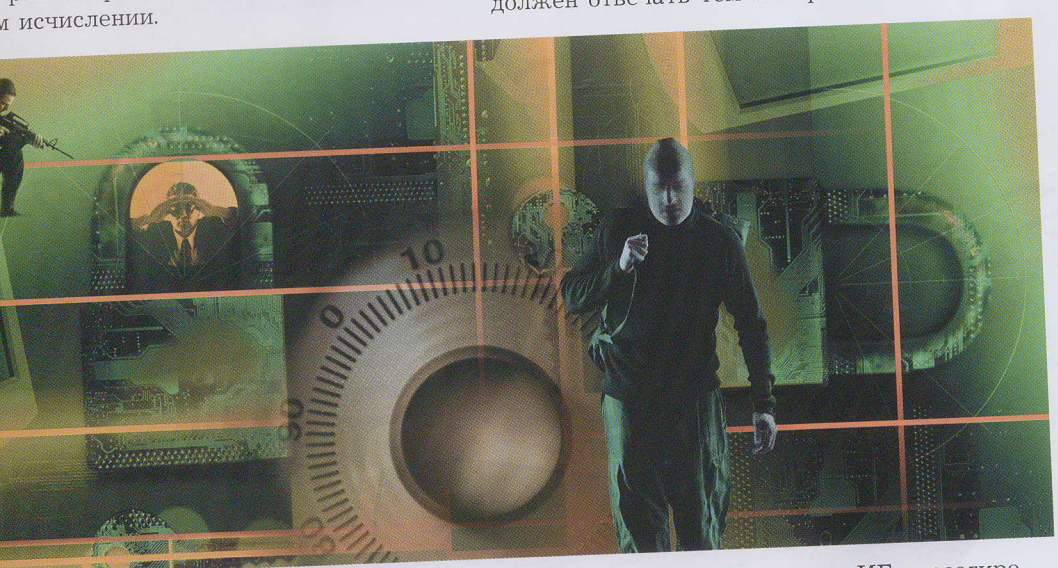
В зоне стабильного роста

истем информационной безопасности да привлекал особое внимание игро- ла сбыта. Причины такого интереса : спрос на продукцию для обеспече- постоянно увеличивается, он не па- е в самые трудные кризисные годы, тающая сложность решений позво- считывать не только на высокую но и на получение дополнительной от внедрений, консалтинга, техни- оддержки и предоставления дру- г.

ценкам экспертов и игроков ИТ-ка- последние несколько лет темпы ро- сийского рынка ИБ измеряются дву- ми цифрами, что является хорошим елем на фоне других сегментов нка. В частности, по словам **Наталии нко,** директора направления инфор- ной безопасности в компании RRC, ный рост в сфере ИБ составляет ее 15%. Похожие цифры называет **ил Пустовой,** директор по развитию Distribution. Он считает, что объемы а за последние годы росли относи- равномерно, на 10–15% в год в ва- м исчислении.

проектов заканчивалось покупкой и установкой продуктов, при этом не уделялось должного внимания процедурам, обеспечивающим интеграцию купленных продуктов в инфраструктуру безопасности предприятия, — говорит **Андрей Зеренков**, эксперт по ИБ компании Symantec. — Безопасность — это быстро меняющаяся область, которая должна оперативно реагировать на появление новых технологий и продуктов и максимально быстро реагировать на появляющиеся новые угрозы. Поэтому принцип „установить и забыть“ для ИБ давно неприменим». Он подчеркнул, что ИБ — это комплекс организационно-технических мер, включающих в себя технологии, воплощенные в продукты, процессы обеспечения ИБ, опирающиеся на политики безопасности и регламенты, а также высококвалифицированные специалисты и обычные сотрудники, знающие актуальную информацию о запретах, разрешениях и действиях в различных ситуациях. Причем это не требование последних лет. Таким было положение дел в течение долгого времени, вне зависимости от стран и континентов. Российский рынок ИБ, как и мировой, должен отвечать тем же требованиям —



охватывать все компоненты ИБ и реагировать на вновь появляющиеся угрозы.

Андрей Зеренков добавил, что данные, предоставляемые глобальной сетью мониторинга Global Intelligence Network (GIN) компании Symantec, наглядно демонстрируют, что атакам подвержены не только крупные фирмы, но и небольшие компании, а также отдельные офисы и филиалы. Поэтому востребованность систем ИБ стала заметно выше, и все большее количество ИТ-компаний вовлекаются в сферу их создания и сопровождения, что невозможно без наличия квалифицированных кадров.

«За последние годы рост рынка ИБ не был впечатляющим. Тем не менее заметное развитие и тенденции к росту воодуговорит **Михаил Лисневский,**

эксперт по ИБ компании OCS Distribution. — Рост этого сегмента рынка обеспечивают постоянно возникающие риски и угрозы. Появились новые продукты, новые вендоры. Активное развитие облачных технологий стало очередной ступенью в развитии ИБ. И несмотря на то, что это направление только набирает обороты, — будущее за ним».

Как отмечает **Михаил Кондрашин,** технический директор российского представительства Trend Micro, последние годы на рынок ИБ оказывал значительное влияние закон «О персональных данных» (152-ФЗ), а сегодня — в основном новое поколение таргетированных угроз, ориентированных на определенные вертикальные рынки, такие как, например, финансовый. Соответственно интерес заказчиков вызывают продукты, которые не только и не столько обнаруживают вирусы, сколько предлагают защиту от неизвестных угроз, используя поведенческий анализ и облачные системы работы с «большими данными».

«Одна из отличительных особенностей рынка ИБ — его стабильность и слабая восприимчивость к изменениям экономического климата. Связано это прежде всего с отраслевым регулированием данного рынка, т. е. существующими законами и стандартами работы с конфиденциальной информацией. В нашей практике мы наблюдаем стабильный рост продаж, на котором не сказался даже кризис 2008 г.», — заявил Даниил Пустовой. Он добавил, что с технологической точки зрения происходит много изменений в направлении усиления безопасност применяемых решений, симметричный отве на ежегодно растущее количество угроз и техническую оснащенность злоумышлен- ников. Яркий пример — повсеместное внед рение системы строгой аутентификации кл ентов банков при использовании платежны систем Visa и MasterCard. Рост популярнос биометрической аутентификации (использ ванной в Apple iPhone 5S), хотя пока это лишь первый столь значимый прорыв дан ной технологии, ее использование в корпо ративной среде сталкивается с рядом сло ностей и остается делом будущего.

Происходит также заметный сдвиг от программных средств ИБ к аппаратным что обусловлено принципиальной невозмо ностью обеспечить с помощью программн решений защиту от ряда внешних и вну ренних угроз. Например, центры сертифи ции (удостоверяющие центры) переходят на аппаратные криптографические средс (аппаратные модули безопасности), поско ку программные решения не могут гаран ровать необходимого уровня безопасност электронных сертификатов.

«Каждый год появляются новые спосо компрометации различных систем. В свя с этим развиваются и системы ИБ. При э

то же представляет собой российский ок ИБ сегодня и как его состояние по- ло на канал сбыта?

о мнению **Владимира Мамыкина,** дирек- по ИБ Microsoft в России, если сравни- наш рынок систем безопасности с ана- чными рынками других стран мира, ючая страны Западной Европы, то мож- казать, что он достиг высокого уровня лости. Представлено множество решений защите информации, и у клиента есть можность выбирать именно те продукты, орые оптимально подходят для конкрет- х бизнес-задач.

«Главное отличие последних лет — это ественный скачок в требованиях заказ- к процессу внедрения решений. Совсем

крупных городах, таких
ва, Санкт-Петербург,
рск и Екатеринбург,
тся и растет быстрее,
угих регионах, —
ает **Сергей Ласкин**, ве-
сперт по ИБ компании
– Многие крупные орга-
помимо стандартных
защиты (таких как ан-
, межсетевые экраны,
ние) используют сете-
ства предотвращения
ий (IPS), информацион-
емы сбора и корреляции
(SIEM), решения по за-
итичных систем (CSP).
ниях среднего и малого
все чаще появляется
почтовых и веб-шлюзов,
ритичные бизнес-сис-
щищаются решениями
ntegrity Control».
говорить о сегменте ан-
ых систем, то в послед-
лет он показывал самые
темпы роста на всем
ИБ, — говорит **Сергей**
управляющий директор
тории Касперского»
, странах Закавказья
ей Азии. — Это было
с несколькими фактора-
ервых, произошло „обе-
рынка ПО: клиенты ак-
реходили с нелицензи-
родуктов на лицензион-
сновном это коснулось
х пользователей, а так-
ента малых и средних
й). Особенно сильно тен-
проявилась, когда госу-
ные органы начали про-
аличия контрафактного
ензионного ПО. Второй
— это изменение зако-
ной базы — вступление
акона о персональных
обязательная сертифи-
ля программных продук-
щающих персональные
и т. д. На сегодня эти
ы исчерпаны, по край-
е, основную свою роль
сыграли.
сегмент рынка транс-
уется от простых анти-
к комплексным реше-
асса end point security:
к от насыщения и будет
ться темпами, опережаю-
ост рынка ИБ и, тем
есь рынок ИТ в сово-
и». Сергей Земков отме-
акцент смещается от ло-
х офисных сетей в сто-
роз для виртуальных
ромышленных объектов,
ых устройств сотрудни-
и этом большинство ком-
е до конца понимают,
г чего себя защищать.

В России новые технологии внедряются не очень быстро. Сложность заключается в недостатке подходящих стандартов и документов, которые регулировали бы работу новых систем — без них затруднена работа в государственных организациях и долго идут проекты в коммерческих компаниях, а зарубежные стандарты и правила далеко не всегда применимы к нашей действительности. Особенно это касается защиты государственных информационных систем. Среди вертикальных рынков, которые больше других готовы к внедрению новинок, можно назвать финансовый сектор, банки, телекоммуникационные компании. Это те отрасли, где ИТ-инфраструктура является основным инструментом работы, для них большая технологичность бизнеса означает его большую эффективность и прибыльность.

«Рынок ИБ за последние годы существенно изменился и до сих пор продолжает расти. Несмотря на некоторое замедление общих темпов роста ИТ-рынка, безопасность остается одним из самых быстроразвивающихся и устойчивых его сегментов, — считает **Катажина Хоффманн-Селицка**, менеджер по продажам HID Global в Восточной Европе. — Уровень инвестиций повышается, что говорит о положительной динамике. Более того, руководители компаний-заказчиков начали принимать активное участие в контроле безопасности, и это также хороший знак. Постепенно приходит понимание, что в большинстве случаев размер убытков может быть значительно выше, чем стоимость систем защиты. Многие клиенты также стали уделять особое внимание показателям эффективности при выборе того или иного решения». Другим важным драйвером российского рынка ИБ Хоффманн-Селицка называет требования регулирующих органов, в частности законы «О национальной платежной системе», «О персональных данных» и пр. Подобные регламентирующие требования способствуют развитию рынка и притоку инвестиций. «Благодаря законодательству усилилась роль российских сертифицированных решений. Их доля за последние пять лет заметно выросла», — отмечает Наталия Базаренко.

Об этих же факторах говорит и **Александр Сауленко**, эксперт по ИБ компании Treolan. Он подчеркивает, что самые значимые изменения на рынке ИБ в последнее время связаны с деятельностью регуляторов. Заказчики стали более внимательно относиться к требованиям, которые им диктуют государственные и отраслевые стандарты. По этой причине рынок ИБ постоянно растет и развивается. «Технологических новинок, которые бы „выстрелили“ в последние пару лет, я выделить не могу, хотя следует отметить возрастающий интерес к решениям SIEM, продуктам по управлению и мониторингу систем безопасности», — добавил Сауленко. Его коллега **Александр Мормуш**, руководитель направления ИБ компании Treolan, говорит, что в целом российский рынок ИБ развивается весьма бурно, поскольку его потенциал огромен. «За последние несколько лет структура рынка изменилась. В Россию пришло много западных игроков, предлагающих широкую линейку комплексных решений, соответствующих основным трендам безопасности, таким как мобильный доступ к ИТ-ресурсам, защита промышленных систем и виртуальных сред, защита от DDoS-атак и т. д. Наряду с этим внедрение таких решений осложняется недостатком стандартов и документов, регламентирующих работу этих систем. Особенно это касается защиты государственных информационных ресурсов. В связи с этим, возможно, в ближайшем будущем мы увидим специализированный орган или министерство, которые возьмут на себя подготовку и реализацию стандартов, связанных с информационной безопасностью», — заявил Мормуш. С ним согласны специалисты компании Safensoft. По их мнению, конкуренция на рынке усилилась. Западные вендоры стремятся соответствовать требованиям российских регуляторов. Заказчики стараются уйти от традиционных средств защиты, их все больше интересуют альтернативные и комплексные подходы к ИБ, позволяющие обойти ставшие стандартными проблемы обновления антивирусных баз и снижения работоспособности машин.

Наталия Тесакова, директор по маркетингу компании «Андэк», отмечает, что предложения интеграторов в части инфраструктурных решений и построения процессов безопасности стали «типовыми», и все чаще за названием «интегратор» скрывается проектный дистрибьютор с прямыми поставками клиенту. С другой стороны, в условиях продолжающегося кризиса и сокращения бюджетов заказчики стремятся получить индивидуальные решения. Таким образом, налицо противоречие между структурой спроса и предложения. За прошедшие два года еще больше возросло значение юридической составляющей в ИБ, которая связана с усилением темы «снижения рисков бизнеса» и борьбы с мошенниками, ну и, конечно же, с деятельностью регуляторов по таким вопросам, как национальная платежная система, персональные данные, защита критически важных промышленных объектов, защита государственных информационных систем и пр.

По мнению **Вячеслава Медведева**, старшего аналитика компании «Доктор Веб», в течение 2012–2013 гг. бизнес привел к «единому знаменателю» различные, ранее разнородные средства безопасности. На рынке отразилось и увеличение финансирования государственных органов, организаций, связанных с деятельностью Министерства обороны Российской Федерации, иных силовых структур. В то же время Медведев отмечает, что к 2013 г. рынок ИБ в значительной мере исчерпал свой потенциал. «Практически прекратилось „воздействие на умы“ Федерального закона № 152-ФЗ „О персональных данных“, многие компании завершили консолидацию и упорядочивание систем защиты или, по крайней мере, приняли решение об этом. Многие антивирусы, ранее считавшиеся лидерами отрасли, фактически исчезли с рынка, — сказал он. — Негативной тенденцией последних лет можно считать бездумный переход в облака. Любая технология имеет свои преимущества и недостатки, и системы виртуализации, внедряемые провайдерами услуг, не являются исключением. Переход в облака повышает надежность хранения данных и решает проблемы с масштабируемостью. Но одновременно он ставит неразрешимые проблемы, связанные с защитой персональных данных, необходимостью увеличения затрат на безопасность, что практически никогда не учитывалось в проектах по переходу в облака. В связи с этим нужно отметить, что бурное развитие

й, к сожалению, не со-
ется ростом осведом-
об их недостатках.
ехнологий доносят до по-
ных клиентов только
ества, а о проблемах
ели узнают, когда слу-
русные инциденты
си данных».
тика защищенности,
Вячеслава Медведева,
ет, к чему приводит
ход. Несмотря на рост
к средствам защиты,
езащищенных ком-
остается на прежнем
ак практически не ме-
структура продаж
ащиты. Это говорит
до сих пор большин-
аний далеко не пол-
щищают свои сети
щита не соответству-
енным угрозам.

плаву

озиции компаний, про-
х решения для ИБ?
ли они в более выгод-
жении по сравнению
игроками рынка?
нию Сергея Ласкина,
нимающиеся информа-
езопасностью, всегда
на плаву. Как извест-
ИБ никогда не падал,
изис.
ется, что во времена
ности финансовой си-
аилучшем положении
ся именно производи-
тв защиты. Дело в том,
бные моменты компа-
учивают гайки", что
иводить к появлению
х сотрудников, а сле-
, к потенциальным
с безопасностью, —
ндрей Зеренков. —
дит к тому, что ин-
едствам защиты рас-
етственно приорите-
ов, связанных с ИБ,
ут». По словам Зерен-
ост влияющих на биз-
их рисков компании,
о, реагируют мерами,
ми эти риски изнут-
вышение защищен-
й и систем от кибер-
ита критической
са информации, обес-
ащиты быстро расту-
тра услуг и техноло-
как BYOD, виртуаль-
ачные среды, приня-
жестких политик
ов, эволюция процес-
елью оградить компа-
ешних и внутренних
акже снизить регуля-
ски.

Как видно, перед компаниями стоят задачи самого разного уровня — от условно простых до труднорешаемых. И все они актуальны, если не прямо сейчас, то станут таковыми в ближайшем будущем. Некоторые из поставщиков пока готовы взяться лишь за простые решения, а другие уже посматривают на самые сложные. Компаний-заказчиков на рынке множество, и каждая из них вынуждена решать ту или иную ИБ-задачу — и с точки зрения обеспечения жизнеспособности бизнеса, и с точки зрения соответствия законодательным и регуляторным требованиям.

«Постоянное изменение ландшафта угроз, особенно появление „нацеленных" атак, порождает спрос, который нельзя удовлетворить использованием традиционных средств безопасности или перенастройкой существующей инфраструктуры», — подчеркивает Михаил Кондрашин. А Даниил Пустовой отмечает, что грядущая сертификация оборудования станет импульсом для очередного скачкообразного роста продаж, как и вступление в силу новых обязательных отраслевых стандартов, например принятого стандарта платежной индустрии PCI HSM, который вскоре станет обязательным. Как отмечают специалисты Safensoft, у компаний, в портфеле которых имеются ИБ-решения, особенно новые, более высокие шансы удовлетворить потребности заказчика за счет современного, полного и комплексного решения задач по построению информационной среды в компании. Если же речь идет о вендорах, то у отрасли ИБ есть одно преимущество по сравнению с остальными — она никогда не потеряет актуальность.

«Неоспоримым преимуществом, которое становится все более выраженным, является стабильность спроса на решения ИБ, — подчеркивает Даниил Пустовой. — Глобальный рост компьютеризации, интернет-активности, интернет-коммерции и циркуляции электронных денег, ставший возможным благодаря развития всех отраслей ИТ, ведет к еще более ускоренному росту как количества угроз, так и спроса на решения ИБ. Но если в условиях кризиса с инвестициями в ИТ можно несколько повременить, то решение задач ИБ во многих сферах бизнеса не терпит ни отлагательства, ни компромиссов».

Плата за привилегированность

Как отмечает Владимир Мамыкин, в связи с киберугрозами, а также изменениями в текущем законодательстве требования к игрокам канала продаж постоянно растут. Рынку необходимы специалисты, прекрасно разбирающиеся не только в технологиях, но и в законодательной базе, а также в текущих бизнес-процессах заказчика. Только при учете всех трех факторов специалист сможет предложить оптимальное решение.

По словам Вячеслава Медведева, средства ИБ будут востребованы всегда, а в связи с постоянным изменением угроз они вынуждены все время развиваться. В то же время усложнение средств защиты и появление все более изощренных угроз поднимают уровень требований к специалистам реселлеров и клиентов. «Гонка вооружений» в области противостояния вредоносного ПО и систем ИБ не даст почивать на лаврах никому. Слишком легко остаться на обочине.

Михаил Кондрашин подчеркивает, что новый ландшафт угроз радикально меняет расстановку сил. Теперь партнер должен быть не только экспертом по самому продукту безопасности, но и разбираться в том, что и как нужно защищать у заказчика. Современные продукты — лишь одна часть решения, другая — сервис. Именно опыт подобных работ, уровень доверия заказчиков и является требованием, выдвигаемым своим партнерам производителями современных решений в области ИБ. Эту точку зрения разделяет Михаил Лисневский. «ИБ-продукты становятся все сложнее. И вся цепочка — от внедрения до обслуживания — стала гораздо сложнее, — говорит он. — Чтобы выживать на этом рынке, необходимо постоянно быть в курсе, повышать квалификацию. Это касается как сферы продаж, так и технологий защиты. Недостаточно знать, для чего нужен тот или иной продукт, необходимо понимать, как он осуществляет защиту. Именно поэтому мы постоянно общаемся с вендорами, устраиваем для партнеров семинары, вебинары и работаем с демостендами. У нас фактически развернута демонстрационная ИТ-инфраструктура с виртуальными рабочими станциями, виртуальными пользователями. И мы на примере этой инфраструктуры показываем, к примеру, как защититься от утечек информации с помощью Symantec DLP. Мы показываем, как госструктуры могут получать удаленный доступ (защищенный по ГОСТу) к инфраструктуре, используя продукты, например, „Кода Безопасности". Мы знаем, как защищать. „Быть на гребне волны" — вот основное требование. Безопасность — это серьезно, а серьезные вещи требуют такой же подготовки».

Даниил Пустовой также отмечает, что в области ИБ в связи с большим разнообразием и усложнением решений и их специализации все востребованнее становятся услуги компаний, обладающих серьезными профессиональными аналитическими, консалтинговыми и интеграционными компетенциями. Заказчики на своих и чужих примерах знакомятся с высокими рисками работы с конфиденциальной информацией, становятся более информированными и разборчивыми, осознают, что универсальных средств защиты нет, а даже один единственный просчет в системе безопасности может легко свести все инвестиции на нет.

«В связи с этими изменениями значительно выросли требования к консалтинговым возможностям системных интеграторов, — говорит Андрей Зеренков. — Поэтому все чаще мы видим не разрозненные продажи отдельных продуктов, а комплексные проекты, охватывающие большое количество взаимосвязанных технологий». Кроме того, как уже было сказано, продолжается выход на российский рынок иностранных компаний, которые предлагают самые разные продукты и решения. Следовательно, выбор расширяется, и требования к специалистам также растут. Достаточно просто сделать выбор между двумя-тремя похожими продуктами, намного сложнее — из десятка разноплановых решений. И здесь вопрос доверия заказчика поставщику и производителю становится все более актуальным. И если решения ведущих производителей регулярно оцениваются международными аналитическими компаниями, то поставщикам нужны собственные весомые аргументы для завоевания клиентов, включая и подтверждение компетенций, и оперативную поддержку производителя в сложных ситуациях. Специалисты Safensoft также подчеркивают, что сейчас происходит переход от шаблонных

индивидуальному под-
ждом этапе цепочки
следствие этого уве-
требования вендоров
ьюторам, как марке-
так и сервисные.
ам Сергея Ласкина,
е системы защиты
ки всегда требуется
ть пилотный проект,
знить возможности
ных решений. Такой
лизуется силами
дистрибьютора
ра. Поэтому у каждо-
который работает
ыми решениями ИБ,
ыть квалифицирован-
алисты по многим на-
м. Когда выбор сделан,
бычно внедряет парт-
лять же требует на-
лифицированных спе-

ые требования к ком-
аботающим в сфере
тся неизменными и ак-
на протяжении деся-
ужно только приобре-
их применения, —
ячеслав Медведев. —
ь есть ряд проблем.
, решения в области
ИБ в основном продвигают небольшие компании, которые практически никогда не специализируются на безопасности и продают все подряд. Такие компании не могут позволить себе иметь выделенных специалистов по различным областям. Вторая проблема касается знаний. Многие вендоры ведут активную работу с партнерами и клиентами, но они не в силах изменить систему образования. Есть такой афоризм: в каждом вопросе должна содержаться половина ответа. Для того чтобы собрать, проанализировать и применить информацию, полученную от разных вендоров, нужен определенный базовый уровень знаний в области ИБ».

Опережающий рост сохранится

Как уже отмечалось, рынок ИБ всегда демонстрировал устойчивость во время кризисов и высокие темпы роста. Судя по прогнозам специалистов, у его игроков неплохие перспективы.

Ссылаясь на данные IDC, Владимир Мамыкин сообщил, что в Западной Европе доля ИТ-бюджета, расходуемого на ИБ, постепенно растет. Сейчас в большинстве компаний она составляет от 5 до 7%. Причем чем крупнее компания, тем больше она тратит на безопасность. В России этот показатель в несколько раз ниже — 1–2% ИТ-бюджета.

Владимир Мамыкин также подчеркнул, что тенденции и перспективы развития рынка ИБ определяются и обществом, и законодательством. Так, острая необходимость в безопасном хранении информации несколько лет назад стимулировала многие страны, в том числе и Россию, принять ряд законов. Здесь важным драйвером рынка ИБ вне всякого сомнения стало принятие закона о защите персональных данных. Кроме того, развитие различных направлений ИТ-индустрии, например облачных технологий и больших данных, а также трансформация существующих бизнес-концепций также требуют переосмысления современных средств защиты.

Несложно сделать вывод о том, что со временем российские компании приблизятся к европейскому уровню обеспечения безопасности, а значит, их расходы на покупку и внедрение новых систем могут вырасти в несколько раз. По словам Андрея Зеренкова, также ссылающегося на отчеты IDC, к 2017 г. общемировой рынок решений в области ИБ достигнет 42 млрд. долл., а среднегодовой рост ИБ-рынка в ближайшие четыре года составит 7,1%. Объемы увеличиваются, соответственно вырастет и прибыль партнеров. «Рынок ИБ растет значительно быстрее, чем рынок ИТ, поэтому перспективы самые радужные, — подчеркнул он. — Все новые тренды, такие как облака, мобильность, консьюмеризация, Интернет вещей, все подталкивают к мысли, что безопасность будет все более и более востребованной». Наталия Базаренко также считает, что российский рынок ИБ далек от насыщения. Об этом свидетельствует ежегодное увеличение продаж на 15%.

«О технологических трендах нынче не говорит только ленивый: мобильность, облака, виртуализация, большие данные. А вот перспективы развития на зрелом рынке, каковым я считаю рынок ИБ, теснейшим образом связаны с потребностями тех сегментов заказчиков, на удовлетворение которых нацелен именно ваш бизнес. Невозможно объять необъятное и кормить организации с разными потребностями и людей с разными вкусами одним и тем же блюдом. И это не зависит от кризиса. От кризиса зависит объем спроса и маржа, острота конкуренции и давления заказчика, — отмечает Наталия Тесакова. — И вне кризиса, и особенно во время компания, которая хочет развиваться и оставаться на рынке, на мой взгляд, должна сосредоточиться на том, чтобы быть полезной покупателям, предлагать востребованные сервисы и продукты. И в кризис и вне его выигрывает тот, кто в традиционных сегментах сумел выстроить отношения с ключевыми заказчиками, а также может предложить им не только типовые, но и уникальные решения, умеет сфокусироваться и сделать кое-что лучше других. В сбалансированном портфеле должны быть и типовые решения с приемлемым качеством по адекватной цене. Ну и, конечно, нужно постоянно искать (или создавать самим) ниши и сегменты, разрабатывая новые решения, до которых не додумались конкуренты».

Катажина Хоффманн-Селицка также считает, что ИТ-безопасность останется одним из самых перспективных сегментов. «Вендоры и партнеры должны прислушиваться к идеям друг друга и действовать более энергично, решительно, чтобы получать больший доход. Будут преуспевать те компании, которые готовы адаптироваться к изменениям и умеют находить новые возможности для развития своего бизнеса.

Самое главное — компаниям необходимо быть профессионалами в своем сегменте, специализироваться именно на том, что они умеют делать лучше других в этой отрасли, и постоянно развивать свои навыки».

«Если бизнес выстроен грамотно, то ИБ — достаточно прибыльный сегмент. Поэтому при правильной организации работа в сфере ИБ сможет вывести компанию в лидеры, — подчеркивает Михаил Лисневский. — Специализация компании эффективна всегда. Однако широкий портфель дистрибьютора удобнее для конечного пользователя. Поэтому лидером станет тот, кто нащупал „золотую середину“ — высокий уровень специализации и широкий продуктовый портфель». ■