Системы защиты информации: проблема выбора исполнителя сегодня и завтра

А.Березин, ОАО «ЭЛВИС+»

В последнее время в компьютерной прессе оживились споры о том, какой тип компании предпочтителен для заказчика в качестве исполнителя работ по построению систем защиты информации (СиЗИ): системный интегратор (СИ), занимающийся построением собственно самой автоматизированной системы (АС) заказчика (в широком смысле), или специализированная компания (СК), бизнес которой ограничен исключительно областью обеспечения информационной безопасности (ИБ)? Пример подобной дискуссии приведен в последнем обзоре российского рынка ИБ, подготовленном агентством «Росбизнесконсалтинг» в сентябре 2001 года (см. http://www.cnews.ru/comments/security/). Этот вопрос, действительно, не только интересен сам по себе, но и вполне актуален уже для многих заказчиков, учитывая рост интереса к области ИБ в России в целом.

Итак, основным доводом в свою пользу со стороны СИ является тезис о том, что СиЗИ ни на техническом, ни на организационном уровнях неотделима от АС и потому невозможно построить СиЗИ без знания той самой АС, которую необходимо защищать. СК, наоборот, утверждают, что, поскольку защита информации у СИ – не основной бизнес, они не имеют возможности уделять ему достаточное количество ресурсов, опыт сотрудников недостаточен и, по этой причине, качество реализуемых СиЗИ не так высоко (в отличие от цен).

С нашей точки зрения, здесь следует оговорить еще один важный момент, который заключается во внутреннем противоречии решаемых задач. Он состоит в том, что задачи, которые решает СиЗИ практически всегда стоят в противоречии с задачами, которые должна решать АС в интересах пользователя. Действительно, самый лучший способ защиты – «выключить» АС - и тогда информация будет в полной сохранности («если у Вас нету друга, Вам его не потерять…»). Но такой вариант вряд ли устроит заказчика. Поэтому, если в качестве исполнителя работ по построению СиЗИ выбран СИ, можно с большой долей уверенности сказать, что возникшее противоречие будет решено в пользу АС в ущерб качеству СиЗИ. Аналогично, с другой стороны, если доверить построение СиЗИ СК, то система защиты будет вносить массу неудобств в работу пользователей АС и море «головной боли» для администраторов.

Но заказчику, тем не менее, необходимо делать выбор!

Нам кажется, что искать ответ на поставленный выше вопрос целесообразнее не в ходе «перетягивания каната» - чей подход лучше? – а взглянув, собственно, на сам объект спора – СиЗИ. Начнем с выдвижения очевидного, с нашей точки зрения, тезиса: СиЗИ – это СИСТЕМА, следовательно, как любая система, она развивается по известным законам. Очень грубо развитие любой системы можно разбить на три этапа:

1) возникновение отдельных элементов будущей системы, которые имеют тенденцию к качественному и количественному росту;
2) возникновение многочисленных связей между отдельными элементами, качественный рост которых ведет, собственно, к появлению самой системы;
3) эволюционный рост системы, который заканчивается либо ее превращением в сверхсистему (путем «поглощения» других систем), либо, обратно, ее превращением в подсистему другой сверхсистемы.

Возьмем на себя смелость утверждать, что в настоящее время СиЗИ находятся на первом этапе своего развития, а в России, скорей всего, и в первой его половине. Набор типовых элементов, из которых строятся сегодняшние «островковые» СиЗИ, крайне ограничен: антивирусы, межсетевые экраны, средства защиты от НСД, реже VPN, еще реже IDS - вот, пожалуй, и все. Выбор поставщиков этих элементов тоже, к сожалению, не велик. По этой причине качество реализуемых СиЗИ (в техническом смысле) главным образом зависит от качества установки и настройки этих самых элементов. А потому, на наш взгляд, в настоящее время, вероятнее всего, СК имеют на рынке преимущество, поскольку, как правило, имеют больший опыт в установке и настройке отдельных средств защиты информации (на поставке и установке которых они, собственно, и специализируются).

Теперь посмотрим, как измениться расстановка сил с неизбежным развитием СиЗИ. Превращение набора различных элементов ИБ в Систему, главным образом, зависит от усилий со стороны разработчиков продуктов ИБ – насколько полно и быстро они смогут интегрировать различные компоненты СиЗИ в единый управляемый комплекс. Но, уже очевидно, что такие комплексы будут включать в себя большое количество сложных высокотехнологичных элементов со сложной структурой внутренних и внешних связей (убедиться в справедливости такого утверждения можно, проанализировав, например, состав продукта приблизительно такого класса - Tivoli SecureWay от компании IBM). Что это означает? А то, что, скорей всего, к этому моменту позиции СИ будут выглядеть предпочтительней, поскольку:

а) СИ наберутся достаточного опыта в построении СиЗИ;

б) СИ более приспособлены к работе с большими сложными системами, которые, к тому же, будут все теснее и теснее интегрироваться с базовыми инфраструктурными элементами АС;

в) у СИ будут нарабатываются типовые комплексные решения по защите, которые по качеству, вероятно, будут не уступать аналогичным решениям от СК, а по цене вплотную приблизятся к ним в силу «типизации»;

г) и главное, в развитие данного перспективного направления бизнеса СИ будут инвестированы большие внутренние ресурсы.

По нашему мнению, СК найти адекватные ресурсы для успешного продвижения компонентов СиЗИ в отрыве от АС, думается, вряд ли удастся. Отсюда следует, что на втором этапе развития СиЗИ выбор заказчика в пользу СИ будет более оправдан. Однако, при этом следует обязательно оговориться: «большими» системами будут интересоваться, в основном, крупные заказчики, а потому ниша средних и мелких заказчиков по прежнему останется за СК.

Теперь перейдем к прогнозу на последний, третий из выделенных нами этапов развития СиЗИ. Главный вопрос этого этапа: сохранит ли СиЗИ самостоятельность в составе АС или будет поглощена ею наряду с другими системами уровня предприятия? Мы придерживаемся мнения, что второй исход более вероятен, т.е. со временем СиЗИ перейдут в разряд подсистем (но – ключевых подсистем!) АС предприятия. Почему? Доказательством данного утверждения могут служить тенденции развития продуктов информационных технологий за последние два-три года. Очевидно, что все чаще и чаще ранее самостоятельные функции защиты информации успешно интегрируются в эти продукты и все большее количество функций защиты реализуется в рамках базовой инфраструктуры АС. Думается, что не за горами тот день, когда мы будем иметь операционные системы со встроенными функциями антивирусной защиты и персонального межсетевого экрана; ПК со встроенной аппаратной защитой от НСД; маршрутизаторы со встроенными функциями реализации VPN и IDS; прикладное ПО со встроенной поддержкой цифровых сертификатов и ЭЦП и т.д. и т.п. Кстати, многое из перечисленного, и даже больше, доступно уже сейчас! Что это означает для нашего вопроса? А то, что вопрос этот исчезнет сам по себе! СИ, даже при очень большом желании, попросту не смогут построить или модернизировать АС без одновременного (автоматического) построения или модернизации СиЗИ. Или, по крайней мере, очень значительной ее части. А заказчики, со своей стороны, будут вынуждены требовать реализации всех заложенных в продукты функций защиты информации – ведь за них заплачены деньги! К этому времени квалификация оставшихся на рынке СИ, скорей всего,

будет достаточна для реализации всей АС заказчика «под ключ», с учетом и всех требований по безопасности.

Однако, означает ли это полную победу СИ и исчезновение с рынка СК? Мы думаем, что нет. Более того, бизнес СК перейдет в другую плоскость, в которой наиболее «продвинутые» СК смогут еще более упрочить свои позиции по сравнению со «старыми добрыми временами». О чем идет речь? Давайте представим себе типичную ситуацию, скажем, 2010-го, а, может быть, и 2005 года. Некий Заказчик силами некого Интегратора в очередной раз модернизировал свою АС. При этом важно, что АС для него уже не является каким-то отвлеченным понятием, как это часто происходит сегодня. На АС «завязан» весь его бизнес: от управления производством и финансового менеджмента, до системы внутрикорпоративной телефонии и автоматического пожаротушения на складах. Объем накопленных информационных ресурсов гигантский, а их стоимость, по сути, равна стоимости самого бизнеса! Стоимость простоя или сбоя в АС исчисляется очень конкретными, и не малыми, цифрами. И т.д. При этом Заказчику совершенно не интересно по чьей вине, хитроумного хакера или нерадивого инженера, произойдет потеря информации или сбой АС – этого просто не должно быть!!! И тут возникает ситуация, когда к Заказчику приходит Интегратор и докладывает ему об успешном завершении работ по модернизации АС. При этом Интегратор утверждает, что все работы по защите информации проведены, ошибок в настройках ПО и оборудования нет, резервное копирование работает «как часы», и вообще все ОК – давай подписывать акты. И что делать Заказчику? Довериться СИ (но кто же скажет, что сделал плохо?) или попробовать каким-то образом проверить полученный результат? Второе, очевидно, лучше – доверяй, но проверяй, особенно когда дело касается бизнеса. Но как это сделать? Нанимать еще одного Интегратора для проверки деятельности первого – безыдейно, они обязательно начнут «тянуть объяло на себя», обвиняя друг друга во всех смертных грехах. Сотрудники собственного IT-подразделения перегружены и недостаточно опытны в области ИБ. Раньше было проще: вот – элементы АС, а вот – СиЗИ: функционально законченный узел, который можно пощупать, протестировать. убедиться в его работоспособности и др. В новых условиях этот фокус не проходит, а тестирование встроенных средств защиты – не всегда наглядно и требует определенных, и глубоких, знаний и опыта.

И вот тут то возникнет потребность в некоторой третьей, независимой, но компетентной Компании, которая, уже не являясь конкурентом Интегратора (по описанным выше причинам), но продолжая глубоко специализироваться в области защиты информации, может еще на этапе подготовки к модернизации АС подсказать

Заказчику как лучше оптимизировать применение средств защиты, а в дальнейшем, после завершения работ, провести для него объективный независимый аудит (или аттестацию) степени защищенности его АС.

Итак, что же мы имеем в результате? В настоящее время выбор исполнителя работ по построению СиЗИ зависит, главным образом, от «масштаба» заказчика и уровня развитости его АС. Если ваша компания относится к числу малых или средних предприятий, и/или уровень интеграции ваших бизнес - процессов в АС вас полностью устраивает, и необходима только установка некоторых элементов СиЗИ для более «спокойной жизни» – мы рекомендуем остановить свой выбор на специализированных компаниях. Если же ваш бизнес можно отнести к разряду крупных, ваша АС достаточно развита и продолжает развиваться – предпочтительней выглядит выбор в пользу системного интегратора.

Попутно сделаем еще несколько замечаний. С учетом вышеизложенных тенденций развития рынка обеспечения ИБ основным его «игрокам» можно порекомендовать следующее: системным интеграторам - больше внимания уделять именно системной стороне ИБ и набираться опыта построения СиЗИ в составе АС; специализированным компаниям нужно подумать о росте квалификации сотрудников в области аудита сложных СиЗИ и, главное, поддержке своей репутации на рынке. А уважаемым заказчикам, особенно крупным, стоит начать приглядываться к имеющимся сегодня на рынке СК: кому из них можно будет доверить аудит своей АС, может быть, всего через два-три года! И к этой проблеме надо подходить так же тщательно, как к выбору своего адвоката или, скажем, семейного доктора!