

05 | 2009



AHK

impuls

Magazin der Deutsch-Russischen Auslandshandelskammer
Журнал Российско-Германской Внешнеторговой Палаты



MEHR TRANSPARENZ
BEI AUSSCHREIBUNGEN
БОЛЬШЕ ПРОЗРАЧНОСТИ
ПРИ РАЗМЕЩЕНИИ ГОСЗАКАЗОВ
ZOLLPROBLEME UND
KEIN ENDE IN SICHT!
ТАМОЖНЯ! КОГДА
ЭТО ЗАКОНЧИТСЯ?
REIFEPRÜFUNG JENSEITS
DES URALS
ЭКЗАМЕН НА ЗРЕЛОСТЬ
ПО ТУ СТОРОНУ УРАЛА

FOCUS:

INFORMATIONSTECHNOLOGIEN

ТЕМА НОМЕРА:

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ



RUSSLAND WIRD HEIMAT FÜR SOFTWAREPRODUKTION

Ich freue mich, den Lesern in dieser Impuls-Ausgabe den russischen IT-Markt vorstellen zu dürfen. Die Informationstechnologien wiesen in den letzten Jahren ein beeindruckendes Wachstumstempo auf. Die Krise hat dieses Tempo zwar bremsen aber nicht stoppen können, das Wachstum liegt nach Angaben des Marktforschungsinstituts IDC immer noch bei 18,7 Prozent.

Das ist mehr als der durchschnittliche Weltmarkt. Die Potentiale des russischen Marktes sind groß.

Ungefähr die Hälfte des IT-Marktes stellt die Produktion von Software: die Herstellung maßgeschneiderter (28 Prozent) und fertiger (20 Prozent) Programme. Ein Großteil dieser Produktion (ca. 50 Prozent) wird ins Ausland verkauft, auch nach Deutschland.

2008 wuchs der Verkaufsumfang von Software in Russland um 35 Prozent. 2007 lag das Wachstum noch höher. Dieses unglaubliche Tempo ist im Wesentlichen auf den Kampf gegen die Produktpiraterie zurückzuführen. Was den Marktumfang betrifft, gehen die Meinungen der Analytiker auseinander. IDC schätzt ihn auf 2,7 Milliarden US-Dollar, die ISDEF-Gruppe auf 3,7 Milliarden US-Dollar. Die Wahrheit liegt vermutlich irgendwo in der Mitte.

In jedem Fall aber ist die Softwareentwicklung das dynamischste und zukunftsreichste Marktsegment. Zwar glaube ich nicht, dass Russland Indien, das einen großen Teil des Marktes für maßgeschneiderte Software erobert hat, den Rang ablaufen wird, aber der russische Weg könnte dem israelischen ähneln, d.h. es könnte sich auf Entwicklung und Verkauf fertiger Angebote für Unternehmen und Privatpersonen konzentrieren. Für Spezialanfertigungen ist ein russischer Programmierer zu teuer; er verdient genauso viel und teilweise sogar mehr als sein deutscher Kollege.

Ich glaube, die russische IT-Industrie hat eine große Zukunft und dürfte auch für deutsche Investoren als potentieller Partner hoch interessant sein.

Natalija Kasperskaja

Mitglied des Vorstandes der AHK Russland
Vorsitzende des Direktorenrates
der Unternehmensgruppe Kaspersky Lab
Geschäftsführerin InfoWatch

РОССИЯ – РОДИНА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Данный выпуск посвящен информационным технологиям (ИТ).

Я имею честь представить читателям российский рынок ИТ, который последние годы демонстрировал опережающие темпы роста. Правда, кризис слегка сократил эти темпы, но, даже с учетом этого, рост российского ИТ-рынка, по оценке исследовательской компании IDC, составил 18,7%, что в несколько раз выше темпов роста мирового рынка. Наш рынок пока еще развивается и поэтому имеет большой потенциал. Примерно половину рынка составляют разработка заказного (28%) и создание готового (20%) программного обеспечения (ПО). Иными словами, российский рынок ИТ – это создание продуктов и разработок на заказ. Причем значительная часть готовых программных продуктов и услуг по разработке (около 50%) поставляется за рубеж, в том числе в Германию.

За 2008 г. объем продаж ПО в России вырос на 35%, тогда как в 2007 г. рост составил 75%(!) (данные исследовательской группы ISDEF). Такой высокий темп роста достигнут в основном за счет борьбы с пиратством. Эти же цифры подтверждают и другие исследователи. Однако, что касается объемов рынка, тут исследователи расходятся в оценках. От 2,7 млрд дол., по оценке IDC, до 3,7 млрд дол., по оценке ISDEF. Истина, наверное, лежит где-то посередине.

В любом случае, сегмент разработки программного обеспечения – самый динамичный и, на мой взгляд, самый перспективный.

Я не верю в то, что России удастся отвоювать лавры у Индии, которая охватила огромную часть рынка заказного программирования.

Мне кажется, что российский путь – это скорее путь Израиля.

Т.е. создание и продажа готового ПО компаниям и частным лицам.

Причина проста – стоимость труда российского программиста равна, а то и превышает стоимость немецкого. Поэтому западным компаниям невыгодно заказывать разработку в России, т.к. стоимость подобного заказа в Индии будет на порядок ниже.

Мне кажется, российская индустрия производства программного обеспечения очень перспективная и должна быть интересна потенциальным партнерам и инвесторам из Германии.

Н.И. Касперская

Член правления Российско-Германской ВТП
Председатель Совета директоров Группы Компаний Kaspersky Lab
Генеральный директор компании InfoWatch



МЕЖДУ ДВУХ ОГНЕЙ

ИНТЕРНЕТ ОТКРЫЛ БЕЗГРАНИЧНЫЕ ВОЗМОЖНОСТИ ДЛЯ ДОСТУПА К ИНФОРМАЦИИ И ОБЩЕНИЮ. НО ВМЕСТЕ С ПРОГРЕССОМ ПОЯВЛЯЕТСЯ И ПОТЕНЦИАЛ ДЛЯ ЗЛУОППОТРЕБЛЕНИЯ НОВЫМИ ТЕХНОЛОГИЯМИ. / ИЛЬЯ ШАБАНОВ, INFOWATCH

Незаметно для самих себя, люди в XXI веке оказались в весьма противоречивой ситуации. С одной стороны, человеку стали доступны такие возможности, о существовании которых раньше могли догадываться только фантасты, с другой стороны, эти самые возможности стали ловушкой для тех, кто их использует. Интернет и всё связанное с ним (от icq/skype до электронной коммерции), компьютеры (от стационарных до коммуникаторов), съемные накопители информации (от компакт-дисков до терабайтовых жестких дисков) — всё это за последние годы стало неотъемлемой частью нашей жизни и в значительной мере облегчило нам деятельность во всех областях: бизнесе, работе, образовании, общении, отдыхе и т.п. Однако очевидно, что одну и ту же вещь можно использовать как во благо, так и во вред. Пираты, вредоносные программы, киберпреступники, хитроумные инсайдеры являются неизбежным злом, с которым приходится бороться производителям софта, ИТ-специалистам, простым пользователям. Именно здесь и кроется ловушка. Многие

из нас до сих пор не осознали степени проникновения информационных технологий и связанных с ними угроз в нашу жизнь и по-прежнему думают: меня-то это не коснется. А между тем сегодня практически вся информация, с которой нам приходится сталкиваться, переведена в электронный вид — а значит, потенциально подвержена как внешним, так и внутренним информационным угрозам. Сам того не подозревая, человек, пользующийся данными, хранящимися в электронном виде, попадает в западню: атака осуществляется извне и изнутри одновременно — конфиденциальные данные компании оказываются между двух огней. Причём о внешних информационных угрозах человек более-менее осведомлён: о хакерах и прочих киберпреступниках снимают фильмы, пишут книги, показывают сенсационные материалы по телевидению, кроме того, антивирусные программы стоят сегодня, наверное, на каждом компьютере, подключённом к Интернет, — о существовании вирусов и их опасности знают все. Однако про угрозы и о том, как от них можно

защититься, до недавнего времени человек просто не задумывался. Точнее не задумывались об этом раньше люди, владеющие или управляющие бизнесом. Потому что источниками внутренних угроз являются собственники компании. Сегодня только в ЕС, США и некоторых других странах есть законы, обязывающие компании оповещать пострадавших об утечке информации. Но в большинстве стран правовой статус пока не определен. Вопрос о важности защиты от внутренних угроз стал довольно остро после того, как в последние годы утечки информации одна за другой начали потрясать крупнейшие предприятия. Виновниками оказываются зачастую сами сотрудники пострадавших компаний. Многие случаи заставляют задуматься о важности защиты информации от утечек и о серьёзности рисков, которым подвергаются компании в случае несанкционированного использования информации внутри компании. Действительно, кому проще получить доступ к папке с документами на

офисном компьютере: хакеру, удалённо пытающемуся сломать корпоративную сеть и подобрать пароли, или сотруднику компании, хорошо разбирающемуся в устройстве сети. До недавнего времени решений, которые обеспечивали бы конфиденциальность данных внутри компании, попросту не было на рынке, и владельцы бизнеса не могли контролировать информационные потоки в компании, обнаруживать несанкционированное использование корпоративных данных. Сегодня такие средства есть - DLP-системы (Data Leakage Prevention). Эти решения осуществляют контроль основных каналов утечек, позволяя предотвратить случайные или умышленные утечки информации.

Многие утечки носят случайный характер - это, в первую очередь, неосторожные действия сотрудников: потери мобильных компьютеров, носителей и архивов, случайная отправка конфиденциальных данных по e-mail и их попадание в Интернет, такие случайные утечки могут стоить компании миллиарды долларов.

Помимо собственно утечек, DLP-система способна обнаруживать нарушения политик информационной безопасности. Это и пересылка конфиденциальной информации на подозрительные почтовые ящики, и публикация в Интернет заведомо ложной или

искаженной информации, порочащей репутацию компании.

Помимо случайных, фиксируются и умышленные утечки, число которых в 2009 г. значительно возросло. С умышленными утечками бороться достаточно сложно. Ведь инсайдер, как правило, имеет время подготовиться, изучить системы защиты в компании. А если он обладает хорошими знаниями в ИТ, то остановить утечку еще сложнее.

Необходимо отметить, что комплексные специализированные DLP-решения являются наиболее эффективным способом борьбы с утечками данных, так как они защищают сразу весь информационный периметр организации, а также обеспечивают исполнение «внешних» требований по защите информации, предъявляемых партнёрами или государственными органами.

На сегодняшний день на российском рынке присутствует несколько игроков, предлагающих DLP-решения: американские компании (Websense, McAfee, Symantec) и российская (InfoWatch). У каждой системы есть свои преимущества. Компания InfoWatch (входит в Группу компаний «Лаборатория Каперского») вышла на рынок DLP в России раньше других и является сегодня лидером этого сегмента рынка.

Современная DLP-система - это, прежде всего, комплексный и многоуровневый подход

к защите от внутренних информационных угроз в компании. Комплексность заключается в том, что помимо технических средств контроля нужна также и административная поддержка. Должны быть выстроены политики доступа к конфиденциальной информации, использованию ИТ-ресурсов и т.п. Под многоуровневостью защиты, как правило, имеется в виду наличие контроля за использованием информации на разных уровнях: на уровне сети (контроль трафика); на уровне рабочих станций (контроль внешних устройств); шифрование (дополнительный уровень защиты).

Кроме этого, для DLP-системы важно иметь возможность пост-анализа, когда офицер безопасности может обнаружить инцидент, анализируя снятую копию трафика. Часто умышленные утечки обнаруживаются именно постфактум, инсайдера берут с поличным, уже имея на руках хорошую доказательную базу.

За несколько лет DLP-системы успели показать свою эффективность. Отдельные случаи выявления и наказания злоумышленных инсайдеров и предотвращения утечек коммерческой тайны попадают в прессу. Опыт эксплуатации показал, что DLP-система в состоянии предотвратить существенное число утечек, а значит, сэкономить деньги компании и сохранить ее имидж.)

Говорите ли Вы по-русски?*

*Sprechen Sie Russisch?

Müssen Sie auch nicht, denn das übernehmen wir für Sie. Rödl & Partner berät Sie fach- und grenzüberschreitend in den Bereichen:

- > **Wirtschaftsprüfung**
- > **Steuerberatung**
- > **Rechtsberatung**
- > **Outsourcing**

In Russland an unseren Standorten Moskau und St. Petersburg sowie Nürnberg, unserem Stammsitz – und 80 weiteren Niederlassungen weltweit.

Ihre Ansprechpartner für Russland:

André Scholz – WP, StB, Partner – andre.scholz@roedl.com

Dr. Andreas Knaut, LL.M. – RA, Partner – andreas.knaut@roedl.pro

Manfred Janoschka – WP, StB, Partner – manfred.janoschka@roedl.com

Bosnien-Herzegowina · Brasilien · Bulgarien · Deutschland · Estland · Frankreich · Großbritannien · Hong Kong · Indien · Indonesien · Italien · Katar · Kroatien · Lettland · Litauen · Moldawien · Österreich · Polen · Rumänien · Russland · Schweden · Schweiz · Singapur · Slowakei · Slowenien · Spanien · Südafrika · Thailand · Tschechische Republik · Türkei · Ukraine · Ungarn · USA · Vereinigte Arabische Emirate · Vietnam · VR China · Weißrussland

> 83 Standorte > 37 Länder > ein Unternehmen

Rödl & Partner Moskau | Business Center LeFort | Elektrosawodskaja 27 – 2 | Moskau 107023 | Tel. +7(495)933 51 20
Rödl & Partner St. Petersburg | Linija 14, Gebäude 7 | Wassiljewskij Ostrow | St. Petersburg 199034 | Tel. +7(812)320 66 93

www.roedl.ru