"Необходимость в ИБ-интеграции продиктована сложностью ИБ-проектов"

Зеленоградскую компанию "ЭЛВИС-ПЛЮС" можно считать старожилом российского ИТ- и ИБ-рынка: в конце 2011-го она отметила свой 20-летний юбилей (www.pcweek.ru/business/article/detail.php?ID=135505). В последнее время компания активно развивалась и, по предварительным данным, в 2011 г. по обороту вышла на показатель 1 млрд. руб.

Своими оценками текущей ситуации на рынке информационной безопасности (ИБ), итогов развития интеграционного направления в этой области за прошедший год, а также перспектив в сфере ИБ на ближайшее будущее поделился генеральный директор "ЭЛВИС-ПЛЮС" ***Виктор Лебедев****.*

Виктор Лебедев

К каким изменениям рынка системной ИТ-интеграции привела тенденция заниматься обеспечением ИБ непосредственно в ходе ИТ-проектов, по возможности интегрируя средства защиты в ИТ-инфраструктуру, а не внедряя наложенные решения через специализированные ИБ-проекты?

Включение требований ИБ в ИТ-проекты сделало такие проекты комплексными. Помимо технического усложнения это, как правило, увеличивает число участников как со стороны заказчиков (их интересы в проекте представляют разные структуры — в первую очередь, учитывая специфику рассматриваемых проектов, это ИТ- и ИБ-службы), так и со стороны исполнителей, что усложняет проекты организационно. На стороне заказчиков, как правило, управление проектом в целом не ведется, и этим вынуждены заниматься мы — интеграторы.

Успех проекта теперь зависит от взаимодействия привлеченных к его выполнению ИБ-интегратора и ИТ-интегратора. Если же решение задач ИБ заказчик делегирует исключительно ИТ-интегратору, то от его компетентности в области ИБ зависит результат проекта в целом.

В любом варианте актуальной является способность генерального подрядчика грамотно управлять проектом. В практике нашей компании, например, есть ИБ-проект, в котором количество привлеченных (узкоспециализированных) субподрядчиков достигало пяти компаний.

Какой из двух упомянутых сценариев сегодня встречается чаще?

Крупные ИТ-интеграторы имеют собственные специализированные ИБ-подразделения, что позволяет им многие проекты выполнять своими силами . Однако кризис 2008 г. привел к тому, что некоторые интеграторы стали избавляться от непрофильных активов, в результате чего их ИБ-подразделения подверглись существенным сокращениям. Таким образом, начал формироваться пул специализированных ИТ- и ИБ-интеграторов, не стремящихся к расширению своих компетенций на смежные области и способных выполнять в кооперации ИТ-проекты любой сложности.
В основном же выбор сценария ИТ-проекта зависит от доверия заказчика к привлеченному исполнителю. У каждой структуры заказчика, заинтересованной в успехе проекта, есть свои профессиональные и партнерские предпочтения, и они с гораздо большей готовностью привлекут те компании, с которыми знакомы по совместной работе. Эти компании уже знают особенности инфраструктуры заказчика, его методы, технологии, системы защиты, а потому априори имеют возможность оказаться эффективными исполнителями проекта.

Кто же он такой — российский интегратор информационной безопасности? Каков его бизнес-портрет?

Необходимость в ИБ-интеграции продиктована прежде всего сложностью обеспечения ИБ в современных условиях. Задачи создания систем защиты информации сегодня ничуть не проще создания систем информационных. Говорить об ИБ-интеграторе вообще трудно. Легче составить представление о них, обсуждая конкретные проекты — разработку документации, консалтинг, создание конкретной ИБ-системы и т. п. Если у заказчика есть потребность в таком проекте, то круг исполнителей, способных его выполнить, в стране известен довольно точно. Среди них — и крупные ИТ-интеграторы со своими ИБ-подразделениями, и универсальные, и узкоспециализированные ИБ-интеграторы. Проводить между ними жирную разделительную черту я не стал бы.

Что же касается некоторых общих черт, присущих всем ИБ-интеграторам, то прежде всего давайте отметим, что каждый из них работает на ИБ-рынке. Рынок этот я характеризую как довольно закрытый и регулируемый намного сильнее, чем ИТ-рынок в целом. У него есть свои специфические требования, свои регуляторы, лицензиары и лицензиаты, есть регламенты использования на стороне заказчика конкретных подсистем защиты.

Те компании, которые взаимодействуют со всеми участниками ИБ-рынка — заказчиками, регуляторами, производителями, интеграторами — и которые в состоянии наиболее полно выполнить все вышеупомянутые требования, я бы и назвал ИБ-интеграторами.

ИТ-интегратор, как правило, сильно уступает ИБ-интегратору в вопросах взаимодействия с регуляторами — он не всегда может компетентно объяснить, чем продиктовано то или иное нормативное требование. Чаще всего он занимает такую позицию: сформулируйте свои требования сами — и я их выполню. Компетентность ИБ-интегратора позволяет ему корректировать требования заказчиков в целях повышения эффективности ИБ-проекта.

Можно ли утверждать, что упомянутая выше тенденция обеспечивать ИБ непосредственно в ходе ИТ-проектов нивелировала остроту противоречий между требованиями ИТ и ИБ?

У заказчика противоречия между ИТ- и ИБ-направлениями рождаются как противоречия между его службами ИТ и ИБ, возникающие при формулировании требований к параметрам систем и режимам их эксплуатации. Идеальная с позиций ИТ информационная система обеспечивает доступ ко всем своим ресурсам для всех, а мнение об идеальной системе у ИБ-специалистов диаметрально противоположное.

Помимо принципиальных, я бы сказал, диалектических противоречий в требованиях со стороны этих двух служб к назначению ИТ есть и куда более прагматичные и, кстати, превалирующие аспекты, как, например, борьба за бюджеты, которые у заказчиков уже разделены.

Что же касается рынка в целом, то тут идет борьба за коммерческие интересы между участниками рынка, в том числе между ИТ- и ИБ-интеграторами. У каждой стороны своя объективная и субъективная аргументация собственных преимуществ в борьбе за заказчика.

Эту коллизию всякий раз разрешает сам заказчик — именно он определяет, какой должна быть реализуемая система. Невозможно не упомянуть, что на позицию заказчика влияет регулирование ИБ. Сегодня это в первую очередь закон "О персональных данных".

Спрос на системы защиты персональных данных породил немало недобросовестных, недостаточно компетентных фирм, которые тем не менее тоже называют себя ИБ-интеграторами. Поскольку закон "О персональных данных" затрагивает миллионы компаний, большая часть которых не имеет должного опыта в области защиты информации, нередко подобных квазиинтеграторов воспринимают как гуру. Их присутствие на рынке приводит к появлению эрзац-продуктов и эрзац-услуг, так как только квазиинтеграторы могут выполнять заказы по диктуемым ими демпинговым ценам, которые ниже среднерыночной себестоимости. В результате у заказчиков, идущих у этих "гуру" на поводу, оказываются измененными привычные бизнес-процессы, а защиты как не было, так и нет.

Чего же все-таки в регулировании ИБ больше — плюсов или минусов?

Упомянутый закон уже несколько лет является основным драйвером рынка, поэтому отношение к нему со стороны интеграторов очевидно положительное. С позиций заказчиков, оценка влияния этого закона неоднозначна. С одной стороны — требования закона являются ограничением и обременением для бизнеса и поэтому воспринимаются негативно. С другой стороны, давайте посмотрим как на пример на требования к оформлению налоговой отчетности. Компании к ним давно привыкли, а собственники бизнеса научились использовать эту отчетность для оценки состояния дел. Нечто похожее происходит в отношении требований к защите информации.

Упомянутый закон во многом уже соответствует Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Это упрощает для российских компаний международное общение, в том числе и трансграничную передачу данных. Ну а внутри страны, отвечая за соблюдение конституционных прав граждан, государство просто обязано принимать меры к защите этого рода личной информации.

Есть мнение, что закон навязывает способы защиты персональных данных. Я так не считаю. Операторам персональных данных следует грамотно различать, что от них требуется для выполнения закона, а что только рекомендуется. Так, в законе говорится об оценке соответствия его требованиям. А ее можно проводить несколькими способами: декларацией, приемо-сдаточными испытаниями и сертификацией. Есть из чего выбирать. Однако нужно грамотно оценивать трудоемкость и стоимость каждого способа в каждом конкретном случае. Вполне может получиться, что без использования сертифицированных средств оценка соответствия системы защиты персональных данных окажется столь же сложной и дорогой, как ее сертификационные испытания. Опыт показывает, что использование сертифицированных средств для заказчика выгоднее во всех аспектах. Кстати, сегодня на рынке доступны самые современные ИБ-средства, сертифицированные в соответствии с требованиями этого закона.

Однако повторю: оптимальный способ оценки соответствия зависит от конкретной ситуации у конкретного заказчика. В практике нашей компании есть созданные нами системы защиты персональных данных, от аттестации которых заказчик отказывался, ограничиваясь только нашей декларацией ее соответствия требованиям закона "О персональных данных", и после этого успешно проходил проверку Роскомнадзора.

Как правило, при проверках заказчики сами взаимодействуют с регуляторами. Вместе с тем по их просьбе мы тоже можем подключаться к проверкам — помогаем им обосновать свою позицию вплоть до обращений в прокуратуру.

Среди клиентов "ЭЛВИС-ПЛЮС" более 40% относятся к госсектору. Что-нибудь изменилось за прошлый год в работе с ними по направлению ИБ?

Во-первых, нужно отметить, что для госорганизаций основным драйвером в области ИБ сегодня является не закон "О персональных данных". Вместо него эту задачу выполняет ряд постановлений и указов руководства страны, определяющих порядок межведомственного взаимодействия и оказания государственных услуг в электронной форме (на которую, согласно указу президента страны, госструктурам надлежало перейти с июля прошлого года). Они вызвали очень интересные процессы в области обеспечения ИБ в государственных организациях и предприятиях, наиболее примечательные из которых относятся к защите не закрытой, а открытой информации — обеспечению ее достоверности и доступности. Ведь известны случаи изменения содержимого страниц даже на президентском сайте.

При оказании госуслуг в электронном виде, когда персональные данные граждан начинают передаваться по различным ведомственным локальным сетям и Интернету, предстоит решить задачу соответствия закону "О персональных данных" межведомственного документооборота. Не менее остро стоит проблема технологического и организационного согласования ведомственных информационных систем между собой. Известно, что построены они в том числе и в сфере обеспечения ИБ, на базе совершенно разных продуктов и разными интеграторами.

Если говорить об изменениях в области ИБ в госсекторе, то в силу упомянутых причин ИБ-проекты там стали масштабнее и существенно превышают по объемам проекты в коммерческих организациях. На ИБ в госструктурах сказывается также длительное недофинансирование ИБ-направления, в результате чего они сильно отстали от коммерческих фирм и многие ИБ-задачи там приходится решать с нуля. Да и проблема с ИБ-кадрами в госструктурах стоит острее, нежели в частном бизнесе. К тому же изначально отношение к защите информации в государственном секторе было более формальным: на первом плане выполнение требований регуляторов, а не борьба с реальными утечками информации.

АРХИВ@ЭЛВИС