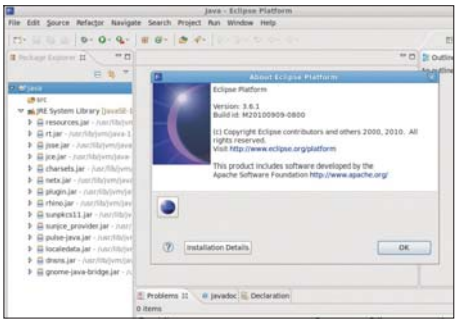
удаленного доступа к рабочему столу Spice. Red Hat приобрела его, поглотив в 2008 году компанию Qumranet, разработавшую для нее гипервизор KVM. Хотя KVM был довольно быстро включен в дистрибутивы Red Hat и других разработчиков Linux, создание протокола Spice оказалось более сложным делом. В значительной мере это было связано с тем, что появился он сначала в виде патентованной технологии.

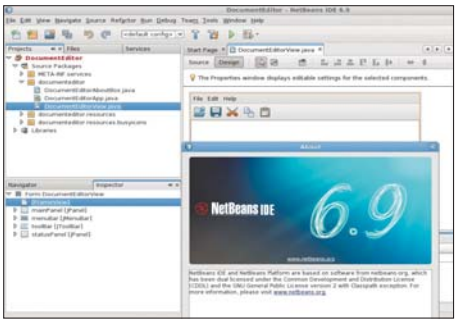
Даже сейчас Spice (а он обещает повышенную производительность по сравнению с обычно используемым в Linux для дистанционного доступа к рабочему столу протоколом VNC) еще не интегрирован с инструментами управления виртуализацией, которые поставляются в составе Fedora. И это до сих пор прочно удерживает данную функцию в категории «ознакомительная версия» (tech preview).

У пользователей, хорошо разбирающихся в Linux и сделавших ставку на продукты Red Hat, Fedora 14 успешно справится с любой из многочисленных ролей, которые играет Linux. Однако в общем и целом Fedora 14 больше всего подойдет для рабочей станции программиста, сервера общего назначения или ознакомления с компонентами, которые вскоре появятся в составе Red Hat Enterprise Linux и ее клонах.

Сравнительно короткий жизненный цикл версий Fedora означает, что примерно раз в год эти системы требуют апгрейда. Поэтому предварительным условием использования данного дистрибутива является заинтересованность в том, чтобы всегда быть на переднем крае. Или хотя бы готовность к этому.

Версии Fedora 14 для платформ x86 и x86-64 можно бесплатно загрузить по адресу: http://fedoraproject.org/get-fedora. Обе они доступны в виде LiveCD (что позволяет провести тестирование, ничего не меняя на жестком диске вашего компьютера), а также в виде образов DVD-дисков (они содержат все доступные пакеты ПО Fedora) и образов для установки через сеть (их объем составляет менее 300 Мб).





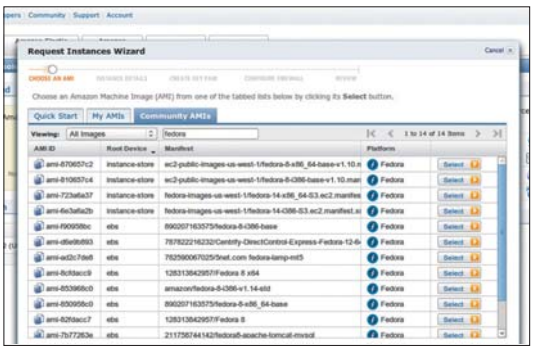
Fedora 14 усовершенствована поддержка Amazon Elastic Compute Cloud. Предыдущим «официальным» релизом с поддержкой EC2 был устаревший Fedora 8

Инсталляция Fedora

Я устанавливал экземпляры Fedora с использованием всех трех типов носителей. На меня действительно произвело большое впечатление (особенно это относится к образу для сетевой установки) то, как славно потрудились Red Hat и команда разработчиков Fedora, чтобы упростить процесс конфигурирования сетевого интерфейса, подключения к инсталляционному репозиторию и начала установки. Работая с другими дистрибутивами и прежними версиями Fedora, мы привыкли к тому, что при сетевой установке приходится сталкиваться с гораздо большими трудностями.

Относительно развертывания следует также сказать, что Fedora 14 является первым релизом данного дистрибутива, который через некоторое время можно будет легко установить в облаке Amazon EC2. Я воспользовался своей учетной записью в Amazon AWS, поискал Fedora в хранилище образов и нашел образы x86 и x86-64 для Fedora 14 и Fedora 8 — предыдущей версии, которой было уделено такое внимание со стороны EC2.

Не то чтобы пользователи не имели прежде возможности создавать свои собственные образы для EC2. Но перейти от инсталляции к созданию образа EC2 не столь просто, как установить ОС на какой-нибудь платформе виртуализации вроде VMware. Поиск в интернете сочетания «Fedora EC2» выдал на удивление много ссылок на сообщения пользователей, мучившихся со старой, уже не поддерживаемой версией Fedora.



В составе Fedora 14 поставляются новейшие версии популярных интегрированных сред разработки NetBeans и Eclipse

Если говорить о виртуализации (и о мучениях), то при тестировании протокола дистанционного доступа к рабочему столу Spice, который входит в состав Fedora 14, мне пришлось преодолеть больше трудностей, чем хотелось бы. Это было связано с тем, что протокол находится на ранней стадии интеграции в дистрибутив. Я начал тестирование данной новой функции с установки 64-разрядной версии Fedora 14 на сервере в нашей лаборатории (серверный компонент Spice не работает на 32-разрядных системах) и создания пары образов гостевых систем, одного под управлением Windows XP, а другого — Fedora 14.

Я воспользовался стандартными инструментами Fedora virtmanager для создания этих экземпляров, а на виртуальной машине под управлением Windows XP также для загрузки и инсталляции графического драйвера qxl, который необходим на клиентской системе для использования Spice. Затем я выключил свои гостевые экземпляры и вновь запустил их в обход стандартных инструментов с помощью механизма эмуляции и виртуализации qemu. Данный механизм используется всеми инструментами виртуализации Red Hat. Он запускается из командной строки с соответствующими аргументами для Spice. После этого я подключился к обоим экземплярам через сеть с помощью отдельного клиента Fedora и отметил, что качество звука улучшилось, а время отклика сократилось.

Однако за всеми этими хлопотами я совершенно упустил из виду сетевой доступ для моих гостевых экземпляров, поскольку у меня возникли трудности с воспроизведением массы аргументов командной строки, от которых абстрагируются инструменты виртуализации Fedora. Я намерен продолжить тестирование Spice и надеюсь, что в ближайшие месяцы эта технология войдет и в другие дистрибутивы Linux.

Хрестоматийный...

◀ ПРОДОЛЖЕНИЕ СО С. 10

Серверы и СХД

В основе аппаратного комплекса лежит работающий под управлением ОС IBM AIX 48-процессорный сервер IBM Power System 770 и СХД IBM System Storage DS5300. Он представляет собой отказоустойчивое решение с полным дублированием сервисов и оборудования на удаленных друг от друга на несколько километров площадках (в качестве резерва пока используется Power System 570, в текущем году его планируют заменить на 770-ю модель). Объем оперативной памяти Power System 770 составляет 512 ГБ, из которых заказчик пока активировал 256 ГБ. Это первый и на данный момент крупнейший в Украине проект с использованием серверов IBM на базе процессоров Power 7 — в «Инкоме» их считают лучшими в отрасли с точки зрения скорости возврата инвестиций (ROI). Часть серверной инфраструктуры составляют лезвия IBM BladeCenter E-серии на одно- и двухпроцессорных платформах Intel Xeon с объемом памяти до 8 ГБ и широко распространенные 2U-серверы HP ProLiant DL380 под управлением ОС Red Hat Enterprise Linux.

ПО

Безусловно, поставленные в рамках проекта серверные системы способны обрабатывать и анализировать огромные объемы данных в режиме реального времени. На них возложена задача обслуживания центральной СУБД Oracle на 1 200 пользователей, терминалов (используется ПО Citrix Systems) и файлового доступа. В качестве автоматизированной банковской системы (АБС) в «Кредобанке» используется Б2 харьковской компании CS. Программно-аппаратный комплекс реализован с применением технологий Oracle Data Guard и Power VM, для управлением базами данных АБС применяется Oracle Grid Control. Система резервного копирования построена на ПО IBM Tivoli Storage Manager.

Безопасность

В помещения ЦОД внедрена система управления доступом. Отдельно стоит сказать про платформу Nexus 7000 — она первая в продуктовой линейке Cisco поддерживает объявленную в конце 2007 года архитектуру Trusted Security, которая интегрирует функции идентификации и учета роли пользователя в ЦОД. Она обеспечивает доверенную сегментацию трафика без сложных моделей адресации и неуправляемых списков контроля доступа (ACL), в результате чего появляется возможность переноса в рамках ЦОД виртуальных машин без ущерба для целостности данных (с использованием технологии шифрования AES-128 на каждом порту Nexus 7000).

Резервирование компонентов

По системам кондиционирования — N+1, энергообеспечения и телекоммуникаций — 2N.

Сервисная поддержка

Важным этапом в достижении поставленных целей стало обучение ИТ-персонала банка для самостоятельной поддержки вычислительных подсистем ЦОД, в частности, RISC-серверов IBM. Вместе с тем, г-н Гентош не исключает подписания сервисного договора с компанией «Инком» на обслуживание наиболее критичных для обеспечения непрерывности бизнеса узлов. Сервисные договора по кондиционерам уже заключены.

Киев — Львов — Киев

MIROHOST

www.mirohost.net

imena.ua

регистратор доменных имен

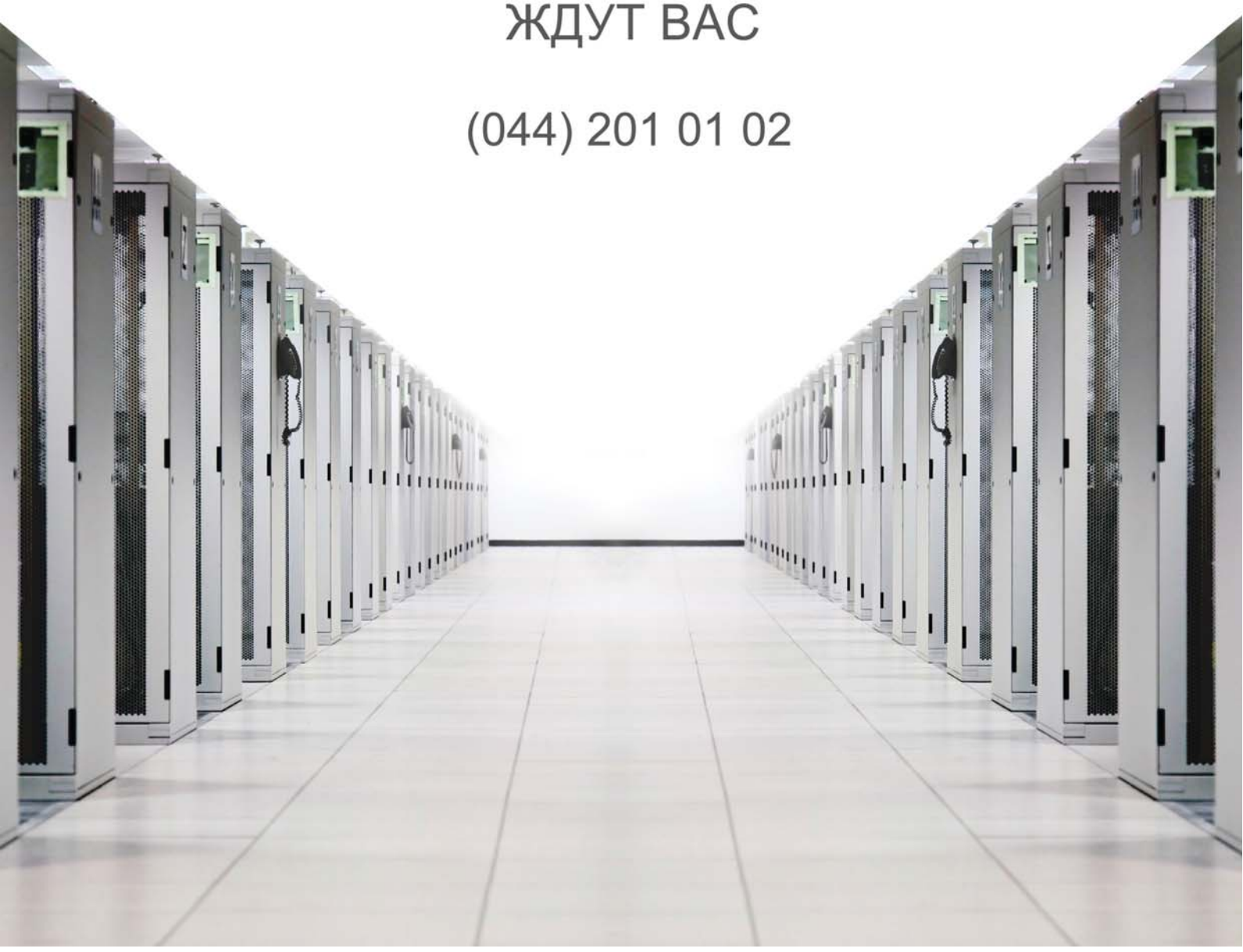
www.imena.ua

ДАТА ЦЕНТР

10 000 серверов

ЖДУТ ВАС

(044) 201 01 02



ОБЛАКА ДЛЯ МАЛОГО БИЗНЕСА

ИНТЕРВЬЮ

Компания Parallels является одним из родоначальников современного рынка виртуализации и, что еще важнее, продолжает оставаться одним из ведущих игроков виртуализационно-облачного направления наряду с мировыми ИТ-лидерами, опираясь на собственные оригинальные технологии. В сентябре 2010-го пост президента компании занял известный ИТ-менеджер Биргер Стен. О перспективах развития технологий и компании с новым CEO Parallels побеседовал обозреватель PCWeek Андрей Колесов.*

PCWeek: До вступления в должность президента Parallels Вы работали в Microsoft – расскажите об этом опыте.

БИРГЕР СТЕН: Летом 2009 года я переехал в корпоративный кампус Microsoft в Редмонде (США), где вступил в должность вице-президента компании по работе по всему миру с компаниями-партнерами категории малого и среднего бизнеса (СМБ), к которым относятся предприятия численностью до 500 человек. Это интересный сегмент бизнеса Microsoft. Здесь продажи идут через двухзвенный канал, дистрибуторов и реселлеров. Надо сказать, что в целом Microsoft старается перевести поставки своих продуктов в некоторый облачно-онлайновый вариант, но как раз в случае СМБ не очень понятно, как это нужно делать. Тут трудно что-то точно смоделировать заранее, во многом поиск новых форм ведется методом проб и ошибок. А с другой стороны, легко себе представить ответственность задачи, если вспомнить, что у корпорации ежемесячно более 100 тыс. реселлеров продают лицензии различного ПО Microsoft.

Должен сказать, что Microsoft очень хорошо понимает потребности заказчиков и имеет четкую стратегию развития всей своей программной системы в направлении облачных моделей. Мне кажется, что пример Office 365 это полностью подтверждает. И клиенты в целом готовы воспринимать подобные инновации. А вот партнерский канал, мне кажется, в этом процессе движения в сторону облаков несколько отстает, не успевает адаптироваться к новым условиям.

В целом работа в Редмонде была для меня очень интересной и полезной. Я получил опыт работы хотя и в специализированном направлении, но в глобальном масштабе всей корпорации.

PCWeek: Как же вы пришли в Parallels?

Б.С.: Я хорошо знал компанию давно. Мы ближе познакомились с главой Parallels Сергеем Белоусовым в начале 2007 года, и уже тогда обсуждали в самых общих чертах возможности ведения бизнеса в новых технологических условиях с использованием интернета (в то время еще даже термина Cloud не было). Задачи, которыми я занимался в штаб-квартире Microsoft, также довольно созвучны с проблемами, стоящими перед Parallels, которой нужно выстраивать партнерскую систему. Раньше компания работала в основном напрямую с хостинг-провайдерами, причем преимущественно из сферы Web-хостинга. Теперь же спектр канала и состав поставляемых им услуг существенно расширяется.

PCWeek: Как вы позиционируете положение Parallels в современном виртуализационно-облачном ИТ-мире?

Б.С.: До недавнего времени Parallels была известна своими технологиями виртуализации. Но представление о компании исключительно как о разработчике средств виртуализации было изначально неверным. Parallels фактически с самого начала своей деятельности делала акцент на комплексное решение задачи создания эффективного сервис-провайдинга в интересах малого и среднего бизнеса. А уже выполнение этой задачи подразумевает использование средств виртуализации серверов, гибкого управления виртуализированными дата-центрами и автоматизации управления услугами для заказчиков. Нетрудно заметить, что эти три компонента — виртуализация, управление ИТ-инфраструктурой и управление услугами (заказ, поддержка, биллинг) — ключевые элементы облачных вычислений.

Я говорю это к тому, что Parallels фактически уже очень давно занимается всем комплексом вопросов облаков для малого бизнеса, но только раньше все фокусировалось на Web-хостинге. Теперь же задача заключается в том, чтобы этот опыт трансформировать на более широкий спектр облачных задач. При этом я хочу подчеркнуть, что конкурентное преимущество Parallels заключается как раз в том, что в отличие от других облачных игроков компания имеет полный набор средств, в том числе пакет Parallels Automation для провайдеров, и реальный опыт в данной сфере.

Но конкурентные возможности еще нужно реализовать, и тут нам предстоит весьма серьезная работа, которая, впрочем, уже начата. Речь идет о том, чтобы помочь хостерам трансформировать и расширить свое поле деятельности и привлечь к сотрудничеству новые категории партнеров.

Кто-то из таких компаний будет предлагать хостинг инфраструктуры, кто-то заниматься перепродажей приложений вендоров в режиме SaaS. Но обратите внимание, что во втором случае речь идет не о традиционных реселлерах, а о продавцах нового типа, которые выполняют не разовые продажи, а работают в постоянном и долгосрочном взаимодействии с клиентами в режиме аренды. Это более сложный бизнес, которому как раз и должны помочь наши решения автоматизации и виртуализации.

PCWeek: Но все же базовой технологией для реализации облаков является виртуализация, и наблюдается серьезная конкуренция, в том числе на уровне стандартов виртуальных машин. Что предлагает Parallels в этой сфере?

Б.С.: Компания еще несколько лет назад, кажется, первой на ИТ-рынке, стала предлагать вариант распространения приложений в виртуальном формате APS (Application Package Standard). С его помощью независимые разработчики «упаковывают» свои приложения для дистрибуции через хостеров и сервис-провайдеров, а те, в свою очередь, получают дополнительные услуги для продажи своим абонентам. Сегодня в нашем каталоге имеется очень большое число APS-совместимых приложений, в том числе корпорации Microsoft.

PCWeek: Какие еще кроме хостеров компании являются вашими потенциальными партнерами?

Б.С.: Очень успешно развивается сотрудничество с телекоммуникационной отраслью. Кроме того, очень важной категорией являются сегодняшние дистрибуторы и крупные реселлеры ПО. Если опять вернуться к конкурентной ситуации, то сегодня почти все основные игроки облачного рынка ориентируются на крупных корпоративных заказчиков. Малый и средний бизнес находится вне поля их зрения, в том числе и потому, что работа на массовом рынке требует наличия средств автоматизации управления услугами. А Parallels давно имеет необходимые решения и может эффективно помогать провайдерам работать в сегменте SMB.

Вот смотрите: у той же Microsoft есть онлайновый набор бизнес-решений BPOS, а в следующем году ему на смену придет Office 365. Эти сервисы могут продавать и независимые облачные поставщики. Причем это могут делать как

Биргер Стен

реселлеры, которые будут предлагать потребителям сервисы самой Microsoft, так и хостеры, которые развернут данные решения на своих площадках. Но в любом случае им понадобятся средства управления услугами и ИТ-процессами. И они у нас уже имеются на базе Parallels Automation, в том числе в варианте для BPOS и Office 365. С помощью наших готовых инструментов облачные поставщики смогут развернуть и начать продавать соответствующие услуги в течение двух-трех месяцев.

PCWeek: Parallels, тогда еще под названием SWsoft, сделала первую попытку расширения своего присутствия на рынке еще в 2003–2005 гг., намереваясь выйти за рамки Web-хостинга и занять определенную долю на рынке корпоративных клиентов. Но, кажется, освоение корпоративного сегмента давалось компании довольно тяжело. Каковы ваши планы сейчас в отношении конечных пользователей?

Б.С.: Да, широкого выхода на корпоративный сегмент у Parallels тогда не получилось, хотя определенные успехи, конечно, были. Но надо сказать, что продвижение виртуализации в этот круг клиентов был весьма непростым и для VMware, и для Microsoft. Ведь поначалу виртуализация применялась предприятиями для решения каких-то частных задач, например для разработки и тестирования ПО. А средства Parallels ориентировались на продуктивное использование, работу с реальными бизнес-приложениями, причем на достаточно большом числе виртуальных машин. Второй момент заключался в том, что технология контейнеров Parallels Virtuozzo Containers ориентирована на высокопроизводительную работу в однородных операционных средах, а в корпоративном секторе наблюдается сильная гетерогенность ОС, тут гипервизоры лучше подходят.

Понимаете, Parallels Virtuozzo Containers была изначально ориентирована на применение в полностью или в значительной степени виртуализированных дата-центрах. А таких ЦОДов в корпоративном секторе почти не было. Такую инфраструктуру под названием «частные» или «внутренние облака» предприятия только сейчас начинают формировать. При этом нужно отметить, что есть вертикальные направления, где нужны высокопроизводительные вычисления, и здесь Parallels Virtuozzo Containers — наиболее оптимальный вариант. Это и разнообразные задачи математического моделирования, и обработка изображений, и создание мультипликации, и многое другое. Это все специализированные, узкие, но довольно глубокие клиентские сегменты.

PCWeek: Но ведь кроме контейнеров в арсенале Parallels еще пару лет назад появились и гипервизоры, в том числе и способный работать на «голом железе». Как идет их продвижение?

Б.С.: Продвижение нашего гипервизора находится, наверное, еще в начальной фазе. В этом сегменте уже сложилась высокая конкуренция, но мы рассчитываем на рыночный успех нашего комбинированного решения Parallels Server Bare Metal, которое включает технологии и контейнеров, и гипервизоров. Оно уже пользуется успехом у хостеров, которые благодаря ему могут обеспечивать эффективность использования вычислительных ресурсов и гибкость применения для различных ОС и приложений.

PCWeek: Parallels при слиянии с SWsoft принесла не только название объединенной компании, но и продукты виртуализации клиентских компьютеров. Как развивается это направление бизнеса?

Б.С.: Очень хорошо, на него приходится около 40% бизнеса Parallels. Тут основной наш продукт Parallels Desktop для Mac — это решение, которое позволяет одновременно работать с Windows-приложениями на компьютерах Mac. Популярность этих систем растет. Еще недавно считалось, что ими пользуются только фанаты Apple, но сейчас их все чаще можно увидеть и у обычных пользователей. Более того, видно заметное проникновение Mac в корпоративную среду, и тут наш Parallels Desktop просто незаменим. Ведь в компаниях применяют много разных Windows-приложений, и надо обеспечить их работоспособность и на компьютерах Apple. Это нужно и в домашнем применении, поскольку во многих семьях сейчас имеется уже не один компьютер, причем разных архитектур.

Должен сказать, что рынок Mac'ов растет, но продажи наших виртуализационных продуктов для них увеличиваются еще быстрее. Наше решение для Apple является самым популярным в мире ПО, созданным третьей стороной.

НОВОСТИ

Gartner: рынок серверов вернулся к росту

Компания Gartner подвела окончательные итоги 4-го квартала и 2010 г. в целом на мировом рынке серверов. В последнем квартале года поставки увеличились относительно Q4'2009 на 6.5%, в деньгах рынок вырос на 16.4%.

В 4-м квартале сильно выросла выручка IBM от продаж систем на платформе System Z — на 68.3%. В результате в последнем квартале прошедшего года выручка IBM увеличилась на 2.8% и компания вышла на первую позицию, заняв 35.5% мирового рынка серверов в денежном выражении. Кроме System Z успехом пользовались и модели линейки IBM System X. В топ-5 двузначные цифры роста выручки кроме IBM продемонстрировали также Hewlett-Packard (HP) и Dell, а у Oracle и Fujitsu объем продаж в Q4'2010 сократился.

По поставкам в штуках лидерство в этот период сохранила HP, в годовом измерении она увеличила отгрузки на 6.9%. Компания увеличила поставки x86-серверов на 7.1%, выручив за них на 20.0% больше, чем в тот же период в 2009 г.

Наиболее высокими темпами в Q4'2010 продажи серверов росли в Северной Америке (на 24.5%), в Азиатско-Тихоокеанском регионе (на 22.4%) и в Латинской Америке (на 12.3%). Регион EMEA показал рост на 10.4%, в Японии отмечен спад на 4.4%.

ПОТРАТИВ ВСЕГО 5 МИНУТ НА ЗАПОЛНЕНИЕ АНКЕТЫ, ВЫ БУДЕТЕ БЕСПЛАТНО ПОЛУЧАТЬ PC Week/UE В ТЕЧЕНИЕ 6 МЕСЯЦЕВ

PCWEEK UKRAINIAN EDITION

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 **50 компьютеров**, дает **право на бесплатную подписку** на газету PC Week/UE в течение полугода с момента получения анкеты. Пожалуйста, будьте внимательны при заполнении анкеты!

Примечание. На домашний адрес PC Week/UE по бесплатной корпоративной подписке не высылается. Данная форма подписки распространяется на территорию Украины.

Вы можете получить анкету в электронном виде, пишите на адрес: anketa@skukraine.com

Название организации: _____

Почтовый адрес организации: _____

Индекс: _____ Область: _____
Город: _____
Улица: _____ Дом _____
Фамилия, имя, отчество: _____
_____
Подразделение/отдел: _____
Должность: _____
Телефон: _____ Факс: _____
E-mail: _____ WWW: _____

Правила заполнения анкеты:
1. Записать полные данные по Вашему предприятию.
2. Поставить «1» напротив выбранной Вами информации

1. К какой отрасли относится Ваше предприятие?

1. Энергетика ☐
2. Связь и телекоммуникации
3. Производство, не связанное с вычислительной техникой (добывающие и перерабатывающие отрасли, тяжелая индустрия, 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-издательская 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. Сборка и производство аппаратного обеспечения ☐
5. Продажа компьютеров ☐
6. Ремонт компьютерного оборудования ☐
7. Разработка и продажа ПО ☐
8. Консалтинг ☐
9. Иное (что именно) _____

3. Форма собственности Вашей организации (только один пункт)

1. Госпредприятие ☐
2. ОАО (открытое акционерное общество) ☐
3. ЗАО (закрытое акционерное общество) ☐
4. Зарубежная фирма ☐
5. СП (совместное предприятие) ☐
6. ЧП (частное предприятие) ☐
7. Иное (что именно) _____

4. К какой категории относится подразделение, в котором Вы работаете? (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 (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. Windows 9x/ME/2K/XP/Vista ☐
2. Windows Server 2K/2003/2008/Small Business/Essential Business ☐
3. OS/2 ☐
4. MacOS ☐
5. AIX ☐
6. Solaris/SunOS ☐
7. OS/400 ☐
8. HP/UX ☐
9. Novell ☐
10. FreeBSD ☐
11. Linux (какой именно дистрибутив) ☐
12. Другие UNIX-подобные ОС (какие именно) ☐
13. Иное (что именно) _____

10. Коммуникационные возможности компьютеров Вашей организации

1. Объединены в ЛВС ☐
2. Имеют распределенные ресурсы ☐
3. Имеют выход в Интернет (каким способом) ☐
4. Объединены с ЛВС в других филиалах/офисах ☐
5. Организована мультисервисная сеть (аудио/видео/данные) ☐
6. Не объеденины между собой ☐

11. Сетевое оборудование каких производителей используется в Вашей организации?

1. 3Com ☐
2. Alcatel-Lucent ☐
3. Allied Telesis ☐
4. ASUS ☐
5. Avaya ☐
6. Cisco Systems ☐
7. D-Link ☐
8. Ericsson ☐
9. Huawei ☐
10. Edimax ☐
11. Enterasys ☐
12. Linksys ☐
13. NetGear ☐
14. Nortel ☐
15. ProCurve (HP) ☐
16. TrendNet ☐
17. ZyXEL ☐
18. Другое (что именно) _____ ☐
19. Не установлено никакое ☐

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

1. Да ☐ 2. Нет ☐

13. Собирается ли Ваше предприятие устанавливать мультисервисную сеть в ближайший год?

1. Да ☐ 2. Нет ☐

14. Сколько серверов в сети Вашей организации?

15. Если в Вашей организации используются серверы класса Enterprise, то на базе какой архитектуры?

1. RISC-архитектура (какие именно процессоры) ☐
2. Itanium-архитектура (какие именно процессоры) ☐
3. x86-архитектура (какие именно процессоры) ☐
4. Иное (что именно) _____
5. Не используются ☐

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

	Настольные ПК	Портативные ПК	Серверы
Diawest	☐	☐	☐
Everest	☐	☐	☐
K-Trade	☐	☐	☐
Prime	☐	☐	☐
АМИ	☐	☐	☐
Навигатор	☐	☐	☐
Спецвузавтоматика	☐	☐	☐
Техника для бизнеса	☐	☐	☐
Acer	☐	☐	☐
Apple	☐	☐	☐
Asus	☐	☐	☐
Dell	☐	☐	☐
Fujitsu	☐	☐	☐
Hewlett-Packard	☐	☐	☐
IBM	☐	☐	☐
Lenovo	☐	☐	☐
Oracle/Sun	☐	☐	☐
Samsung	☐	☐	☐
Sony	☐	☐	☐
Toshiba	☐	☐	☐

Иное (что именно) _____

17. 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. Клиенты электронной почты ☐
10. САПР ☐
11. Браузеры Internet ☐
12. Web-серверы ☐
13. Системы управления ресурсами предприятия (ERP-системы) ☐
14. Системы управления отношениями с клиентами (CRM-системы) ☐
15. Системы бизнес-аналитики (BI-системы) ☐
16. Иное (что именно) _____

18. Если в Вашей организации используются бизнес-приложения (ERP-, CRM-, BI-системы и ПО для автоматизации бюджетирования), то каких фирм-разработчиков?

1. 1С ☐
2. Галактика ☐
3. Парус ☐
4. HansaWorld ☐
5. IBM (Cognos) ☐
6. Microsoft ☐
7. Naumen ☐
8. Novell ☐
9. Oracle ☐
10. SAP ☐
11. Terrasoft ☐
12. Другое (что именно) _____
13. Не установлено никакое ☐

19. Если в Вашей организации используются ПО для обеспечения безопасности, то каких фирм-разработчиков?

1. Доктор Веб ☐
2. Лаборатория Касперского ☐
3. CA (Computer Associates) ☐
4. Check Point ☐
5. Cisco Systems ☐
6. McAfee ☐
7. Novell ☐
8. Symantec ☐
9. Trend Micro ☐
10. Другое (что именно) _____
11. Не установлено никакое ☐

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

1. Да ☐ 2. Нет ☐

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

1. Да ☐ 2. Нет ☐

22. 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. MySQL ☐
11. Oracle ☐
12. Postgress ☐
13. Sybase ☐
14. Не используем ☐
15. Иное (что именно): ☐

23. Как Вы оцениваете свое влияние на решение о покупке средств информационных технологий для своей организации? (отметьте 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) _____

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

Системы
1. Серверы ☐
2. Рабочие станции ☐
3. ПК/автоматизированные рабочие места ☐
4. Тонкие клиенты/сетевые компьютеры ☐
5. Ноутбуки ☐
6. Карманные ПК ☐

Сети
7. Активное сетевое оборудование ☐
8. Пассивное сетевое оборудование ☐
9. Компоненты беспроводных сетей ☐
10. Компоненты глобальных сетей ☐

Периферийное оборудование
11. Принтеры/МФУ ☐
12. Мониторы ☐
13. ИБП (UPS) ☐

Память
14. Различные накопители ☐
15. Системы архивирования ☐
16. SAN-компоненты ☐

Программное обеспечение
17. Электронная почта ☐
18. СУБД ☐
19. Сетевое ПО ☐
20. Электронная коммерция ☐
21. ПО для Web-дизайна ☐
22. ПО для Интернета ☐
23. Java ПО ☐
34. Операционные системы ☐
25. Мультимедийные приложения ☐
26. Средства разработки программ ☐
27. CASE-системы ☐
28. САПР (CAD/CAM) ☐
29. Системы управления проектами ☐
30. ПО для архивирования ☐
31. Бизнес-приложения (ERP-, CRM-, BI-системы) ☐

Внешние сервисы
32. ☐

Ничего из вышеперечисленного
33. ☐

25. 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) _____

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

1. Укртелеком ☐
2. Астелит (Life) ☐
3. Datagroup ☐
4. Киевстар/Beeline ☐
5. MTS ☐
6. Vega ☐
7. Lucky Net ☐
8. Intellecom ☐
9. UNTC ☐
10. Украинская Мультисервисная Сеть (ТелеХаус) ☐
11. Релком ☐
12. Українські новітні технології (Freshtel) ☐
13. PEOPLEnet ☐
14. ColoCall ☐
15. Mirolink.net ☐
16. Воля ☐
17. Через других (каких именно): ☐

27. Из каких источников Вы узнали о газете?

Дата заполнения_____

Заполненную анкету пришлите по адресу:

04052, Украина, Киев, ул. Гоголевская, 49, офис 30

BARRACUDA NETWORKS

SECURITY • NETWORKING • STORAGE

Бюджетное решение по защите сети.

Более 85,000 организаций по всему миру доверяют Barracuda Networks. Решения функциональны и удобны в использовании, обеспечат надежную защиту Вашему бизнесу.

ГАРАНТИЯ 5 ЛЕТ

НЕ ЗАВИСИТ ОТ КОЛИЧЕСТВА ПОЛЬЗОВАТЕЛЕЙ

РУССКОЯЗЫЧНЫЙ ИНТЕРФЕЙС

Barracuda Spam & Virus Firewall

Скажи стоп вирусам и спаму. Шлюзовое решение по защите электронной почты. Позволит увеличить производительность почтового сервера.

Barracuda Web Filter

Фильтрация Web-контента, блокировка вредоносных программ. Позволит увеличить производительность труда.

Barracuda IM Firewall

Контроль IM сообщений. Решение для архивирования, фильтрации исходящего контента. Гибкое управление политиками безопасностями.

Barracuda Web Application Firewall

Избегайте простоя. Защита корпоративных web-серверов и web-приложений от атак злоумышленников

IT LAND ООО "ИТ Лэнд" | www.itland.com.ua