

роля над исходящим трафиком сетевых пейджеров (IM — Instant Messenger), что позволяет не только обеспечить соответствие нормативным актам, но и обезопасить этот канал связи от ряда внутренних и внешних угроз.

Правда, Symantec нельзя считать полноценным игроком этой отрасли. Сейчас ходят слухи о том, что она приобретет компанию Vontu, одного из конкурентов InfoWatch. Правда, эксперты сомневаются, что это произойдет. Дело в том, что руководство корпорации сейчас озабочено совсем другим. По результатам деятельности за 2006 финансовый год чистая прибыль Symantec резко упала, составив \$157 млн против \$536 млн в 2005 финансовом году. Если говорить о прибыли на акцию, то за год она составила \$0,15 против \$0,74 в прошлом году. То есть чистая прибыль компании упала на 71%. Так что топ-менеджмент сейчас думает скорее о том, как удержаться в своих креслах, нежели о выходе на новый перспективный рынок. Вдобавок все указывает на то, что акционеры Symantec устали от постоянных поглощений, а без них выйти в новый сегмент вряд ли удастся. Разрабатывать свои технологии с нуля слишком поздно.

А недавно к рынку внутренней безопасности проявила интерес корпорация IBM. Причем не просто проявила — IBM купила одного из нишевых игроков компанию Consul. Решения этой фирмы теперь органично дополняют функциональность IBM Tivoli, которой не хватало как раз внимания к внутренним угрозам. Сравнения решения Consul с InfoWatch, нельзя не отметить коренного различия в подходах. Продукты Consul концентрируются на аудите действий служащих и выполнении требований нормативных актов. Другими словами, они не предотвращают утечку, но минимизируют риски юридического преследования и позволяют выявить внутреннее нарушение постфактум. Решения InfoWatch, напротив, работают в активном режиме — выявляют и пресекают утечку сразу, хватая инсайдера за руку. Здесь снова проявляется то преимущество во времени, которое «Лаборатория Касперского» успела использовать, выйдя на рынок внутренней ИБ раньше конкурентов.

Нельзя обойти стороной и довольно интересную и странную сделку компании WebSense. Прежде всего заметим, что эта фирма является довольно диверсифицированным поставщиком решений в сфере ИТ-безопасности. Она защищает от вредоносных кодов, нецелевого использования ИТ-ресурсов, фишинга и т. д. Несмотря на это, корпорация WebSense поглотила компанию PortAuthority Technologies, которая, как и InfoWatch, занимается только защитой от инсайдеров и утечек. Почему сделка названа странной? Из-за финансовых условий. Дело в том, что WebSense согласилась заплатить \$90 млн наличными. Между тем оборотный капитал PortAuthority составляет всего \$5 млн, а долги — целых \$4 млн. Что же купила корпорация WebSense? Получается, что нематериальные активы. Например, технологии и раскрученную марку. Однако с технической точки зрения продукты PortAuthority выглядят далеко не так блестяще, чтобы за них можно было выложить почти \$100 млн. Так что коэффициент х15 в данном случае указывает на то, что руководство PortAuthority просто смогло на волне интереса к рынку внутренней ИТ-безопасности продать свою компанию по значительно более высокой цене, чем она на самом деле стоит.

На рынке ИБ есть еще одна крупная компания, решившая диверсифицировать свой бизнес и отправиться в новый сегмент. Это корпорация McAfee, которая довольно неожиданно купила небольшую израильскую фирму Onigma, специализирующуюся на предотвращении утечек и защите от инсайдеров. За нее McAfee заплатила \$20 млн наличными, что можно считать вполне справедливой ценой. Дело в том, что о компании Onigma и ее технологиях известно очень мало. Сайт фирмы появился в 2005 году, причем на нем не сообщалось ни об одном клиенте ком-



IBM ВСЕГДА НАЙДЕТ КОГО КУПИТЬ

пании, а также об используемых технологиях. Вполне возможно, что за вывеской Onigma скрывалась небольшая команда израильских инженеров и разработчиков. И McAfee обеспечила себе быстрый выход на рынок, сразу интегрировав продукты Onigma в свою линейку.

Подводя итоги, можно сказать, что волна слияний и поглощений на рынке внутренней ИБ не закончилась. На рынке еще есть крупные и средние игроки, которые могут захотеть интегрировать функциональность по защите от утечек и инсайдеров в свои продукты или просто включить дополнительные продукты в свою линейку. Не исключено, что следующей стратегической покупкой станет одна из российских компаний.

ПИГМЕИ ПРОТИВ ГИГАНТОВ \$1,5 млрд — это сумма, в которую сегодня принято оценивать рынок внутренней ИТ-безопасности. Причем по итогам 2007 года он достигнет \$2,5 млрд. Так что здесь определенно есть предмет для разговора (см. рис. 1).

Откуда взялись такие цифры? Прежде всего компания IDC в 2006 году оценила лишь один из сегментов рынка внутренней ИТ-безопасности в \$600 млн. Это так называемый сегмент OCC (Outbound Content Compliance), куда входят продукты и услуги для защиты от утечек по сетевым каналам (например, по электронной почте и интернету). Однако если оценивать весь рынок, то в него входит еще целый ряд каналов: принтеры, порты рабочей станции, сменные носители и т. д. Причем, по оценке аналитическо-

го центра InfoWatch, в 2006 году общий размер рынка составил почти \$1,5 млрд. Правда, на Россию приходится лишь небольшая часть этого — \$50 млн.

Такие объемы, безусловно, привлекают внимание многих игроков, но наибольший энтузиазм инвесторов и менеджеров вызывают темы роста рынка. В среднем в мире рынок растет на 60–65% ежегодно.

Если на Россию приходится всего 3% рынка, то где же его львиная доля? Известно где — в США. Именно там сегодня находится основное количество поставщиков, каждый из которых уже привлек несколько десятков миллионов долларов на раскрутку. Анализ фандрайзинг-активности пяти крупнейших конкурентов показывает, что в период 2002–2005 годов средний объем венчурных инвестиций составил около \$35 млн. К примеру, Proofpoint — \$36 млн, Reconnex — \$37 млн, Vontu — \$30 млн, Tablus — \$24 млн, PortAuthority — \$31 млн, Orchestra — \$49 млн, Oakley Networks — \$20 млн, Vericept — \$37,5 млн.

Постоянно растет интерес к рынку внутренней безопасности со стороны крупных игроков. Например, IBM и Symantec, McAfee и WebSense, а также «Лаборатория Касперского» уже обеспечили свое присутствие в этом сегменте. Причем если гиганты ИТ-индустрии просто купили действовавших на этом рынке поставщиков, то «Лаборатория Касперского», как уже говорилось, разработала собственную технологию InfoWatch, которая сегодня развивается в виде самостоятельной компании InfoWatch.

В интернете бытует шутка, что Билл Гейтс даже не останвится, чтобы поднять с пола \$100, так как его время стоит значительно дороже. Однако в каждой шутке есть доля правды. Корпорация Microsoft может по праву считаться гигантом ИТ-индустрии, и отрасль размером менее \$1 млрд ее в принципе не должна интересовать. Но если какой-то сегмент ИТ-рынка перейдет этот порог, софтверный гигант приложит все усилия к тому, чтобы начать доминировать в новом для него сегменте. То же справедливо и для других крупнейших игроков, за спиной которых огромные маркетинговые возможности, сеть партнеров по всему миру и практически неограниченный потенциал инвестиций. Все это позволяет захватить новый рынок довольно быстро, лишь бы игра стоила свеч.

А уже сейчас ясно, что рынок внутренней ИТ-безопасности — это интересный сегмент и что по своим размерам он уже превосходит либо перерастет в ближайшем будущем рынки антивирусов, межсетевых экранов, фильтров спама и многие другие сегменты. Прямо сейчас на рынке наблюдается бум слияний и поглощений, причем комбинации могут быть самые разные.

Не исключено, например, что в недалеком будущем InfoWatch выкупит активы материнской компании и «удочерит» «Лабораторию Касперского».

Но что будет с рынком дальше? Тут возможно несколько сценариев.

Весь рынок как самостоятельный сегмент может просто исчезнуть. Например, крупные игроки используют приобретенные технологии, чтобы встроить в свои продукты. Другими словами, эти компании ищут синергию между своими продуктами и купленными средствами по защите от инсайдеров и утечек. Создав комплексное решение, поставщики хотят повысить ценность своего предложения именно за счет этой антиинсайдерской составляющей. Эта функциональность не случайно названа антиинсайдерской, так как пример того, как вполне определенный сегмент рынка ИТ-безопасности был по кусочкам растащен всеми игроками, лежит на поверхности. Это антишпионские программы.

Еще три года назад было много небольших компаний, разрабатывавших средства защиты от шпионов. Но где они все сейчас? Куда подевался вообще весь этот сегмент рынка? Его разобрали по частям крупные антивирусные компании. Теперь антишпионских программ в чистом виде нет, есть комплексные антивирусы, которые защищают в том числе и от шпионов.

То же самое может произойти и с системами защиты от утечек. Действительно, что может сделать маленькая фирма, если на нее покусилась транснациональная корпорация? Основное конкурентное преимущество небольшой семейной фирмы чаще всего состоит в 10–15 технарях, которые разбираются в какой-то области настолько глубоко, что могут время от времени выдавать блестящие технические решения. Однако это отражается только на функциональных характеристиках продукта, а они решают далеко не все.

И все же рынок решений для защиты от инсайдеров вполне может сохранить самостоятельность. Это произойдет в том случае, если крупным игрокам индустрии не удастся нащупать синергию или она будет настолько мала, что покупать комплексное решение будет невыгодно. Кроме того, даже если большие рыбы съедят почти всех маленьких, почти всегда оставшиеся в живых компании смогут занять очень удачную позицию, заявив о том, что сфокусированы на внутренней ИТ-безопасности. Действительно, поставщик, который позиционируется как разработчик средств защиты от какой-то одной определенной группы угроз, будет иметь неоспоримое преимущество по сравнению с поставщиком универсальных продуктов. Так что позитивные перспективы рынка очевидны в любом случае. ■

ВОЛНА СЛИЯНИЙ И ПОГЛОЩЕНИЙ НА РЫНКЕ ИБ НЕ ЗАКОНЧИЛАСЬ. ЕЩЕ ЕСТЬ КРУПНЫЕ ИГРОКИ, КОТОРЫЕ МОГУТ ЗАХОТЕТЬ ВКЛЮЧИТЬ ДОПОЛНИТЕЛЬНЫЕ ПРОДУКТЫ В СВОЮ ЛИНЕЙКУ. НЕ ИСКЛЮЧЕНО, ЧТО СЛЕДУЮЩЕЙ ПОКУПКОЙ СТАНЕТ ОДНА ИЗ РОССИЙСКИХ КОМПАНИЙ



КОНКУРЕНТЫ

САМЫЕ КРУПНЫЕ ПОГЛОЩЕНИЯ НА РЫНКЕ ИТ-БЕЗОПАСНОСТИ	
КОМПАНИЯ	ПОГЛОЩЕНИЕ
SYMANTEC	В ФЕВРАЛЕ 2006 ГОДА КОРПОРАЦИЯ SYMANTEC ПОГЛОТИЛА IMLLOGICS, РАЗРАБОТЧИКА СРЕДСТВ ЗАЩИТЫ ИМ-ТРАФИКА, В ТОМ ЧИСЛЕ, И ОТ ИНСАЙДЕРОВ. ЭКСПЕРТНАЯ ОЦЕНКА СУММЫ СДЕЛКИ \$15 МЛН.
MCAFFEE	В ОКТЯБРЕ 2006 ГОДА КОМПАНИЯ MCAFFEE ПРИОБРЕЛА НЕБОЛЬШУЮ ИЗРАЙЛЬСКУЮ ФИРМУ ONIGMA ЗА \$20 МЛН. ONIGMA СПЕЦИАЛИЗИРОВАЛАСЬ ТОЛЬКО НА ЗАЩИТЕ ОТ ИНСАЙДЕРОВ И УТЕЧЕК.
WEBSense	В ДЕКАБРЕ 2006 ГОДА КОМПАНИЯ WEBSense ПОГЛОТИЛА PORTAUTHORITY, ВЫЛОЖИВ \$90 МЛН. ПРОДУКТЫ PORTAUTHORITY ПРЕДНАЗНАЧЕНЫ КАК РАЗ ДЛЯ ЗАЩИТЫ ОТ ИНСАЙДЕРОВ.
IBM	В ДЕКАБРЕ 2006 ГОДА КОРПОРАЦИЯ IBM ОБЪЯВИЛА О ПОГЛОЩЕНИИ CONSUL, ПОСТАВЛЯЮЩЕЙ ПРОДУКТЫ ДЛЯ ОБЕСПЕЧЕНИЯ СОВМЕСТИМОСТИ С НОРМАТИВНЫМИ АКТАМИ И ВНУТРЕННЕГО АУДИТА. ЭКСПЕРТНАЯ ОЦЕНКА СУММЫ СДЕЛКИ \$40 МЛН.
CISCO	В ЯНВАРЕ 2007 ГОДА CISCO КУПИЛА ЗА \$800 МЛН. КОМПАНИЮ IROREPORT, ЗАНИМАЮЩУЮСЯ ФИЛЬТРАЦИЕЙ ВХОДЯЩЕГО И ИСХОДЯЩЕГО ТРАФИКА.