

чи данных через защищенные каналы в «облако» и механизмов обеспечения ответственности сервис-провайдера. В третьих, отсутствует необходимая «критическая масса» позитивного общественного мнения, подтверждающего техническую и финансовую эффективность данного решения.

## Безопасность виртуальной инфраструктуры

Третья необычная задача, практически не решавшаяся ранее, — обеспечение безопасности вирту-

альной инфраструктуры. Среди списков воздействий, представляющих угрозу для виртуальных сред, значатся, например, атаки на гипервизор и на виртуальные машины с других виртуальных машин и из физической сети, неконтролируемый рост числа виртуалок, атаки на средства администрирования виртуальной инфраструктуры. Для противодействия таким специфическим угрозам существуют два типа решений.

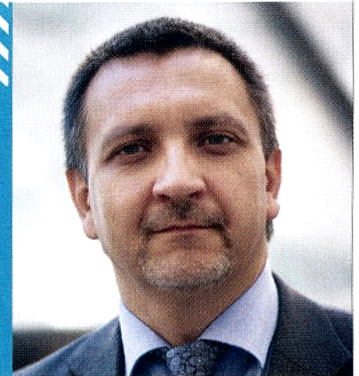
Первое — это адаптация существовавших ранее средств защиты для применения в виртуальных средах. Как таковую безопасность виртуализации они не обеспечивают, но по-

зволяют снизить затраты на эксплуатацию средств защиты. Как правило, они легко узнаваемы по приставке Virtual Appliance.

Второй тип решений занимается снижением угроз с помощью контроля на уровне гипервизора и усилением безопасности непосредственно виртуальных машин. В их функционал, как правило, входят защита от вторжений (IDP), антивирусные решения, межсетевое экранирование и контроль политик безопасности в виртуальной среде. Монополии на данном рынке средств защиты нет — их разрабатывают несколько компаний (CheckPoint, TrendMicro, «Код Безопасности» и т.д.). ●

## Рустэм Хайретдинов:

заместитель генерального директора InfoWatch



# Мы сохраняем лидерство на российском рынке, диверсифицируем линейку продуктов и начинаем активную экспансию на Ближний Восток и в Европу

— Как вы оцениваете темпы становления российского рынка ИТ, в частности сегмента информационной безопасности, по итогам 2010 года?

— Прошлый год стал годом «отложенного спроса» — заказчики, отложившие приобретения в 2009 году из-за кризиса, разморозили бюджеты в 2010-м. Мы, например, выросли на 130%, причем более 60% этого роста обеспечили именно новые клиенты — заказчики вернулись покупать наш продукт. В 2011 году подобного взрывного роста ожидать не стоит. Мы, к примеру, нацелены на сохранение текущих лидерских позиций со средними показателями роста в пределах 20–30%.

— Какие основные тенденции сложились на рынке информационной безопасности и, в частности, в сегменте DLP к настоящему времени?

— Рынок DLP растет не так быстро — ведь это довольно специфический сегмент ИБ. Хотя он, по сути, — первая настоящая система именно информационной безопасности: ведь

все остальное сегодня защищает не информацию, а элементы ИТ-инфраструктуры (сервера, каналы и пр.).

— Расскажите, пожалуйста, о наиболее интересных ИТ-проектах, реализованных вашей компанией в 2010 году.

— Мы завершили очень серьезный проект по защите информации в Федеральной таможенной службе, а также несколько проектов в структурах Рособоронэкспорта и Рособоронпрома. Мы также очень рады, что наше решение выбрал Райффайзенбанк, который жестко придерживается корпоративных стандартов. Но прямое тестирование нашего продукта показало, что оно лучше, чем имеющийся корпоративный стандарт применительно к переписке на русском языке.

— Каковы стратегические цели компании на ближайшие три-пять лет?

— Мы сохраняем лидерство на российском рынке, диверсифицируем линейку продуктов и начинаем активную экспансию на Ближ-

ний Восток и в Европу с нашим продуктом InfoWatch Traffic Monitor Enterprise, в основе которого — собственные лингвистические технологии, позволившие сделать систему обучаемой. Что крайне важно для качественного категорирования информационных потоков организации — это основное условие эффективности DLP-системы. Кроме того, наработки в области лингвистики позволили нам выпустить новое поколение систем мониторинга и анализа блогосферы (InfoWatch KRIBRUM) — заказчик здесь скорее не «безопасник», а маркетолог, но решение уже вызвало большой интерес.

— Каковы приоритеты вашего развития на вертикальных рынках?

— Прежде всего это государственный сектор, нефтегазовая отрасль (наши клиенты здесь — почти все нефтяные компании), телеком-сектор (мы уже работаем с «Вымпелкомом» и «МегаФоном» и собираемся сотрудничать с МТС). И, конечно же, финансовые организации: более 50 крупнейших банков страны являются нашими заказчиками, сотрудничество с ними продолжается.