Аутсорсинг ИТ и ИБ – оценка экономической эффективности и рисков использования

Анна Соколова, Ирина Филиппова, *эксперты компании "ЭЛВИС -ПЛЮС"*

Одним из важных препятствий для развития ИТ-аутсорсинга в России являются вопросы обеспечения безопасности. Аргументов "за" использование аутсорсинга часто не хватает, чтобы перевесить аргументы "против". Поэтому одним из дополнительных, но весомых критериев принятия решения об использовании аутсорсинга как такового либо выбора исполнителя и/или функций, передаваемых на аутсоргинг, может стать его экономическое обоснование.

Сложность информационных систем и скорость обновления технологий с каждым годом возрастает, поэтому для поддержания ИТ-систем предприятий и организаций в рабочем состоянии все больше ощущается потребность не только в соответствующем техническом оснащении, но и в квалифицированных кадрах. Затраты на содержание высококвалифицированного персонала, как показывает практика, весьма велики и продолжают расти.

Одним из возможных способов обеспечения адекватного развития и качественного сопровождения ИТ-инфраструктуры является передача каких-либо вспомогательных функций другой компании, специализирующейся в данной области. В этом и заключается суть аутсорсинга, который, в отличие от разовых услуг, оказываемых сторонними организациями, предполагает наличие длительного процесса и устойчивых взаимоотношений между заказчиком и исполнителем. Ключевыми факторами, влияющими на принятие решения об использовании аутсорсинга, являются возможность его органичного встраивания в бизнес-процессы компании, экономическая эффективность и минимизация потенциальных рисков его использования. Однако достижение всех этих преимуществ доступно лишь при грамотной организации самого процесса аутсорсинга.

В принципе при рассмотрении вопроса об использовании аутсорсинга (причем любого, а не только в сфере ИБ) возможны три альтернативных решения:

- отдать все функции на аутсорсинг;
- отдать только часть функций;
- не использовать аутсорсинг.

Чтобы сделать окончательный выбор того или иного варианта решения логично использовать и экономические критерии. Для сравнительного расчета вариантов здесь можно применить модель ТСО (совокупной стоимости владения), которая уже стала "классической" для сфер ИТ и ИБ. В рамках данной модели учитываются все возникающие затраты[1].

Все или ничего

С точки зрения проведения экономической оценки наиболее "простыми" будут два крайних случая – "все" и "ничего" (рис. 1).

Если сторонней организации передаются все функции, то основные затраты определяются аутсорсером при формировании коммерческого предложения для заказчика. В таком случае аутсорсер оказывает своеобразную "помощь" в определении некоторых составляющих ТСО (в части прямых затрат). Однако следует помнить, что процессы обеспечения ИБ являются составной частью общих бизнес-процессов. Поэтому, хотя функции и переданы сторонней организации, каким-то образом придется обеспечивать взаимодействие с ней, контролировать качество оказываемых услуг, выполнение принятых аутсорсером обязательств и т.п. Отсутствие контроля, тем более для таких критических функций, как обеспечение информационной безопасности, приведет к возникновению дополнительных и неоправданных рисков. В зависимости от масштабов компании для этого выделяется один сотрудник или создается специальное подразделение. Подготовительные работы, необходимые для передачи функций на аутсорсинг, также могут потребовать достаточно больших затрат: например, формализация процессов, покупка дополнительного оборудования и ПО и т.п.

Кроме того, в случае передачи всех функций аутсорсеру остается такая проблемная составляющая ТСО, как косвенные расходы (т.е. затраты, вызванные сбоями в работе системы, ненадлежащей поддержкой со стороны специалистов аутсорсера, адаптацией сотрудников к данным нововведениям и т.п.). Одной из причин использования аутсорсинга как раз является сокращение этой статьи затрат (так, по оценке Gartner Group, в среднем уменьшение косвенных затрат может составлять до 30%), но в основном это зависит от качества работы аутсорсера и профессионализма его специалистов. Если аутсорсинг не используется, расчет ТСО сводится к определению затрат на сопровождение системы

"Промежуточные" варианты

Как видно из вышеизложенного, определение экономических оценок двух крайних вариантов (когда аутсорсинг используется в полном объеме и не используется вообще) дело относительно несложное. Однако для поиска оптимального сочетания в разделении "сфер влияния" между ИТ-отделом (или службой ИБ) компании и аутсорсером целесообразно рассмотреть промежуточные варианты, то есть когда на аутсорсинг передается только часть функций. Этот процесс является достаточно трудоемким и заключается в определении граничных значений ТСО для каждой функции, которую планируется передать на аутсорсинг. В результате можно найти наиболее рациональное соотношение, определяющее, какие функции и в каком объеме целесообразно передать на аутсорсинг. Причем очень многое будет зависеть от специфики самой ком-

[1] *Подробнее см. статью А.А. Соколовой и И.А. Филипповой "Косвенные расходы при оценке ТСО" в журнале "Information Security/Информационная безопасность" № 5, 2006.*

Комментарий эксперта

Андрей Никишин,
директор направления аутсорсинга ИТ-безопасности компании "Лаборатория Касперского"

Аутсорсинговая модель организации систем ИТ-безопасности только зарождается в России. Мировой опыт показывает, что первые шаги в предоставлении услуг аутсорсинга будут довольно трудными как для поставщиков услуг (необходимо убедить потенциальных клиентов в привлекательности модели аутсорсинга), так и для клиентов (требуется преодолеть осторожное отношение к аутсорсингу и найти исполнителя, которому можно доверять). Авторы статьи затронули очень интересный и важный аспект – экономическую привлекательность модели аутсорсинга. Жаль только, что в статье не было приведено реальных цифр, но, полагаю, в следующей статье мы их увидим. По опыту же наших клиентов могу сказать, что TCO сервисных (аутсорсинговых) решений для средних компаний (300–1000 человек) на 25–35% ниже по сравнению с аналогичными решениями, но поддерживаемыми силами клиента. А ведь у таких компаний уже есть свои ИТ-специалисты довольно высокого класса. По моему глубокому убеждению, аутсорсинг ИБ – это выигрышная модель, несущая массу выгод бизнес-клиентам, и именно за ней – будущее.

пании и ее внутрикорпоративных характеристик: квалификации и численности персонала, используемых технологий, масштаба, территориальной распределенности и т.д.

В качестве одной из методик, которую можно использовать как "первую итерацию", предлагается расчет следующего коэффициента:

$$D=X \bullet \frac{Z+K}{T} - A \bullet K_p,$$

где X – предполагаемые трудозатраты сотрудника (в часах);

Рис. 1.

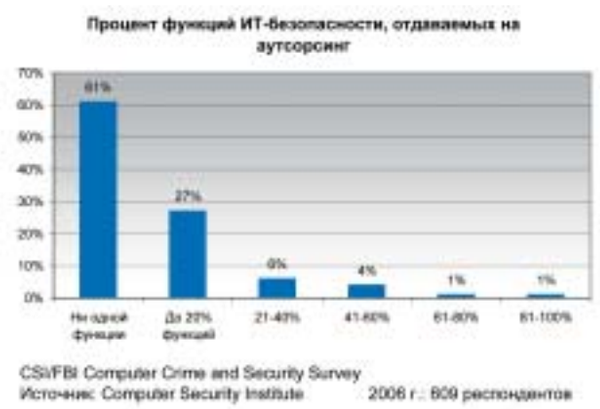

Рис. 2.

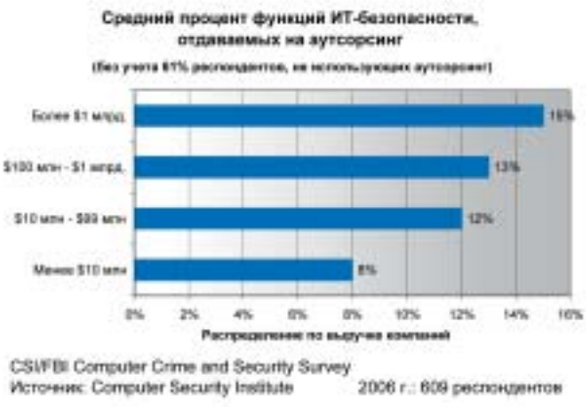

Рис. 3.

Осторожное использование аутсорсинга как в России, так и за рубежом может быть обусловлено, в том числе и отсутствием адекватных оценок его эффективности и оптимальных вариантов использования. Поэтому одно из условий развития услуг по аутсорсингу заключается в более широком применении соответствующих методик для его экономической оценки.

Z – величина заработной платы (в месяц);

K – величина накладных расходов на сотрудника в месяц (соцпакет, обеспечение рабочего места и пр., что может составить 200–500% от фонда оплаты труда);

T – количество рабочих часов в месяц (обычно равно 176);

A – стоимость услуг аутсорсинговой компании;

K_p – коэффициент риска.

Если D>0, то эффективнее использовать атусорсинг. Однако при этом затраты не учитываются в полном объеме, а "абстрактный" коэффициент риска вносит некоторую субъективность. Кроме того, не следует исключать существование рисков при выполнении каких-либо функций по обеспечению безопасности "внутренними" специалистами.

У них и у нас

Если обратиться к зарубежной практике, то и здесь картина получается неоднозначной. С одной стороны, с учетом более высокого уровня развития рынков ИТ и ИБ, ситуация с аутсорсингом должна быть более привлекательной, но, с другой стороны, результаты исследования "2006 CSI/FBI Computer Crime and Security Survey" мало отличаются от полученных в предыдущие два года (рис. 2 и 3). Как и раньше, более половины организаций-респондентов не отдают на аутсорсинг ни одной из функций по обеспечению ИБ, а среди тех, кто его использует, прослеживается тенденция, свойственная и для России: чем крупнее организация, тем больше функций передается. Однако, по данным того же исследования, максимальная доля передаваемых функций не превышает 15%. Для России даже такие показатели пока недостижимы. Кроме того, подобные регулярные крупномасштабные исследования у нас до сих пор не проводятся и информацию можно получить только по результатам отдельных исследований компаний, работающих на рынке ИБ.

Так, результаты исследования рынка услуг, проведенного компанией "ЭЛВИС-ПЛЮС" в 2006 г., в чем-то повторяют основные тенденции, указанные выше. Из всего спектра услуг в сфере ИБ аутсорсинг относится к наименее популярным, причем более высокий интерес отмечается среди представителей крупных[2] компаний (14% респондентов[3], а для средних компаний – 9%). ●

Ваше мнение и вопросы присылайте по адресу
infosec@groteck.ru

[2] *С численностью более 300 человек.*
[3] *Общее число респондентов – 120.*

Лучше поздно, чем никогда

На прошедшей в начале 2007 г. в Сан-Франциско конференции RSA было объявлено о смене парадигмы защиты одним из крупнейших поставщиков систем хранения и управления данными – EMC. В своих долгосрочных планах компания намерена перейти от периметрового обеспечения безопасности к защите самой хранимой в базах данных информации.

На конференции было заявлено, что хотя затраты ИТ-индустрии на безопасность в 2006 г. оцениваются в 40 млрд долларов, корпоративные данные остаются уязвимыми к атакам. Именно поэтому EMC приобрела компанию RSA Security, сделав ее своим подразделением по ИБ. Сумма сделки составила 2,1 млрд долларов.

Характерно, что рынок положительно откликнулся на давно назревшую необходимость интеграции механизмов безопасности в средства хранения данных: акции RSA после одобрения сделки выросли на NASDAQ на 6 центов, а акции EMC – на 12 центов.

Информационная безопасность является приоритетом для руководителей во всем мире и неотъемлемым атрибутом управления информацией. Предприятия не могут защищать то, чем они не управляют, и когда речь заходит о защите информации, это означает две вещи – управление данными и управление доступом к ним.

По мнению экспертов, большинство решений по безопасности не защищают информацию, они защищают лишь периметр. Между тем, большое значение имеют внутренние угрозы, создаваемые злоумышленниками, находящимися как внутри, так и вне компании (социальная инженерия). Для защиты от этих угроз в решения ЦХД интегрируются технологии RSA Security.

Пока неясно, будут ли технологии RSA применяться и в других решениях EMC, например, в линейке продуктов на основе Clarion. По всей видимости, Symmetrix является своего рода опытной площадкой, на которой обкатываются новые для компании решения безопасности.

От редакции

Наверное, читатели журнала с удивлением узнают, что элементарные механизмы безопасности только-только начинают внедряться в отдельные зарубежные продукты систем хранения и управления данными. Ведь в этих системах аккумулированы терабайты информации, в том числе, исключительно важной. Но такова реальность.


BYTE

В отличие от зарубежного подхода, при создании отечественных центров хранения данных (ЦХД), информационной безопасности изначально уделяется большое внимание. Так, в целях программы "Электронная Якутия до 2010 г.", в соответствии с которой создано ЦХД, записано: "Разработать и обеспечить необходимый уровень системы информационной безопасности Республики Саха (Якутия), содержащей комплекс организационно-административных и технических мер".

По материалам CRN, ИА REGNUM, EMC, BYTE