За периметром

Идеальная ИБ-экосистема — это вектор, а не набор статичных решений, уверен руководитель направления продаж в УрФО компании ARinteg **Сергей Добронравов**

— Какой вызов вы назвали ключевым для российского ИБ-рынка?

— Как ни прискорбно, но им стала неблагоприятная экономическая ситуация. И это несмотря на значительный рост числа и эффективности атак. Принято считать, что в кризисное время работодатели склонны «закручивать гайки», что в теории должно выливаться в перераспределение ИТ-бюджета и дополнительные поставки средств защиты. Но на деле основная масса компаний решила «придержать» расходы до стабилизации экономической ситуации.

— Мировые эксперты в качестве ключевой тенденции и одновременно главной «головной боли» выделяют развитие BYOD и выход за корпоративный периметр безопасности. Актуально ли это для Урала?

— Действительно, размытие корпоративного периметра одна из ключевых проблем, не дающих спокойно спать сотрудникам отделов ИБ. Отсутствие контура безопасности как такового усложняет контроль за информационными потоками. Как показывает практика, отечественные (в том числе и уральские) компании исповедуют два противоположных подхода. Первый — все запретить. ИБ-специалисты многих организаций идут по пути «нет размытого периметра, нет проблемы». Второй подход — все разрешить. Эта идеология встречается в организациях с высоким уровнем мобильности сотрудников.

Причина полярности в том, что решения класса BYOD требуют немалых инвестиций, которые бизнес зачастую считает «слишком дорогой платой». К сожалению, только время покажет, сможем ли нащупать некое промежуточное состояние.

— Что может стать «локомотивом» рынка в таких сложных условиях?

— Сегодня обороты набирает безопасность АСУ ТП. Этот довольно крупный сектор пока находится в стадии формирования предложения. Драйвером его развития является государство. Первый шаг был сделан 14 марта 2014-го, когда был подписан 31-й приказ ФСТЭК (речь о документе, регулирующем требования к защите информации в АСУ ТП на критически важных, потенциально и особо опасных объектах. — *Ред.*). Уверен, что в ближайшие годы он перейдет в разряд обязательных к исполнению. Дело за малым — обеспечить предложение не только документально, но и технически.

— Как скажется на сфере ИБ курс на импортозамещение?

— На мой взгляд, от реализации этой политики однозначно выиграет сектор разработки программного обеспечения. В России есть софтверные ИБ-компании, способные разрабатывать продукты мирового уровня (например, Kaspersky Lab, InfoWatch, Аладдин Р.Д.).

В то же время в hardware-секторе пока особых прорывов нет. Отечественные производители не демонстрируют особого рвения к местным разработкам. Здесь можно увидеть различные интересные варианты «упаковки» зарубежных OEM-продуктов под лейблом «сделано в России».

— Какой вы видите идеальную ИБ-экосистему предприятия?

— Идеальная ИБ-экосистема есть вектор, как бы это странно ни звучало. Информбезопасность — очень динамичный сектор, который во многом обязан развитием киберпреступникам, постоянно наращивающим компетенции. Потому информбезопасность — это не набор статичных решений, это процесс.

Подготовил Сергей Ермак

в рублях, по оценке J'son & Partners Consulting, прирос на 13% к 2013-му.

— Рынок изменился неоднородно, — замечает Рустэм Хайретдинов. — Компании и банки, пострадавшие в 2014 году из-за повышения активности хакеров, вкладывают в безопасность даже больше, чем раньше. По нашим данным, ИБ-рынок в рублях прирос на 10 — 12%, но в основном за счет увеличения бюджетов в государственных и окологосударственных (нефтегаз, энергетика, госбанки) структурах. Быстрее остальных растут ненасыщенные ниши вроде DLP (Data Leak Prevention) и решений по защите от DDoS-атак.

Аналогичные оценки дает руководитель направления информационной безопасности компании «Открытые технологии» **Алексей Филатенков**: «Несмотря на кризис, предприятия закупки ИБ-средств не прекратили. Основными факторами, способствующими развитию рынка, стали новые требования регуляторов (например, закон о переносе обработки персональных данных россиян на территорию России). Наиболее быстрорастущим сегментом ИБ-рынка сегодня можно назвать внедрения в госсекторе, к которому требования законодательства применимы в полном объеме».

В среднесрочной перспективе представители ИТ-компаний не ожидают падения спроса на ИБ-решения. Большинство опрошенных нами топ-менеджеров склоняются к тому, что рынок будет медленно, но расти.

— Безопасность — это то, на чем буду экономить в последнюю очередь, — увере руководитель направления информацион ной безопасности компании «Крок» **Мих ил Башлыков**. — Поэтому динамика ра вития рынка должна быть позитивной. Е ли конкретизировать, то, безусловно, буде расти доля услуг и развиваться направле ние ИБ-аутсорсинга. Уже сейчас внешни подрядчикам активно отдают базовые зада чи по мониторингу защищенности инфра структуры и защите периметра.

Дополнительным драйвером разви тия российского ИБ-рынка может стат курс государства на импортозамеще ние. Информбезопасность — редкий се мент, в котором уже работают несколь компаний, предлагающих антивирусы криптосредства и системы предотвраще ния утечек мирового уровня (Kaspersky InfoWatch, Аладдин и другие), а также во дутся исследования в новых направлени ях (например УЦСБ работает над решени ями в области безопасности АСУ ТП и си стемой автоматизации управления безо пасностью организации). По оценке Ми хаила Башлыкова, сегодня отечественны решения закрывают около 40% потребно стей внутреннего рынка. То есть потенци ал велик. Правда, велики и риски. На ни указывает Дмитрий Огородников:

— Во-первых, на рынке информацион ной безопасности использовать полно стью отечественные решения мы може достаточно ограниченно. Во-вторых, мно гие отечественные продукты являются ли бо надстройкой над чем-то импортным, ли бо содержат в составе свободное ПО. Это по большому счету, несет те же риски, чт и импортные продукты.

А закончить нам бы хотелось двумя вы сказываниями. Они, как нам кажется четко отражают специфику текущего мо мента в области внешних угроз и отсыла ют нас к будущей ИБ-стратегии предпри ятий. Первое принадлежит Рустэму Хай ретдинову: «Сегодня большинство ата — комплексные, с привлечением соци альной инженерии и добавлением фак тора паники. Противодействовать им н уровне отдельных модулей нельзя, поэто му надо строить комплексную эшелони рованную оборону с мониторингом все возможных видов угроз».

Второе высказывание — гендиректор ГК «Хост» **Константина Суслова**: «Кибер преступность от вирусов, червей и трояно перешла к таргетированным атакам, вымо гательствам, хактивизму и промышленно му шпионажу. Мировые лидеры в област ИБ пытаются оперативно подстраиватьс под новые тенденции. Но в этой гонке зло умышленники будут всегда на шаг впере ди. Внедряя решения по безопасности про шлого поколения, компания отстает уже н