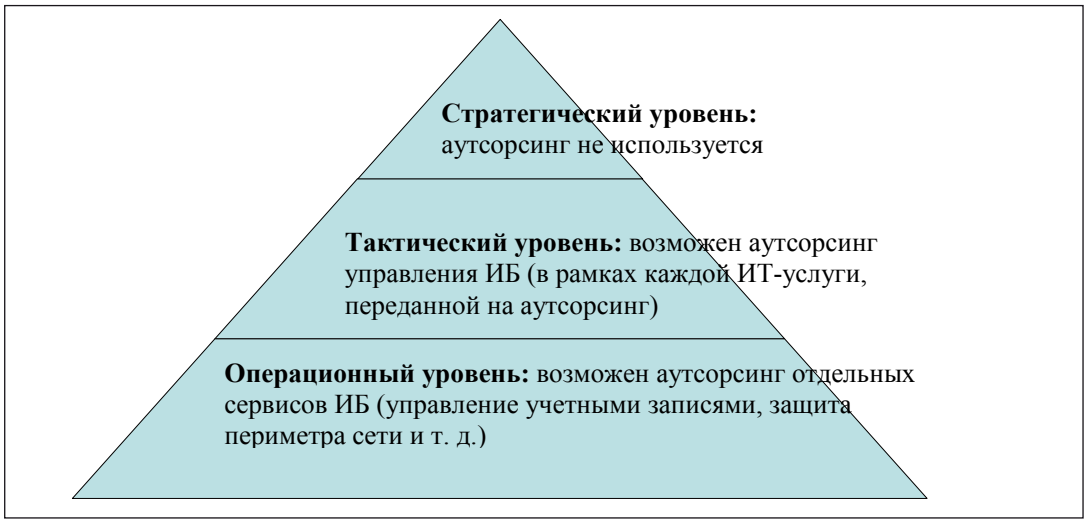
Е. В. Минаева, И. А. Пономарев

АУТСОРСИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: УПРАВЛЕНИЕ УРОВНЕМ УСЛУГ

В современных условиях ужесточившейся конкуренции и резкого сокращения расходов компаний вследствие мирового экономического кризиса повышение эффективности вложений в средства обеспечения информационной безопасности (ИБ) становится одной из первоочередных задач. Далеко не все компании могут позволить себе иметь в штате службу информационной безопасности, способную самостоятельно решать задачи в области ИБ на требуемом уровне. В этой ситуации одним из возможных вариантов является передача этих функций на аутсорсинг сторонней организации, специализирующейся на предоставлении данного вида услуг.

Аутсорсинг (от англ. outsourcing — внешний источник) — это передача компанией-заказчиком определенных **бизнес-процессов или производственных функций** на обслуживание компании-исполнителю, специализирующейся в соответствующей области. Аутсорсинг может быть полным или частичным, внутренним или внешним. Спецификой аутсорсинга ИБ является то, что он практически никогда не бывает полным (так как существует ряд функций ИБ, которые не могут быть переданы третьей стороне ни при каких обстоятельствах), а также в большинстве своем является внутренним (услуги аутсорсинга предоставляются структурным подразделением компании на основе внутреннего соглашения о предоставлении услуг, Service Level Agreement — SLA), что обусловлено критичностью обрабатываемой в системах ИБ информации для эффективного функционирования бизнеса. Если сделан выбор в пользу стороннего провайдера ИБ, необходимо четко определиться, какие именно функции по защите информации допустимо передать третьей стороне.

Интересный подход к выделению совокупности компонентов ИБ — потенциальных кандидатов на аутсорсинг — был предложен специалистами IBM GTS в [1]. В соответствии с ним, информационная безопасность компании может рассматриваться на трех базовых уровнях: стратегическом, тактическом и операционном.



Управление ИБ на стратегическом уровне не может быть передано на аутсорсинг, так как окончательная ответственность за все действия, предпринятые на данном уровне, лежит непосредственно на самой компании. Управление ИБ на тактическом уровне позволяет устранить разрыв между стратегическим и операционным уровнями и может быть подвергнуто частичному аутсорсингу, поскольку на уровне компании оно обычно является одним из процессов,

осуществляемых в рамках управления ИТ. Операционный уровень ИБ, имеющий сервис-ориентированную архитектуру, может быть полностью передан на аутсорсинг внешней компании-аутсорсеру.

В качестве основных компонентов операционный уровень ИБ включает в себя администрирование и обслуживание средств обеспечения ИБ. На аутсорсинг чаще всего передаются сложные средства обеспечения безопасности, управление которыми требует большого количества ресурсов и высокой квалификации персонала. К ним относятся системы обеспечения периметровой защиты, анализа и фильтрации контента (требующие «тонкой» настройки и корректной трактовки событий ИБ), а также службы технической поддержки средств защиты с круглосуточным режимом работы. При этом разработка политик ИБ остается в ведении самой компании, аутсорсер же обеспечивает только настройку средств защиты в соответствии с требованиями политик.

Многие ошибочно полагают, что использование аутсорсинга означает полное переложение рисков ИБ на провайдера услуг. В действительности, компания возлагает на аутсорсера лишь ответственность за совершение конкретных действий по обеспечению ИБ. Это не освобождает ее от ответственности за общее состояние дел в области безопасности (например, риски по защите персональных данных в принципе не могут быть переданы аутсорсеру).

Более того, привлечение услуг аутсорсера, изначально призванное снизить риски ИБ, возникающие в компании, нередко порождает целый комплекс новых рисков, связанных с передачей критичных функций обеспечения информационной безопасности «третьей стороне». Фактически, при аутсорсинге одни риски заменяются другими. Уходит риск потери компетенции (например, при увольнении технического персонала), так как эта проблема переходит на сторону аутсорсера, но, с другой стороны, возникают риски, связанные с «попаданием в зависимость» от аутсорсера, и уже именно эти риски находятся в зоне ответственности компании-заказчика.

Риски аутсорсинга ИБ обладают всеми чертами, присущими рискам аутсорсинга как такового, но при этом имеют также и ряд своих отличительных особенностей. Основными рисками аутсорсинга ИБ являются:

- **Потеря доверия к поставщику услуг.** В силу специфики своей деятельности аутсорсер зачастую имеет доступ к информации ограниченного распространения, раскрытие которой может нанести значительной ущерб бизнесу компании.
- **Операционная зависимость от поставщика.** Ориентация на использование услуг конкретного аутсорсера повышает зависимость компании от стабильности бизнеса последнего (например, уход с рынка).
- **Разделение «сервисного пространства» аутсорсера между несколькими компаниями-клиентами.** Наличие единого сервисного пространства увеличивает вероятность несанкционированного доступа к «чувствительной» информации компании со стороны других компаний-клиентов этого же аутсорсера.
- **Риски внедрения «внешнего» сервиса.** Внедрение внешнего сервиса ИБ в инфраструктуру компании добавляет комплекс рисков, аналогичных рискам внедрения любого нового функционала ИТ/ИБ, что связано с дополнительными расходами на реализацию необходимых интерфейсов для взаимодействия с основными ИТ/ИБ-системами компании.
- **Нарушение партнерских отношений с поставщиком.** Один из самых больших рисков заключается в неверном планировании взаимодействия между компанией и аутсорсером услуг ИБ. Контракт с аутсорсером должен предусматривать все возможные варианты развития событий в процессе предоставления услуг, включая досрочное расторжение договора, порядок смены/расширения услуг, изменения тарифов и обеспечения предоставления услуг в чрезвычайных обстоятельствах.

• **«Скрытые» расходы.** Не все расходы учитываются при определении стоимости услуги, поскольку не могут быть однозначно установлены на этапе формирования контракта аутсорсинга (например, необходимость дополнительного обучения персонала аутсорсера в случае потери им ключевых специалистов, издержки планирования уровня сервиса и управления отношениями с аутсорсером).

• **Правовые риски.** Компания и аутсорсер должны заранее оговорить юридические последствия инцидентов информационной безопасности, в которые оказываются вовлечены обе стороны.

Ключевая часть любого аутсорсингового контакта — это Соглашение об уровне услуг (SLA). Помимо общих договорных обязательств обеих сторон SLA содержит подробное описание услуг, которые будет оказывать аутсорсер; сроки оказания этих услуг; параметры и гарантии качества обслуживания; ответственность обеих сторон.

«Грамотный» SLA, содержащий четко определенные параметры услуг, выгоден обеим сторонам: он позволяет компании контролировать качество предоставляемых ей услуг, а аутсорсеру — планировать необходимые для их выполнения ресурсы.

При составлении SLA, регламентирующего аутсорсинг ИБ, следует использовать общепринятые подходы и стандарты. Например, стандарт ISO 27001:2005 (раздел A.10.2) [2] предписывает управлять предоставляемыми аутсорсером услугами, контролировать, пересматривать и управлять изменениями в этих услугах.

Кроме того, рекомендуемая этим стандартом структура контролей в ИБ помогает определить области, в которых следует устанавливать показатели качества услуг аутсорсинга (Key Performance Indicators — KPI).

В общем случае следование стандартам позволяет:

· четко определить зоны ответственности компании и аутсорсера;

• выявить набор ключевых параметров, характеризующих услуги;

• установить порядок оценки и контроля этих параметров (в том числе и их регулярного независимого аудита).

И, как следствие, позволяет значительно минимизировать возможные угрозы ИБ.

Различные исследования [3] в области ИБ и аутсорсинга показывают, что большинство случаев нарушения ИБ вызваны действиями персонала самой компании (так называемый «человеческий фактор»), а не опасностью передачи функций ИБ вовне.

Набор параметров, которые следует регулярно контролировать при аутсорсинге ИБ, может сильно различаться, в зависимости от характера этих услуг и целей аутсорсинга как такового. Поэтому разумно определить эти параметры на основе результатов анализа рисков. Такой подход позволит минимизировать набор контролируемых параметров.

При анализе рисков следует принять во внимание:

• риски, специфичные для самой компании;

• опыт уже имевшихся прерываний и сбоев в ИБ;

• риски, присущие самой процедуре аутсорсинга как таковой.

По нашему мнению, в SLA следует также зафиксировать:

• права компании на получение компенсации (или, как минимум, сокращения предстоящих платежей) в том случае, если оговоренные параметры не соблюдаются;

• права компании на периодический пересмотр набора контролируемых параметров услуг (например, из-за смены приоритетов по развитию бизнеса или внешних факторов, в частности экономической ситуации);

• юридическую ответственность аутсорсера за инциденты ИБ как способ защитить компанию от неправомочного использования (распространения) ее данных и данных ее клиентов.

Методология, системы и инфраструктура ИБ постоянно развиваются и в значительной мере определяются характером бизнеса компании и набором переданных на аутсорсинг услуг, поэтому «универсального» набора KPI не существует. Рациональным подходом к разработке набора KPI является подход «сверху—вниз»: от общих целей и задач программы обеспечения ИБ компании и определения перечня передаваемых на аутсорсинг услуг к выработке специфичных KPI, характеризующих работу аутсорсера.

В ряду общих требований, которым должны удовлетворять KPI, можно назвать:

- S.M.A.R.T.-критерий (specific, measurable, attainable, repeatable, time-dependent);
- связь с целями компании (например, обеспечение операционной эффективности, повышение управляемости и гибкости и т. д.)
- связь с элементами «триады» ИБ: конфиденциальность, целостность, доступность;
- связь с требованиями стандартов и нормативных актов (ISO 27001, PCI DSS, 152-ФЗ, СТО ИББС 1.0 и т. д.);
- экономическую эффективность (уровень расходов на обеспечение того или иного сервиса ИБ, а также на контроль правильности его функционирования).

На наш взгляд, можно выделить ряд типовых параметров:

KPI	**Примеры**	**Комментарий**
Экономическая эффективность услуги		
Стоимость в расчете на единицу оказываемых услуг (за определенный промежуток времени)	• Стоимость создания/настройки параметров учетной записи пользователя. • Стоимость контроля (анализа протоколов ИБ) одного активного сетевого устройства в год. • Стоимость обновления антивирусных баз (в расчете на одну рабочую станцию)	Позволяет контролировать пропорциональность стоимости услуг при фиксированной стоимости соглашения по аутсорсингу. Также позволяет оценить экономическую эффективность аутсорсинга (по сравнению с расходами на собственную службу ИБ).
Операционная эффективность услуги		
Максимальное время простоя в оказании услуг в случае сбоев и прерываний со стороны аутсорсера	• Время реакции (регистрации) запроса на создание/настройку параметров ИБ.	Позволяет определить порог, по достижении которого к аутсорсеру могут быть применены штрафные санкции.
Время исполнения запроса по настройке параметров безопасности (по типам запросов)	• Время на создание/настройку параметров учетной записи пользователя. · Время на настройку параметров нового активного сетевого устройства. • Доля запросов по настройке параметров ИБ, выполненных в рамках первоначальной оценки срока данных работ.	Позволяет определить и контролировать нормативы на выполнение задач ИБ (по типам запросов).
Выделенный объем ресурсов со стороны аутсорсера (человеко-часов).	• Гарантированный ресурс в 120 человеко-часов в месяц по настройке параметров безопасности.	В сочетании с оговоренным в SLA временем исполнения запросов по услугам позволяет эффективно контролировать реально предоставляемый объем этих услуг.

Современность используемых аутсорсером технических решений по ИБ	• Обязательная периодичность обновления версий ПО и аппаратных средств, используемых аутсорсером для контроля и предоставления услуг по ИБ. • Количество (и доля) идентифицированных и неустраненных известных ИБ-уязвимостей в ПО и аппаратных средствах (используемых компанией и самим аутсорсером при оказании услуг).	Позволяет повысить гарантии того, что аутсорсер принимает во внимание современные угрозы ИБ; следует также оговорить, за чей счет будут выполняться данные обновления.
Соответствие стандартам и нормативным требованиям		
Уровень экспертизы компании-аутсорсера	• Доля сертифицированных ИТ-специалистов (Microsoft, Oracle, Cisco, CISA, CISSP, CERT/CIRT и т. д.) в общем числе специалистов, непосредственно оказывающих услуги по ИБ.	Позволяет повысить гарантии качества предоставляемых аутсорсером услуг.
Периодичность независимых проверок внутренних процессов ИТ и ИБ компании-аутсорсера	• Ежегодный аудит на соответствие требованиям стандартов ИБ, законодательных и отраслевых требований (например, ISO 27001, PCI DSS, 152-ФЗ, СТО ИББС 1.0). • Количество выявленных в ходе аудита нарушений и несоответствий в работе оговоренных контрольных механизмов по ИБ.	Позволяет повысить гарантии качества предоставляемых аутсорсером услуг.
Уровень обеспечения конфиденциальности, целостности, доступности информации компании		
Регулярность установки критических обновлений систем по ИБ	• Доля рабочих станций в вычислительной сети, на которых установлены последние обновления антивирусных баз. • Максимально допустимое время задержки в установке критических обновлений систем (после даты их тестирования на совместимость).	Позволяет повысить гарантии защиты от вновь выявляемых угроз ИБ.
Число достоверно выявленных и предотвращенных нарушений ИБ	• Количество и характеристика выявленных внешних/внутренних атак на информационные ресурсы компании.	Позволяет повысить уверенность в том, что аутсорсер действительно выполняет работы по контролю и предотвращению нарушений ИБ.
Уровень осведомленности пользователей компании о рисках ИБ	• Периодичность информирования пользователей компании о рисках ИБ (e-mail рассылки, информация на веб-портале компании). • Периодичность и результаты опросов (контроля знаний) пользователей по вопросам ИБ.	Позволяет повысить уверенность в том, что аутсорсер уделяет должное внимание «человеческому фактору» в вопросах ИБ.

Наличие KPI еще не гарантирует удовлетворительной работы аутсорсера и уверенности в качестве его услуг. Важной составляющей является то, как организован сам процесс контроля значений KPI.

Смысл мониторинга KPI состоит в своевременном определении их выхода за пороговые значения (а лучше в предсказании такого выхода) и, как следствие, в принятии соответствующих мер по недопущению этого или же компенсирующих шагов (например, штрафных санкций).

Пожалуй, самыми важными аспектами в процессе мониторинга являются:

• процедуры, по которым организовано отслеживание («измерение») KPI, и кто их выполняет (сама компания или аутсорсер);

• процедуры информирования компании о текущих значениях KPI;

• периодичность контроля KPI.

По нашему мнению, для объективной оценки того, какого качества услуги ИБ получает компания (особенно в том случае, когда KPI рассчитываются аутсорсером), полезно определить следующие элементы:

• формат предоставления данных о величинах KPI — это обеспечит возможность их ретроспективной оценки и сравнения;

• время информирования компании о величинах KPI — тут важна регулярность и практически фиксированная периодичность такого информирования (например, еженедельно, в одно и то же время, в понедельник);

• временной интервал отслеживания KPI, обеспечивающий минимизацию эффекта «статистического усреднения», — с практической точки зрения разумным является ежемесячный или еженедельный контроль;

• обязательства аутсорсера по хранению статистических данных, используемых при расчете KPI, — эта информация должна быть доступа независимым аудиторам для оценки правильности расчета KPI.

Даже несвоевременность информирования компании о величинах KPI и исходных данных, использованных для их расчета, может служить одним из важных контролируемых параметров.

В заключение следует отметить, что при разработке системы KPI и определении условий SLA нельзя не учитывать текущую ситуацию на рынке подобных услуг в России, которая характеризуется следующими особенностями:

• нехватка квалифицированных специалистов по ИБ и ИТ, аналитиков и инженеров (причем как у самих компаний, так и у аутсорсеров);

• высокая стоимость таких услуг (квалифицированные специалисты и средства обеспечения ИБ не могут стоить дешево);

• проблема взаимного доверия и деловой репутации аутсорсеров, особенно в таком «чувствительном» вопросе, как обеспечение ИБ;

• недостаточная нормативно-правовая база.

В ряду положительных аргументов аутсорсинга ИБ можно назвать: более высокий уровень экспертизы (чем у самой компании), качество предоставляемых услуг (зачастую недостижимое без серьезных вложений), минимизация собственных ресурсов на выполнение этих задач.

На практике же любая компания должна понимать, что полностью передать все задачи ИБ на аутсорсинг в существующих реалиях невозможно. А значит, какую-то часть функций ИБ придется выполнять самостоятельно, как раз к одной из таких функций и относится разработка и контроль KPI ИБ.

СПИСОК ЛИТЕРАТУРЫ:

1. IBM Global Technology Services. Outsourcing and Information Security (BUW0309-NLEN-00). URL: http://www.ibm.com/services/nl/bcrs.

2. ISO 27001:2005 Information technology — Security techniques — Information security management systems — Requirements.

3. CSI Computer Security Institute «Computer Crime and Security Survey». URL: http://www.csiannual.com.