Д. Б. Фролов, Д. Ю. Персанов

ПРАКТИЧЕСКИЕ АСПЕКТЫ АУТСОРСИНГА ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Понятие аутсорсинга

В настоящее время термин «аутсорсинг» используется очень часто. Исходный смысл понятия происходит от английского «out» — внешний и «source» — источник, таким образом, мы получаем внешний источник, т. е. внешний ресурс по отношению к деятельности.

«АУТСОРСИНГ — (англ. outsourcing) — передача традиционных не ключевых функций организации (таких, например, как бухгалтерский учет или рекламная деятельность для машиностроительной компании) внешним исполнителям — аутсорсерам, субподрядчикам, высококвалифицированным специалистам сторонней фирмы; отказ от собственного бизнес-процесса, например, изготовления отливки или составления баланса, и приобретение услуг по реализации этого бизнес-процесса у другой, специализированной организации. Разновидность кооперирования» [1].

Как следует из определения, аутсорсинг выражается в передаче нетипичных и не ключевых функций от одной компании другой с целью повышения эффективности функции за счет квалификации, опыта и ресурсов подрядной организации. Важным моментом в данном определении является «в передаче **не ключевых** функций», так как в указанном контексте вопрос, какие функции являются ключевыми, остается открытым.

Безусловно, к ключевым функциям следует отнести (не ограничиваясь) общий менеджмент и стратегическое планирование, а также собственную безопасность. В случае если в принятии решений о стратегии деятельности компании задействован внешний участник, с большой долей вероятности можно предположить, что стратегия может частично или полностью утратить исходные ценности и цели компании, а приоритеты — сместиться в сторону интересов внешней компании-участника.

Собственная безопасность как вид деятельности представляет собой совокупность организационных, технических и физических аспектов, которые также можно разделить на уровни управления по аналогии с общим менеджментом организации:

- стратегический уровень — формулирование стратегии обеспечения собственной безопасности предприятия, организации, выработка основных принципов;
- тактический уровень — формирование программы и «дорожной карты» реализации стратегии безопасности на основе оценки условий деятельности и ключевых факторов влияния, в том числе бюджетных оценок;
- оперативный уровень — определение перечня основных видов деятельности, обеспечивающих реализацию программы безопасности, ее постоянное функционирование и улучшение.

Можно также выделить в процессе обеспечения безопасности ключевые активности (например, стратегическое планирование в области безопасности), равно как виды деятельности, по которым возможно привлечение сторонних организаций по объективным причинам (например, с точки зрения финансовой эффективности).

Принимая во внимание все вышесказанное, **аутсорсинг безопасности** — это передача части не ключевых функций в области обеспечения безопасности третьей стороне с заданным уровнем показателей сервиса.

Факторы влияния

Следует отметить, что для российской действительности вопрос передачи функций безопасности является достаточно «щепетильным» в силу сложившихся стереотипов и широкого

распространения командного типа управления. Поэтому одним из ярких и характерных для России факторов является недоверие руководства, ощущение утраты контроля над ситуацией при передаче функций, в том числе безопасности.

Также к особенностям, влияющим на принятие решений о реализации стратегии безопасности, можно отнести следующие:

1. Осведомленность и компетентность руководства в вопросах безопасности. Зачастую руководство предприятия больше озабочено созданием новых мощностей, увеличением доли занимаемого рынка и прибыли, нежели защитой собственных активов.

2. Наличие иностранного капитала и участия (влияет на общую стратегию, в том числе стратегию безопасности, компании), так как модель ведения бизнеса и государственного управления на Западе сильно отличается от российской.

3. Основные виды деятельности предприятия: банки и другие финансовые институты зачастую сильнее озабочены собственной безопасностью не только в силу внутреннего законодательного регулирования, но и в силу того, что безопасность банка эквивалентна безопасности денежных средств вкладчиков.

4. Размер организации (крупный, средний, малый бизнес; государственная организация; некоммерческая организация) влияет на финансовые возможности.

5. Территориальный признак (компания/организация дислоцирована в одном месте либо имеет разветвленную структуру с удаленностью филиалов / штатных единиц).

6. Обрабатывает / не обрабатывает информацию, содержащую государственную тайну (более жесткие и законодательно закрепленные меры безопасности).

Так или иначе, при выборе стратегии обеспечения безопасности, будь то полный, частичный аутсорсинг либо обеспечение безопасности своими силами, во главу угла будет поставлен экономический аспект (в меньшей степени — для государственных организаций, обрабатывающих государственную тайну). Экономика складывается из двух составляющих:

— профиль рисков для исследуемого вида деятельности / объекта оценки:

- ценность актива/процесса для деятельности в области безопасности;
- характерные угрозы;
- известные уязвимости и внедренные компенсирующие меры;

— сравнительная финансовая оценка совокупных затрат на организацию штатной единицы (комплектация, наделение дополнительными обязанностями и пр.) в противовес стоимости услуг третьей стороны с заданной квалификацией и уровнем обслуживания.

Профиль рисков в данном случае — общая оценка рисков, характерных для защищаемого объекта при известных уязвимостях и реализованных защитных мерах, с учетом ценности объекта для бизнеса. Например, в случае передачи информации категории «строго конфиденциально» выглядит неразумным использовать простые бумажные конверты и передачу путем обычных почтовых отправлений. Для данной категории информации показатель важности является очень высоким, угроза раскрытия информации при использовании обычного конверта либо утраты в силу ненадежности почтовой системы также очень высоки: стоимость специализированной курьерской доставки (например, для государственных структур — спецсвязь) либо отправки корпоративного автомобиля с курьером будет неизмеримо ниже, чем утрата/раскрытие информации.

Финансовая оценка затрат на обеспечение безопасности по конкретному направлению будет складываться из следующих составляющих:

- расходы на персонал;
- расходы на обслуживание, амортизационные отчисления и пр.;
- прочие затраты (косвенные расходы).

Рассмотрим альтернативы реализации функций безопасности с учетом возможных сценариев в виде полного или частичного аутсорсинга.

Физическая безопасность

— Общий менеджмент — только внутренние службы.

— Обеспечение контроля и режима на объектах:

- Герметичность помещений (контроль закрытия дверей, системы контроля доступа, сигнализация и пр.).
- Видеонаблюдение.

Возможна аренда оборудования и составных частей оборудования, при этом функции контроля остаются в ведении внутренних служб.

— Безопасность персонала:

- Пожарная безопасность и охрана труда.

Пожарная безопасность — разумно иметь в штате лиц, подготовленных для выполнения неотложных действий по пожаротушению, равно как по обслуживанию систем пожаротушения, при этом функции штатного обслуживания систем, обучения персонала могут быть выведены на аутсорсинг.

Охрана труда — законодательно закреплено наличие в штате организации лица, ответственного за организацию работ по охране труда. При этом консультационные функции, естественно, могут быть переданы профильным специалистам внешних компаний.

- Охрана VIP-персон.

Внутренняя служба.

— Перевозка ценных грузов.

Возможны как использование собственных курьерских служб предприятия, так и договор об оказании услуг со специализированными компаниями.

Информационная безопасность

— Общий менеджмент и управление рисками.

Внутренняя служба.

— Криптографическая защита информации.

В зависимости от потребностей предприятия: для использования в собственных нуждах коммерческими предприятиями лицензия не нужна; может быть частичный аутсорсинг (обслуживание оборудования, предоставление услуг), в части управления ключами — только внутренние службы.

— Контроль доступа:

- Операционные системы и сети передачи данных.

В зависимости от подхода компании к поддержке собственной инфраструктуры: например, для малого бизнеса с локализованной в одном физическом месте сетью можно использовать полный аутсорсинг инфраструктуры и полностью передать все функции по настройке и поддержке третьей стороне. Для распределенных сетей с высокими требованиями отказоустойчивости и повышенной критичностью передаваемых данных может быть более эффективным использование собственной службы поддержки, хорошо знакомой с топологией и особенностями ЛВС и ее взаимосвязями.

- Приложения.

Владельцы приложений (лица, ответственные за использование данных приложений и информационную безопасность, в том числе за определение и пересмотр прав доступа к информационным системам) — внутренние службы. При этом если поддержка приложения выведена полностью на аутсорсинг (в том числе хостинг, администрирование базовой части (ОС), администрирование прикладной части (приложение, СУБД)), а предприятие является лишь потребителем сервиса — в этом случае проще передать технические функции контроля доступа к приложению сервис-провайдеру, тогда как предприятие сохраняет за собой право определять на бизнес-уровне правила доступа к информационной системе.

— Операционная безопасность:

- Защита от утечек.

В ведении внутренних служб, так как указанные системы позволяют получить доступ к информации ограниченного доступа.

- Антивирус.

Может быть полностью передан на аутсорсинг с обеспечением информирования заказчика об инцидентах.

- Инцидент-менеджмент и расследование инцидентов.

Управление инцидентами может осуществляться сервис-провайдером, в случае если инциденты возникают в его зоне ответственности (например, если имеет место аутсорсинг сетевого оборудования и серверов). При этом расследование инцидентов высокой критичности должно осуществляться либо непосредственно службами заказчика, либо с привлечением указанных служб.

— Сетевая безопасность.

Зависит от архитектуры сети, в случае если сеть полностью находится под управлением сервис-провайдера, имеет смысл передать функции безопасности сети (например, эксплуатацию системы обнаружения вторжений) также на обслуживание, при этом необходимо обеспечить полное информирование заказчика о событиях и инцидентах информационной безопасности.

— Безопасность приложений.

Разработка приложений в современных условиях обычно передается компетентным специалистам по договору. При этом бизнес-требования и требования безопасности должны формулироваться заказчиком либо консультантами совместно с заказчиком.

— Построение безопасной архитектуры.

В случае если инфраструктура и ее поддержка выведены на аутсорсинг, разумно осуществлять указанную деятельность сервис-провайдеру совместно с заказчиком.

— Непрерывность бизнеса.

Все фазы планирования непрерывности, т. е. создания плана непрерывности и (или) планов аварийного восстановления, должны осуществляться внутренними службами (возможно, с привлечением консультантов по методологии). Тестирование планов должно осуществляться внутренними службами с привлечением лиц, которые в будущем будут претворять эти планы в жизнь, если произойдет активация плана.

— Комплаенс и аудит в области ИБ.

Комплаенс, т. е. соответствие требованиям законов и стандартов, предполагает анализ применимых к деятельности предприятия нормативных правовых актов и стандартов. Указанный анализ целесообразно выполнять внутренним службам, как обладающим осведомленностью о принципах и механизмах функционирования предприятия. При этом в отдельных случаях, требующих комплекса мероприятий по приведению в соответствие требованиям законов и стандартов, возможно привлечение профильных организаций, имеющих подтвержденную компетенцию в данной предметной области (пример — использование подрядных организаций для выполнения работ по приведению в соответствие требованиям 152-ФЗ, PCI DSS, СТО БР ИББС).

Внутренний аудит является инструментом повышения эффективности функционирования предприятия, таким образом, проводить его необходимо внутренним службам. При этом большинство предприятий так или иначе участвуют во внешних аудитах (например, анализ отчетности и пр.).

Экономическая безопасность

— Общий менеджмент и управление рисками.

Как и в предыдущих случаях, указанная деятельность должна осуществляться внутренними службами.

— Борьба с коррупцией.

Рационально использовать внутренние службы, так как привлечение сторонних компаний может создать нежелательную огласку или привести к появлению еще одного звена коррупционной цепочки.

— Противодействие мошенничеству.

Аналогично предыдущему. Также в качестве инструмента противодействия может использоваться внешний (независимый) аудит.

— Защита имиджа, бренда и репутации компании.

Внутренние службы.

— Проверка персонала перед наймом.

Внутренние службы. Для государственных организаций такие проверки могут осуществляться в соответствии с законодательством.

ПРИМЕР 1

Для осуществления деятельности в области криптографической защиты информации необходимо иметь в штате одного руководителя (стаж 5 лет в области ИБ, профильное образование и т. д.), а также как минимум двух специалистов соответствующей квалификации. Таким образом, предприятие, которое собирается осуществлять деятельность с применением криптосредств в части, подлежащей лицензированию (например, для оказания услуг процессинга платежных карт), обязано удовлетворять вышеуказанным условиям (помимо прочих лицензионных требований), соответственно, финансовая составляющая поддается вполне конкретной оценке (фонд з/п 1 руководитель + 2 подчиненных; обслуживание криптосредств (электричество, аренда, амортизация), другие косвенные расходы).

С другой стороны, предприятие может заключить договор об оказании услуг с компанией, имеющей лицензии на предоставление услуг, распространение и техническое обслуживание средств шифрования, а также лицензию на техническую защиту конфиденциальной информации, с предметом договора в виде оказания услуг по криптографической либо иной технической защите информации, с заданным уровнем сервиса. В этом случае предприятие избавляется от необходимости получать лицензии и содержать штат профильных специалистов и руководителя (руководителей), а также нести все прямые и косвенные расходы, связанные с эксплуатацией средств защиты информации (из тех, что поставлены на обслуживание по договору), но несет ежемесячные расходы в соответствии с условиями договора.

В данном примере стоит обратить внимание на тот факт, что наличие собственного персонала априори подразумевает лояльность, управляемость и соответствие заявленным целям организации, чего сложнее добиться путем заключения договора.

ПРИМЕР 2

Для бизнеса в сфере торговли характерен следующий пример: для обеспечения физической безопасности заказчика используются подразделения ЧОП и УВО МВД, при этом контроль и общий менеджмент остаются за представителями заказчика. В данном случае компания-заказчик избавляется от необходимости содержать в штате, готовить и лицензировать сотрудников низкой квалификации по совершенно непрофильному виду активности: достаточно иметь несколько менеджеров.

В качестве выводов по применению услуг аутсорсинга безопасности стоит отметить следующее:

1. Для малого бизнеса в условиях сильно ограниченных финансовых возможностей целесообразно применять аутсорсинг высокотехнологичных и ресурсоемких процессов. Безопасность в данном случае будет являться неотъемлемой частью пакета предоставляемых услуг с заданным уровнем сервиса.

2. Нецелесообразно приобретать в собственность оборудование и целые функциональные процессы, если это не является основным видом деятельности компании либо актив не является

ликвидным. Например, нет смысла приобретать в собственность дорогой сервер DLP (data leak prevention, защита от утечек), если экономическая отдача на ближайшем горизонте не поддается оценке, рациональнее взять сервер в аренду.

3. Целесообразно применять аутсорсинг процессов в тех случаях, когда стоимость обучения собственного персонала и набора в штат даже в перспективе 2-3 лет не окупит затраты на персонал.

4. Общий менеджмент и контроль над организацией и исполнением процессов безопасности должны быть на стороне предприятия-заказчика.

5. Договор об оказании услуг должен содержать детальное описание показателей уровня сервиса (процедуры обеспечения показателей сервиса должны быть доведены до сведения заказчика) и гарантий его предоставления. Также неотъемлемым условием договора об оказании услуг должно быть соглашение о конфиденциальности.

СПИСОК ЛИТЕРАТУРЫ:

1. *Райзберг Б. А., Лозовский Л. Ш., Стародубцева Е. Б.* Современный экономический словарь. 5-е изд., перераб. и доп. М.: ИНФРА-М, 2007. – 495 с. (Библиотека словарей «ИНФРА-М»).
2. «Трудовой кодекс Российской Федерации» от 30.12.2011 № 197-ФЗ (ред. от 22.11.2011, с изм. 15.12.2011).
3. Федеральный закон № 99-ФЗ «О лицензировании отдельных видов деятельности» от 27.04.2011.
4. Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006.
5. Стандарт безопасности индустрии платежных карт Payment card industry Digital security standard (PCI DSS).
6. Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС-1.0-2010) от 21.06.2010.
7. Федеральный закон от 27.07.2004 № 79-ФЗ (ред. от 21.11.2011, с изм. от 06.12.2011) «О государственной гражданской службе Российской Федерации».
8. Постановление Правительства РФ № 957 от 29.12.2007 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».