

Управление ИТ-рисками: стратегия развития инфраструктуры дает конкурентное преимущество

Еще не так давно управление ИТ-рисками было узкой специализацией в составе дисциплины управления операционными рисками по изучению влияния отказов систем и причин неудач ИТ-проектов. Сегодня ИТ-системы пронизывают все аспекты бизнеса, но многие организации все еще относят информационные риски к области операционных проблем. Между тем ИТ-риски стали важной составляющей общих бизнес-рисков организации, а меры по их анализу и минимизации составляют предмет отдельной дисциплины – управление информационно-технологическими рисками (Information Technology Risk Management – ITRM), которая помогает организациям управлять работой информационных систем, согласуя степень рисков с затратами на их предотвращение. Но ITRM может дать больше, чем просто помощь в управлении. В настоящей статье содержатся практические рекомендации и примеры использования ITRM для определения стратегии построения ИТ-инфраструктуры – проектирования и распределения ресурсов обработки данных, хранения данных и сетей таким образом, чтобы они поддерживали конкурентное преимущество и долгосрочные бизнес-цели организации.

Управление рисками в авиационной электронике

Технологии решают назревшие проблемы, но и создают новые риски. Управление ими имеет критическое значение для любой технологически ориентированной стратегии ведения бизнеса. Примером может служить переход от аналоговых систем управления полетом к цифровым.

Системы управления самолетом развивались от механических приводов через гидравлику к аналоговым электронным системам – и все они были целиком основаны на действиях пилота. Но к 1970-м годам конструкция авиадвигателя и самолета “вырвалась из под контроля” человека: предельные скорости, силы и маневры, инициированные пилотом, приводили к возмущениям в системе управления, попытки справиться с которыми вручную приводили лишь к дальнейшему усугублению ситуации.

С появлением управляемых с помощью компьютеров систем регулирования, называемых системами дистанционного управления (fly-by-wire systems), стало возможным поддерживать в допустимых пределах значения потерь скорости, углов поворота и ускорений, а также

фильтровать входные воздействия, исключая возмущения, вызываемые действиями пилота. Но эта технология принесла с собой свои риски, связанные с возможностью отказа компонентов и программного обеспечения. Для управления рисками, вызываемыми этими новыми технологиями, пришлось добавлять резервные системы, проводить специальное обучение экипажа, создавать стандарты сертификации безопасного программного обеспечения и принимать многие другие меры. Эти инвестиции в управление рисками более чем оправдались, позволив в полной мере использовать преимущества безопасности и технического совершенства технологии цифрового дистанционного управления.

Но цифровое дистанционное управление пошло гораздо дальше защитных мер, исключая возмущения и ошибки в системе управления. Так, конструкторы компании Boeing соединили цифровое управление полетом с управлением двигателями и другими системами, чтобы оптимизировать продольный наклон, лобовое сопротивление, уменьшить вес и потребление топлива – и в итоге добились того, что их изделия стали лидерами мировых рынков.

Управление рисками в ИТ

Аналогично тому, как принципы управления рисками действуют в вышеприведенном примере, они определяют и стратегию ИТ-инфраструктуры. ИТ-инфраструктура – кадры, процессы и технологии, стоящие за новыми бизнес-приложениями, – несут с собой радикальные усовершенствования и новые коммерческие возможности, но и создают новые категории риска. Как и в случае цифрового дистанционного управления, управление риском помогает выявить и измерить компоненты ИТ-рисков и определить инвестиции, необходимые для их ограничения. Отсутствие грамотно организованной системы управления ИТ-рисками в организации может привести:

- ▶ к **недофинансированию** мер безопасности, что создает ИТ-риски, которых можно было бы избежать при разумных затратах;
- ▶ к **избыточному финансированию** и напрасному расходованию ресурсов, которые можно было бы эффективнее использовать в других местах;
- ▶ к **отказу от инноваций** из-за переоценки риска и, соответственно, к упущению привлекательных коммерческих возможностей;

► к метаниям между недофинансированием и избыточным финансированием при отсутствии четкого плана (ИТ-аналог возмущений в системе управления, вызываемых действиями пилота).

Управление ИТ-рисками позволяет получить полный эффект от инвестиций в ИТ-инфраструктуру, обеспечивая динамичное и планомерное развитие. ITRM не только служит защитной мерой, но и создает возможность для организаций использовать ИТ-инфраструктуру в качестве ключевого элемента в своей стратегии конкурентной борьбы.

Категории ИТ-риска

К ИТ-рискам относятся уязвимости информационных систем, которые могут привести к прерыванию или нарушению бизнеса, в частности:

- **Риски безопасности.** Включают потерю важных данных или раскрытие конфиденциальной информации в результате мошенничества или воровства.
- **Риски готовности.** Определяются временем простоя и восстановления информационных систем после природных катастроф, отказа или из-за ошибки работника.
- **Риски производительности.** Медленная реакция приложения может привести к потере транзакций, клиентов или партнеров.
- **Риски несоответствия нормативным требованиям.** Судебные издержки и потери репутации в связи с несоблюдением законодательных норм.

Границы затратного подхода

Когда ИТ обслуживали главным образом конторские задачи, ИТ-подразделения придерживались затратного подхода. Они соизмеряли результаты своей работы с условиями соглашений об уровне обслуживания (SLA), сопоставляли расходы с отраслевыми нормами на единицу дохода и на одного работника и следовали практическим рекомендациям по стандартизации, консолидации, автоматизации и управлению ИТ-услугами с целью минимизации затрат. Затратный подход привел многие из них к реализации модели частичного или полного аутсорсинга ИТ-операций. Логика здесь такова: операции поддержки ИТ-инфраструктуры представляют собой универсальные, недифференцируемые службы и не дают конкурентных преимуществ – так почему бы не передать их сторонним поставщикам?

Некоторым затратная стратегия принесла успех – главным образом поставщикам услуг, но рынок быстро нивелировал преимущества большинства организаций, полученные с ее помощью. Консультанты, вендоры и подрядчики делают общим достоянием конкурентов методы сокращения расходов. Стандарты также выравнивают игровое поле для всех. А инновации, такие, например, как распределенные открытые системы, распространяются по рынку столь стремительно, что более мелкие конкуренты быстро начинают получать те преимущества, которые еще недавно были прерогативой крупнейших корпораций.

Чтобы получить долговременные конкурентные преимущества от ИТ-инфраструктуры, сегодня ИТ-руководство компаний имеет на выбор три стратегические альтернативы:

1. Выиграть “гонку ко дну”, превосходя конкурентов в проведении поэтапных временных мер по достижению экономии в структуре затрат.
2. Конкурировать на основе экономии, но в качестве “быстрого преследователя” – перенимая лучшие методы и предоставляя рисковать лидеру.
3. Найти новый способ создания конкурентных преимуществ из инвестиций в инфраструктуру.

Так как ИТ-инфраструктуре принадлежит важнейшая роль в стратегии конкурентной борьбы, концептуальной основой для третьей альтернативы становится управление ИТ-рисками.

Баланс между риском и затратами

Понятие поддержки конкурентоспособности подразумевает удовлетворение потребностей определенного сегмента заказчиков, предоставление продуктов или услуг с определенными параметрами или выполнение требований определенного канала сбыта. Когда стратегическая позиция по этим вопросам определена, с ней согласовывается вся остальная деятельность фирмы в существующих практических и экономических рамках. ИТ-инфраструктура поддерживает конкурентоспособность организации при помощи технологий, кадров и методов, которые обеспечивают обработку, хранение данных и связь для бизнес-приложений и бизнес-процессов.

Но вместо того, чтобы пытаться конкурировать исключительно на основе экономии, передовые ИТ-руководители теперь используют инвестиции в инфраструктуру для согласования ИТ-рисков с затратами, поддерживая точное соответствие между инвестициями в инфраструктуру и общекорпоративной стратегией. Ключом служит баланс: хотя теоретически безрисковая инфраструктура обеспечила бы полную защиту от атак, безотказно справляясь с системными авариями или с последствиями природных катастроф в точном соответствии с нормами, стандартами и правилами безопасности, она потребовала бы неподъемных расходов. Для поиска реалистичного компромисса между рисками и затратами, современные инфраструктурные стратегии используют управление ИТ-рисками.

Язык управления ИТ-рисками наиболее полезен при взаимодействии с бизнесом. ИТ-подразделения слишком долго пользовались в этом диалоге специализированным, техническим языком, переводя проблемы бизнеса в термины SLA, допустимого времени восстановления, допустимого уровня потери данных, числа инцидентов и времени реагирования.

Сегодня наиболее успешные ИТ-менеджеры для согласования стратегии управления инфраструктурой с бизнес-стратегией оперируют понятиями бизнес-рисков и затрат, как это сделали менеджеры фи-

нансовых рисков. Эти стратеги должны давать ответы на следующие вопросы:

- ▶ Какие бизнес-процессы вносят наибольший вклад в увеличение общей конкурентоспособности — то есть, каковы главные отличия компании от конкурентов?
- ▶ Какие процессы наиболее серьезно повлияют на состояние бизнеса в случае их нарушения или прерывания?
- ▶ Каким технологическим рискам эти критические процессы подвержены больше всего: рискам безопасности, надежности, производительности или соответствия нормативным требованиям?
- ▶ Как распределить инвестиции в инфраструктуру — кадры, процессы, технологию и информацию — для достижения оптимального баланса между рисками и затратами?

Управление ИТ-рисками помогает согласовать ИТ-инфраструктуру с конкурентной позиции компании при помощи инвестиций, сбалансированных по окупаемости с учетом риска, которые поддерживают или защищают эту позицию. Этот баланс служит основой управления ИТ-рисками: общекорпоративного подхода к оптимизации инвестиций в ИТ-процессы, кадры и системы с целью повышения конкурентоспособности организации.

Как конкурировать

Классическая бизнес-стратегия ставит отдельные вопросы: где конкурировать и как конкурировать. Общая позиция компании определяет, где она будет конкурировать, а решения по поводу компромисса между риском и стоимостью инфраструктуры помогают определить, как она будет конкурировать в рамках корпоративной стратегии.

Одно из фундаментальных решений, которые приходится принимать, отвечая на вопрос “как конкурировать” — это выбор внутреннего или внешнего источника услуг для поддержки инфраструктуры. Учитывая разнообразие существующих вариантов, эксперты в данной области оценивают тот или иной внутренний источник на основе анализа ответов на следующие вопросы:

- ▶ Какова стратегическая выгода от внутренней реализации деятельности по поддержке инфраструктуры? Можно ли вести эту деятельность каким-то особенным образом, так что заказчики или партнеры заметят определенные преимущества?
- ▶ Насколько велики риски или расходы, если не пользоваться внешними услугами? Сможем ли мы выполнить требования мировых стандартов по риску и затратам и чем грозит их несоблюдение?

Многие повседневно используемые ИТ-сервисы плохо поддаются такому анализу, и вместо того, чтобы уделить больше внимания стратегии оптимальной организации инфраструктуры, менеджеры передают их внешним провайдером услуг. Первоочередным кандидатом на аутсорсинг является деятельность с высоким уровнем риска и слабым стратегическим эффектом. Примером может служить резервное копирование данных: мало кто из клиентов выбирает банк за высокое качество плани-

рования операций резервного копирования. Зато риски от плохой организации системы резервного копирования очень велики и их реализация влечет за собой массу проблем, в числе которых такие события, как пристрастное внимание со стороны совета директоров, публичная огласка и вмешательство регулирующих органов могут оказаться не самыми большими неприятностями.

Вопрос о выборе источника услуг касается также количества внешних поставщиков и разделения ответственности. Что лучше — вступить в тесные отношения с одним-двумя подрядчиками или застраховаться, взаимодействуя с несколькими? Одно время было принято поручать все управление ИТ-инфраструктурой таким компаниям, как EDS или Perot Systems, но теперь многие предприятия отказываются от единого поставщика услуг в пользу более сбалансированного подхода: передача одному-двум главным поставщикам обычных услуг и поручение более специализированных видов деятельности соответствующим специалистам. Например, один крупный производитель напитков передал заботу о большей части своей ИТ-инфраструктуры одному крупному поставщику услуг, а для операций, связанных с обеспечением безопасности, использует специализированную компанию.

Для той деятельности в области инфраструктуры, для которой был выбран внутренний способ доставки, необходимо явно выразить баланс инвестиций в кадры, процессы и технологии. Значительные улучшения в одной сфере без соответствующих изменений в двух других не дают большого эффекта. Исследования по управлению ИТ-рисками показывают, что наиболее эффективные организации демонстрируют лучшие показатели в области кадров, процессов и технологий, тогда как организации с худшими результатами сосредоточены на тактических технологических мерах.

Эти идеи по поводу стратегии конкуренции в целом хорошо известны, но на практике их реализуют лишь немногие организации. Вместо того чтобы начать с выбора источника услуг, а затем распределить инвестиции между кадрами, процессами и технологиями, часто начинают с технологического решения — и на этом останавливаются.

За дело!

От 60 до 80 % всех инвестиций в ИТ идут на инфраструктуру, поэтому достижение максимальной окупаемости таких крупных затрат трудно переоценить. Принципы управления ИТ-рисками помогают прояснить и продемонстрировать проблемы согласования стратегии в области инфраструктуры с конкурентным положением фирмы. Зачем же ждать? Чтобы быстрее начать, наложите стратегию компании на ее ИТ-инфраструктуру, воспользовавшись в качестве руководства теми примерами стратегий, которые содержатся в этой статье. При активном участии руководителей ИТ- и бизнес-подразделений это гарантирует отличный старт на пути к выигршной стратегии бизнеса.

**Грег Хьюз, вице-президент
отделения Global Services,
корпорация Symantec**