Российский ИБ-рынок: точки изменений

ВАЛЕРИЙ ВАСИЛЬЕВ

ОБЗОРЫ

Еще недавно Минэкономразвития РФ давал обнадеживающие прогнозы позитивных изменений в состоянии экономики России в 2016-м, но реалии наступившего года говорят об обратном. Эксперты предрекают длительный период низких цен на нефть, и уже на Гайдаровском форуме Дмитрий Медведев призвал готовиться к негативному развитию событий, если падение цен продолжится. Впереди — 10%-ное сокращение госбюджета по незащищенным статьям. Таким образом, рассчитывать на общее оживление рынка пока нет оснований.

Совершенно очевидно, что в такой ситуации тенденция к сокращению ИТ-бюджетов российских компаний, скорее всего, сохранится и в нынешнем году. Тем не менее у них остаются нерешенные ИТ-задачи, откладывать которые не всегда допустимо. А кроме того, появляются новые, обусловленные необходимостью защиты и общего повышения эффективности бизнеса, снижения капитальных и операционных расходов. Среди важнейших в общем списке задач по-прежнему значатся вопросы обеспечения информационной безопасности компаний и организаций, а также удовлетворения нормативных требований в этой области.

Какие задачи информационной безопасности были главными для ИБ-отрасли страны в прошлом году, какие предстоит решать заказчикам в первую очередь в наступившем, какие в связи с этим можно ожидать точки роста в различных сегментах российского ИБ-рынка? Всё это мы намерены обсудить в данном обзоре с участием экспертов.

Главные изменения в области ИБ в 2015 г.

Экономика и ИБ. "Нынешние политико-экономические условия, с одной стороны, привели к стагнации рынка ИБ, а с другой, помогают его оздоровлению. В итоге преимущества получают потребители, поскольку возрастающая конкуренция среди поставщиков обещает им ИБ-продукты с улучшенным функционалом и по более низким ценам" — так заместитель генерального директора компании "Аладдин Р.Д." Алексей Сабанов охарактеризовал текущую ситуацию в ИБ-сфере.

Кризис, по его мнению, способствует тому, что на ИБ-рынке останутся наиболее высокотехнологичные и перспективные решения, для разработки которых были вовремя созданы научные и производственные заделы. Среди подобных он выделяет поддержку юридической значимости электронных документов, в том числе в сегменте M2M, создание доверенных платформ и решений на их основе, комплексное управление безопасностью.

Вместе с тем, по словам Григория Васильева, менеджера по продуктам НИИ СОКБ, "…в сложной экономической ситуации, как всегда, пользователи больше внимания уделяют не приобретению новых продуктов, а повышению эффективности использования ранее внедренных, а также внешним сервисам ИБ". При этом он отмечает заметное смещение ИБ-рынка в сторону услуг, что, по его мнению, обусловлено как общими технологическими тенденциями в ИТ и ИБ, так и тактическим стремлением заказчиков снизить затраты, отложив приобретение программного и аппаратного обеспечения до лучших времен.

В том же ключе высказываются и некоторые другие эксперты. Констатируя, что потребность российских пользователей в ИБ-услугах в прошлом году не снизилась, директор Центра информационной безопасности компании "Инфосистемы Джет" Алексей Гришин отмечает, в частности, растущий интерес банковского бизнеса к услугам по обеспечению ИБ в вебе, по защите интернет-банкинга и ДБО, по противодействию DDoS-атакам, организации межсетевого экранирования на уровне приложений и борьбе с транзакционным мошенничеством.

О резком увеличении спроса на ИБ-сервисы и услуги по сопровождению ИБ-систем при одновременном росте разнообразия востребованных ИБ-услуг говорит и технический директор компании "Информзащита" Иван Мелехин, что, по его мнению, обусловлено повышением уровня зрелости российских заказчиков.

В числе услуг, пользующихся растущим спросом, Андрей Перкунов, руководитель направления ИБ компании "Стэп Лоджик", отмечает консалтинговые ИБ-услуги, направленные на практическое решение вопросов защиты данных, выявление и устранение случившихся инцидентов: тесты на проникновение, расследование инцидентов, обеспечение успешного прохождения проверок у регуляторов, приведение ИТ- и ИБ-инфраструктуры в соответствие нормативным требованиям.

Прямо противоположного мнения, однако, придерживается генеральный директор компании "Код безопасности" Андрей Голов. Он считает, что распространение ИБ-услуг и ИБ-аутсорсинга для России в настоящее время не характерно и сдерживается стремлением пользователей ограничить обработку критически важных данных периметром организации: "Я думаю, что ИБ-аутсорсинг и ИБ-услуги — это пока не для нашей страны. В силу специфики российского бизнеса никто не готов отдавать на сторону вопросы обеспечения своей информационной безопасности. Чтобы пойти на это, либо надо быть крайне неосмотрительным, либо размеры бизнеса должны быть несущественными для его владельца".

Импортозамещение. Курс на импортозамещение заставляет российских заказчиков отказываться от зарубежных продуктов в пользу отечественных, что для российских ИБ-вендоров, по мнению г-на Васильева, стало серьезной встряской: "Выяснилось, что не все готовы полностью заменить зарубежные аналоги, а некоторые иностранные продукты просто не имеют российских альтернатив. Тем не менее это полезный шок, который заставляет активнее развивать отечественные решения, доводить их до ума и до массового промышленного применения".

"На фоне ужесточения регулирования по модели "закручивания гаек" кажется парадоксальным сокращение закупок сертифицированного ПО. С одной стороны, в условиях курса на импортозамещение ряд отечественных производителей демонстрирует неготовность снижать цены ради повышения объемов продаж, а с другой — ввиду позднего [календарного] формирования бюджетов, видимо, запоздали некоторые закупочные конкурсы. Тем не менее выскажу предположение, что ИБ-рынок будет пополняться новыми агрессивными игроками, способными на демпинг, и в ближайшие год-два цены на нем могут стать рыночными", — комментирует влияние импортозамещения на российский рынок ИБ г-н Сабанов.

Со своей стороны директор по развитию бизнеса компании "Перспективный Мониторинг" Роман Кобцев отмечает повышение активности российских ИБ-разработчиков в прошлом году: "Отечественные производители в первую очередь постарались заполнить традиционно удерживаемый международными лидерами емкий сегмент средств мониторинга ИБ".

Кроме того, по наблюдениям Вячеслава Медведева, ведущего аналитика отдела развития компании "Доктор Веб", импортозамещение подвигло многие российские компании, ранее использовавшие зарубежное ПО, к переводу своих инфраструктур на отечественные аналоги. В то же время, считает эксперт, не получила развития тенденция создания такого отечественного ПО, которое могло бы заменить импортное, превосходящее отечественное по функционалу либо вовсе не имеющее аналогов.

Алексей Сабанов обращает внимание также на следующие издержки политики импортозамещения: "Несмотря на то что значительная часть государственных баз данных по-прежнему остается недостаточно защищенной, объем продаж в сегменте средств защиты данных снизился". Он объясняет это нежеланием заказчиков тратить средства на защиту того, что в скором времени им нужно будет переносить на другие платформы.

ИБ как зеркало ИТ. ИБ-рынок зависит от рынка инфотелекоммуникационных технологий, уверены наши эксперты: всё, что происходит в ИКТ, отражается на рынке ИБ.

Так, развитие рынка интернет-услуг вызвало, по словам г-на Медведева, рост интереса со стороны бизнеса к защите сайтов. Сформировавшийся, как он считает, за прошедший год рынок 3D-печати требует создания 3D-моделей и систем контроля их качества в плане ИБ.

Как отдаленную перспективу для нашей страны г-н Голов видит развитие ИБ мобильных решений и облачных структур, подчеркивая при этом, что средства защиты мобильных устройств доступа нужно делать по возможности массовыми, чтобы производители смогли зарабатывать больше денег.

Оппонируя ему, г-н Васильев отмечает: "Уже есть российские средства криптографической защиты для различных [мобильных] платформ, отечественные системы MDM для управления ИБ-политиками на мобильных устройствах, решения, предоставляющие офисный инструментарий для безопасной работы. Это все зрелые продукты, опробованные в реальных проектах по отдельности и в комплексе. Серьезные усилия прилагаются сегодня для появления доверенной мобильной ОС и отечественной мобильной аппаратной платформы. Так, успешно сертифицирована во ФСТЭК мобильная ОС Tizen, а компания Yota Devices заявила о переводе производства YotaPhone2 в Россию".

Мнение главного инженера представительства Citrix в России и странах СНГ Сергея Халяпина по поводу развития технологий ИБ для мобильного доступа в нашей стране тоже не совпадает с рассуждением г-на Голова. На его взгляд, технологии защиты мобильных устройств и мобильных приложений в прошлом году развивались активно, что однозначно связано с глубоким проникновением мобильных устройств в корпоративную среду, использованием персональных устройств для рабочих целей и хранения на них корпоративных документов. "Возможности для сотрудников работать мобильно и удалённо с корпоративной информацией привлекают внимание заказчиков к решениям по защите соответствующих каналов передачи данных", — утверждает он.

На ИТ-индустрию, как отмечает Андрей Перкунов, значительное влияние сейчас оказывают технологии программно-конфигурируемых сетей, виртуализации и облачных решений. "В ближайшие три-пять лет следует ожидать значительной трансформации ИТ, к которым придется адаптировать решения и технологии ИБ. Уже сейчас ведущие поставщики ИБ-решений пересматривают свои продуктовые портфели с тем, чтобы улучшить интеграцию ИБ-продуктов с виртуальными средами, платформами оркестровки сервисов и облачными системами", — считает он.

Отдельного внимания, по мнению г-на Гришина, заслуживают тенденции, связанные с активно использующим АСУ ТП промышленно-энергетическим ▸

Наши эксперты

ГРИГОРИЙ ВАСИЛЬЕВ, *менеджер по продуктам, НИИ СОКБ*

АНДРЕЙ ГОЛОВ, *генеральный директор, "Код безопасности"*

АЛЕКСЕЙ ГРИШИН, *директор Центра информационной безопасности, "Инфосистемы Джет"*

СЕРГЕЙ ЗЕМКОВ, *управляющий директор в России, странах Закавказья и Средней Азии, "Лаборатория Касперского"*

РОМАН КОБЦЕВ, *директор по развитию бизнеса, "Перспективный Мониторинг"*

ВЯЧЕСЛАВ МЕДВЕДЕВ, *ведущий аналитик отдела развития, "Доктор Веб"*

ИВАН МЕЛЕХИН, *технический директор, "Информзащита"*

АНДРЕЙ ПЕРКУНОВ, *руководитель направления ИБ, "Стэп Лоджик"*

АЛЕКСЕЙ САБАНОВ, *заместитель генерального директора, "Аладдин Р.Д."*

СЕРГЕЙ ХАЛЯПИН, *главный инженер, представительство Citrix в России и странах СНГ*

комплексом и характеризующиеся “законсервированным” спросом, который формируется под воздействием ожидаемого изменения статуса нормативных документов для этой области с рекомендательного характера на обязательный (предположительно, по его оценкам, это произойдет в 2016 г.). “Практически все российские промышленные предприятия активно изучают этот вопрос и потенциально готовы в случае утверждения данных нормативов как обязательных инициировать соответствующие проекты”, — сообщил он.

“Идет переход к реальному, а не “бумажному” обеспечению ИБ, — констатирует г-н Мелехин. — Заказчики все чаще проводят анализ защищенности своих ИКТ-инфраструктур и данных. Все чаще предлагается к обсуждению тема обеспечения ИБ в технологических процессах. Эти вопросы актуальны для целого ряда секторов экономики, и уже есть решения, которые помогают предотвратить угрозы, связанные с автоматизацией технологических процессов”.

Влияние ландшафта угроз. Эксперты обращают внимание на превращение киберпреступности в высокотехнологичный, отстроенный по современным экономическим схемам криминальный бизнес. Киберпреступники оперативно реагируют на все изменения, происходящие в ИКТ-сфере, примером здесь может служить оперативное реагирование киберкриминалитета на смещение в Интернет розничных продаж, банковского и других видов бизнеса.

Вот какие данные привёл г-н Гришин: “По экспертным оценкам нашей компании, в кредитно-финансовой отрасли объем потерь от мошеннических действий в 2015 г. по сравнению с 2014-м увеличился в среднем на 26,8%, в телекоммуникационном секторе — на 6,8%, в ритейле — до 16% в зависимости от сегмента. Поэтому проекты по развитию как интернет-сервисов, так и программ лояльности должны сопровождаться внедрением средств и мер по защите платежных транзакций и пользовательских аккаунтов, а также по предотвращению внешнего и внутреннего мошенничества. Можно с уверенностью ожидать роста количества подобных проектов в 2016 г.”.

Примерно с прошлой осени г-н Голов отмечает рост внимания в России к таргетированным атакам: “Они существовали всегда, но сегодня увеличилось число профессионалов, которые умеют эти атаки реализовывать, причем таким образом, что стал заметен ущерб от них”.

Стремление снизить ущерб от таргетированных атак стимулирует спрос на средства консолидации ИБ-данных, мониторинга и централизованного управления ИБ. Как следствие, растет потребность в услугах центров управления безопасностью (SOC) и средствах аналитики ИБ (Security BI). “Специалисты стали задумываться над тем, что же в принципе происходит с корпоративной ИБ, как измерять её уровень, детектировать и коррелировать ИБ-события”, — отмечает г-н Голов.

Алексей Гришин отмечает резкий рост кроссканального мошенничества, атак на клиентов организаций с использованием социальной инженерии. В сфере классической корпоративной ИБ фокус, по его мнению, сместился в сторону модернизации инфраструктурной ИБ и использования высокоинтеллектуальных средств защиты. Основной акцент сосредоточен при этом на том, что и как можно делать с данными, поступающими от имеющихся ИБ-инструментов — IdM, DLP, SOC и др., — т. е. на выстраивании вокруг этих систем процессов, которые при небольших (относительно) вложениях привнесут новое интеллектуальное качество в ИБ.

Существенно повысилась, по мнению г-на Гришина, актуальность появившихся на российском рынке еще пару лет назад специализированных аналитических систем (как отечественных, так и зарубежных), позволяющих по определенным логам в ИТ-системах (таких, как ERP, CRM и т. п.) выявлять случаи мошенничества, обмана, воровства в торговых сетях.

Некоторые из российских ИБ-вендоров видят для себя новые возможности в сегменте решений класса Anti-APT (защита от целевых атак). К числу таких компаний, как сообщил Сергей Земков, управляющий директор “Лаборатории Касперского” в России, странах Закавказья и Средней Азии, относится и та, которую он представляет.

Согласно наблюдениям г-на Медведева, важной тенденцией прошедшего года стал рост интереса злоумышленников к системам на основе ОС Linux, к решениям по управлению технологическими АСУ — всему тому, что раньше или не защищалось вовсе, или защищалось крайне слабо. Количество взломов таких систем в прошлом году было невелико, но, по его прогнозам, оно будет расти, в том числе по мере подключения “умных” устройств к Интернету.

Хотя Интернет вещей не стал пока актуальным для России, наши эксперты считают необходимым готовиться к его вызовам уже сейчас, прорабатывая сценарии защиты его инфраструктуры. Вячеслав Медведев заявляет, что рынок носимой и встраиваемой электроники, “умных” устройств, оборудования и комплексов формируется непосредственно у нас на глазах и уже требует защиты, так как злоумышленники оценили его потенциал.

“Современное общество стоит на пороге перехода в состояние, которое ранее считалось фантастикой, — утверждает он. — Совсем скоро нас будут окружать устройства, контролирующие каждое наше действие в любой момент времени, и далеко не все из них будут создаваться и использоваться во благо тех, кого они будут контролировать”.

Поскольку именно человек является слабым звеном в любой системе ИБ, важными и востребованными, как утверждает г-н Земков, оказались сервисы по обучению специалистов и программы повышения осведомленности персонала в вопросах ИБ, предложенные заказчикам представляемой им компанией.

Прогнозы на 2016 год

Вячеслав Медведев с сожалением отмечает, что, по его наблюдениям, многие специалисты в нашей стране считают задачу защиты от злоумышленников и вредоносных программ давно решенной. Это, однако, не подтверждается практикой: системы антивирусной защиты, например, в подавляющем большинстве российских компаний оставляют желать лучшего и не защищают от современных угроз. Как правило, это является следствием того, что и руководители компаний не уделяют должного внимания организации защиты в этой области. “ИБ-риски оцениваются российским бизнесом как пренебрежимо малые. Во многом это обусловлено “режимом умолчания” в отношении ИБ-инцидентов в нашей стране, из-за чего складывается впечатление, будто количество инцидентов мало, а размер денежных потерь от них невелик. Между тем накопленная нашей компанией экспертиза в области анализа таких инцидентов свидетельствует об обратном”, — говорит он.

Влияние политико-экономической ситуации. По мнению г-на Мелехина, неопределенность экономической ситуации в нынешнем году не позволяет корректно делать какие-либо прогнозы изменения состояния ИБ-рынка страны. Тем не менее наши эксперты высказались по поводу некоторых наиболее очевидных, по их мнению, тенденций в области ИБ.

Заказчики в условиях секвестирования бюджетов и сокращения штатов, предупреждает г-н Сабанов, будут более требовательны к функционалу и стоимости закупаемых (увы, во все меньших объемах) ИБ-продуктов и особенно к исполнителям ИБ-проектов. “Они будут требовать единого поставщика продуктов и услуг по всему спектру сформулированных ими ИБ-задач при повышенной ответственности интегратора за жизненный цикл ИБ-систем. Это приведет к обострению конкуренции среди интеграторов, к расслоению поставщиков услуг и очередному переделу ИБ-рынка. При этом в выигрыше помимо крупнейших интеграторов окажутся разработчики, предугадавшие конкретные направления его развития”, — полагает он.

По мнению г-на Голова, ИБ-бюджеты будут формироваться только на основе ситуационного реагирования заказчиков, а нынешняя экономическая ситуация хуже, чем была в кризис 2008 г., поскольку нынешний кризис имеет политико-экономический характер. “Наслоилось много негативных факторов. Разрушились экономические связи, введены санкции, происходит падение биржевых котировок, падение курса национальной валюты. Поскольку у государства нет четких стресс-сценариев, прогнозы строить сложно”, — соглашается он, выражая, однако, уверенность в том, что направления, связанные с обороноспособностью страны, будут развиваться и гособоронзаказ будет расти.

Хотя Интернет вещей не стал пока актуальным для России, эксперты считают необходимым готовиться к его вызовам уже сейчас, прорабатывая сценарии защиты его инфраструктуры.

Поскольку экономия на ИБ таит в себе большие риски, игнорировать стоящие перед компаниями и организациями ИБ-вызовы можно лишь до определенного предела. Иван Мелехин полагает, что стабильность или даже рост могут показать те направления, которые позволят оптимизировать затраты, увеличить доходность основного бизнеса, защитить критически важные активы. “Можно ожидать роста востребованности сервисно-облачной модели ИТ и ИБ, которая позволяет получать только необходимые для обеспечения ИБ ресурсы, причём в нужное время”, — предполагает он.

Если оценивать ИБ-рынок в показателях, не привязанных к курсу рубля (например, по общему количеству проектов или человеко-дней), то, по мнению г-на Гришина, российский рынок ИБ в 2016 г. вырастет, а сегмент аутсорсинга — даже в разы. Он ожидает увеличения ИБ-бюджетов в топливно-энергетическом комплексе: здесь, как правило, ИБ-проекты связаны с переводом ранее созданных ИБ-подсистем на российские продукты или с созданием высокотехнологичных подсистем с нуля.

Импортозамещение и ИБ. Негативное влияние на ИБ-бюджеты существенного снижения курса рубля (поскольку цены на импортируемые решения исчисляются в иностранной валюте) играет на руку отечественным поставщикам, и тема импортозамещения в 2016 г., как считают наши эксперты, будет особенно актуальна.

По мнению г-на Васильева, в пользу импортозамещения сказывается недоверие российских заказчиков к иностранным вендорам в связи с имеющими место политическими процессами, а также снижением их активности в нашей стране как по политическим, так и по экономическим причинам. “Для российских ИБ-разработчиков и поставщиков услуг, — говорит он, — складываются уникальные, практически “тепличные” условия, которыми необходимо воспользоваться”.

Цикл появления новых отечественных ИБ-продуктов сегодня существенно сократился, констатирует г-н Гришин, так как заказчики стали покупать и внедрять перспективные решения и вкладываться в их развитие, вынуждая разработчиков дополнять свои решения и продукты нужными свойствами и доводить их до необходимого заказчикам уровня. При этом заказчики и интеграторы принимают на себя риски, связанные с внедрением незрелых решений.

Регулирование и ИБ. Регулирование, по мнению некоторых экспертов, остается одним из важнейших движителей российского рынка ИБ.

“Сообщество специалистов и пользователей, — говорит г-н Кобцев, — по-прежнему ждет закона, регулирующего ИБ критически важных информационных инфраструктур, поскольку специалистам необходимо понимание процессов развития как системы ГосСОПКА, так и систем защиты промышленных АСУ. Возможно, некоторое влияние на рынок окажет ожидаемый в этом году стандарт безопасной разработки СЗИ, который продвигает ФСТЭК России. Конечно, локомотивом он не станет, но как минимум свежую струю в обсуждения внесет и, возможно, через несколько лет преобразуется в какой-то более обязательный документ…”

Большие перспективы, по мнению г-на Васильева, перед российскими вендорами открываются в связи с требованиями регуляторов осуществлять сбор и уточнение персональных данных на территории страны.

Технологические и маркетинговые локомотивы ИБ. Динамика расходов на ИБ, как утверждает г-н Гришин, в наступившем году будет ощутимо различаться в разных отраслях экономики. Банки, например, сокращают свои ИБ-бюджеты — поступать так позволяет им запас прочности, накопленный благодаря сделанным ранее вложениям. Зато инвестируются те направления ИБ, которые наиболее критичны на данный момент. К первоочередным, на его взгляд, относится обеспечение ИБ в вебе.

Определенная активность отмечается, согласно наблюдениям г-на Кобцева, и в традиционно “российских” сегментах рынка ИБ, что связано с переходом игроков от разработки отдельных продуктов к созданию комплексных инфраструктур заказчиков. Отечественные производители, ожидает эксперт, в 2016 г. будут и дальше усиленно наращивать функциональность своих средств сетевой безопасности в направлении NGFW и полноценных ИБ-продуктов для защиты конечных точек, увязываемых (впоследствии) с экспертной (чаще облачной) поддержкой. “Некоторые российские разработчики уже в 2015 г. практически завершили этот процесс, другие только приступили к нему. Но в любом случае наступивший год станет показательным в конкурентной борьбе по этому направлению, потому что высвобождающиеся в результате импортозамещения и других рыночных событий (слияний, поглощений, изменений в стратегии развития некоторых вендоров) доли рынка быстро заполняются”, — считает он.

Другим интересным трендом, по мнению г-на Кобцева, станет увеличение количества российских ИБ-компаний, пытающихся выйти на международные рынки, что в значительной степени связано со стагнацией рынка российского: “Думаю, стратегии такого выхода и результаты у всех будут разные. Но в любом случае будет интересно за этим понаблюдать”.