

НЕОБХОДИМОСТЬ УПРАВЛЕНИЯ РИСКАМИ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Песоцкая Е.Ю.

Московский государственный областной университет, Москва

Использование информационных технологий (ИТ) является сегодня обязательным условием для эффективного управления предприятием и повышения его конкурентоспособности. Внедрение информационной системы и автоматизация деятельности организации представляет собой достаточно трудоемкий и болезненный процесс, сопровождающийся множеством рисков и непредвиденных ситуаций.

Для решения множества проблем, с которыми сталкиваются руководители ИТ-проектов целесообразно использование корпоративной системы управления рисками, включающей в себя набор организационных принципов, методологий, стандартов, шаблонов документов и процедур по управлению рисками.

На фоне расцвета экономики в России в настоящее время отмечается готовность предприятий тратить немалые деньги на самые передовые информационные технологии (ИТ). Все больше руководителей предприятий понимают необходимость внедрения информационных систем и четко представляют себе те конкурентные преимущества, которые могут дать их производству современные информационные технологии в условиях все возрастающей масштабности сложности реализуемых проектов.

В последние годы заметный рост демонстрировали многие отрасли отечественной промышленности: авиа- и машиностроение, добывающие отрасли, энергетика, нефтегазовый сектор и металлургия и др. Именно в этих сегментах и наблюдался наибольший интерес к активному использованию ИТ. Характерно, что возможности финансирования достаточно крупных ИТ-проектов теперь появились не только у крупных холдингов. Если в советские времена производственное управление, стандарты финансовой отчетности и пр., регулировались жесткими отраслевыми нормативами, то сегодня все определяется условиями рыночной экономики. На многих предприятиях неоднократно сменились акционеры. Нередки случаи, когда в числе владельцев - теперь и западные акционеры. Многие предприятия вошли в состав промышленных холдингов и финансово-

промышленных групп. Таким образом, появились новые управленческие задачи: переход на новую систему бизнес-планирования и финансовой отчетности, обеспечение информационной прозрачности для акционеров, инвесторов и партнеров. А в целом — переход на новые стандарты управления, отвечающие современным условиям рынка.

Процесс управления рисками можно определенно назвать актуальным и необходимым для реализации успешных ИТ-проектов. В условиях развивающегося рынка и спроса на ИТ услуги, их поставщики должны обеспечивать высочайшее качество услуг, которое они могут контролировать только учитывая и анализируя все возможные риски. В числе рисков, в частности, можно отметить непонимание акционерами роли и места информационных технологий, сомнения в окупаемости ИТ-проектов, низкую степень готовности персонала к использованию новых технологий вообще и информационных технологий — в частности, слабую материально-техническую базу многих предприятий, которая препятствует созданию фундамента для развития ИТ.

Современные информационные системы представляют собой достаточно сложные и комплексные решения, и их внедрение, как правило, требует значительных инвестиций со стороны предприятия. ИТ системы - это комплекс про-

граммных и технических средств, которые используются для анализа, хранения и обработки данных. Средства анализа, входящие в ИТ системы, позволяют с высокой скоростью обрабатывать гигантские массивы данных и на основе полученных результатов предлагать корректирующие действия в соответствии со сложившейся ситуацией.

По оценкам международного исследовательского агентства IDC мировой объем ИТ-услуг будет увеличиваться до 20% ежегодно и составит к концу 2006 года 626 млрд. долл. (объем услуг в области разработки ПО должен достигнуть по разным оценкам от 100 до 150 млрд. долл.).

Современные информационные системы представляют собой достаточно сложные и комплексные решения, и их внедрение, как правило, требует значительных инвестиций со стороны предприятия. ИТ системы - это комплекс программных и технических средств, которые используются для анализа, хранения и обработки данных. Средства анализа, входящие в ИТ системы, позволяют с высокой скоростью обрабатывать гигантские массивы данных и на основе полученных результатов предлагать корректирующие действия в соответствии со сложившейся ситуацией.

Современные информационные технологии очень тесно интегрированы в бизнес-процессы компании, связывая все службы и уровни предприятия. Следовательно, любое изменение в информационной инфраструктуре оказывает прямое или косвенное влияние на все стороны деятельности предприятия. Данное обстоятельство значительно затрудняет анализ эффективности внедрения ИТ, поскольку очень сложно выделить влияние информационных технологий на функционирование компании, как отдельную переменную и достаточно трудно охватить все направления влияния используемых ИТ.

Перечислим несколько наиболее типичных, по мнению автора, причин возникновения рисков при реализации ИТ-проектов:

1. Неготовность топ-менеджмента к изменениям в бизнес-процессах предприятия и организационной структуры.

2. Незаинтересованность руководителей основных подразделений и их прямых подчиненных.

3. Смена в ходе реализации проекта менеджера проекта.

4. Недостаточная квалификация менеджера проекта и ответственных исполнителей.

5. Отсутствие ясных и четких методологических основ этого процесса.

Основываясь на перечисленных факторах, управление рисками проектов по внедрению информационных технологий, аппаратного обеспечения, программного обеспечения, технологий хранения информации, сетевых технологий, обеспечивающих коммуникации и информационных систем (ИТ-проектов) заключается в том, чтобы заранее выявить все возможные риски и провести комплекс предупреждающих мероприятий для избежания серьезных проблем во время реализации проекта.

Успех ИТ-проекта зависит от многих факторов. Но из их числа можно выделить три основных: время, качество, ресурсы. Главная задача руководителя ИТ-проекта - уложиться в выделенный бюджет и заданные сроки и обеспечить требуемое качество имеющимися трудовыми ресурсами. Поэтому основные риски, как правило, характерные для любых ИТ-проектов заключаются в несоблюдении сроков реализации проекта, превышения стоимости и несоблюдения параметров качества. Однако основной причиной возникновения этих рисков, особенно в ИТ-проектах, является неготовность предприятия к реализации подобных проектов.

Говоря о проектах внедрения ИТ нужно отметить, что любые новые технологии реализуются в условиях большой неопределенности и негативного воздействия окружающей среды. Это вызвано тем, что осуществление большинства ИТ-проектов, особенно крупных, происходит в условиях, когда трудно применить стандартные методы управления. Уникальность целей проекта и отсутствие подобных практик в компании порождает неопределенность относительно выбора новых технологий, определения методов и

средств достижения поставленной цели, принятия той или иной методологии.

Управление рисками в современных преуспевающих организациях является тщательно планируемым процессом. Процесс управления рисками должен рассматриваться не как отдельно стоящая задача, требующая решения, а как часть изменения общей корпоративной системы управления. Целью управления рисками, в конечном счете, является повышение эффективности бизнеса за счет контроля деятельности компании и максимальная отдача от используемой методики.

Существует множество методик, предлагающих различные варианты и методы управления проектными рисками. Но так как все проекты внедрения, как правило, уникальны в связи со спецификой организации компании, ее структурой и существующими бизнес процессами, всегда находятся некоторые моменты, которые не в полной мере подходят для конкретной компании. Это значит, что процесс управления рисками в значительной мере определяется спецификой отрасли и направлением деятельности предприятия. Часто специалисты разрабатывают собственный подход к управлению рисками, который является комбинацией нескольких методик и специально приспособлен к требованиям компании. Стремительное распространение информационных технологий требует особого внимания и разработке специальных методов управления рисками, связанными с внедрением и использованием информационных технологий на предприятии.

Согласно разнообразным источникам выделяется 6 основных процедур управления рисками, которые можно адаптировать к специфике ИТ-проектов:

1. *Планирование управления рисками* – выбор подходов и планирование деятельности по управлению рисками проекта.

Этот процесс может включать в себя решения по организации, кадровому обеспечению процедур управления рисками проекта, выбор предпочтительной методологии, источников данных для идентификации рисков, регламент выполнения процедур. Важно спланировать управление

рисками, адекватное как уровню неопределенности и риска, так и важности проекта для организации.

По статистике мировой консалтинговой компании Accenture, занимающейся реализацией проектов в области ИТ, на стадии предварительной проработки и планировании внедрения проекта (первые 10%) закладывается более 90% его полезности. Именно в это время закладываются наиболее болезненные последствия: срыв сроков, нереальный бюджет, ущербная функциональность. При этом консультанты и заказчики видят проблемы неодинаково, что приводит к различным методам управления рисками, которые планируются на ранних этапах. Поэтому каждая компания должна разработать собственный план управления рисками, содержащий общие регламенты и рекомендуемые методики.

2. *Идентификация рисков* – определение рисков, способных повлиять на проект, и документирование их характеристик.

Идентификация рисков ИТ-проекта заключается в составлении перечня факторов рисков, которые могут повлиять на выполнения ИТ-проекта в срок, в рамках бюджета и с заданным качеством. Выполнение идентификации рисков требует понимания процессов ИТ внутри компании, понимания бизнеса, поддерживаемого с помощью ИТ и отдельно, ключевых взаимосвязей информационных, производственных и управленческих процессов в компании, их связи с окружением и внешними сторонами.

Начальный список рисков разрабатывается командой ИТ-проекта или группой аналитиков рисков. В качестве средств идентификации может использоваться обзор документации, который предполагает проведение обзора существующих документов группой управления рисками проекта, включает структурированный анализ плана проекта и имеющихся предложений (ограничений), как на уровне всего проекта, так и на уровне отдельных работ. Также могут использоваться методы «мозгового штурма», Дельфи (Delphi), интервьюирование, SWOT-анализ и пр.

3. *Качественная оценка рисков* – качественный анализ рисков и условий их возникновения с целью определения их влияния на успех проекта.

Качественная оценка рисков выполняется на этапах анализа, планирования и реализации проекта с учетом полученных данных в результате идентификации рисков. Примером объективного критерия и качественной оценки в ИТ-проекте может являться вероятность выхода из строя какого-либо оборудования, например ПК, за определенный промежуток времени. Примером субъективного критерия при оценке ИТ риска может являться оценка владельцем информационного ресурса риска выхода из строя ПК. Для этого обычно разрабатывается качественная шкала с несколькими градациями.

Источниками информации, предназначенной для оценки риска ИТ-проекта могут, например, служить:

- техническая инфраструктура для определения технических и технологических рисков;
- требования к безопасности данных для определения рисков информации;
- организационная структура и штатное расписание предприятия для выявления организационных рисков;
- карты технологических потоков для определения технико-производственных рисков;
- договоры и контракты для определения деловых и юридических рисков и пр;

4. *Количественная оценка* – количественный анализ вероятности возникновения и влияния последствий рисков на проект.

При качественной оценке, выполняется ряд мероприятий для определения уровня каждого риска, который также может быть применим для оценки рисков ИТ-проекта. Наибольшее распространение получил метод вероятностной оценки риска, который вычисляется с использованием вероятностного анализа для каждого риска на основе двух факторов: вероятности возникновения и степени управляемости/влияния риска.

5. *Планирование реагирования на риски* – определение процедур и методов по ослаблению отрицательных последствий рисков событий и использованию возможных преимуществ.

Специфические методы реагирования для ИТ-проекта включают в себя дополнительные методы реагирования на риски ИТ, такие как:

- Комплексный подход. Необходимо учитывать тенденции в собственном бизнесе и выбранной области автоматизации, стратегию развития компании, установленные системы, привычки и культуру пользователей.

- Заинтересованность. Привлечение к проекту всех тех, кто будет пользователями системы. Это позволит снизить негативное отношение к проекту и повысить его внедряемость.

- Дробление. Деление проекта на как можно меньшие этапы или на небольшие проекты с отдельными задачами и целями, составляющие проектную программу. Реализовывать систему рекомендуется поэтапно — от прототипа до полноценной системы и от ядра с минимумом функций до функционально богатой версии, то есть «очередями».

- Выделенность. В проекте должно быть два подразделения: одно отвечает за качество проекта, другое — за сроки и стоимость работ.

В соответствии с планом реагирования на риски ИТ-проекта принимается решение об осуществлении или отказе от противорисковых мероприятий.

б. *Мониторинг и контроль рисков* - мониторинг рисков, определение остающихся рисков, выполнение плана управления рисками проекта и оценка эффективности действий по минимизации рисков.

Осуществление мониторинга и контроля рисков может повлечь за собой выбор альтернативных стратегий, выполнение корректирующих действий, перепланирование проекта. Корректируется база данных по рискам, которая может в дальнейшем использоваться при реализации подобных проектов и в текущей деятельности организации. С целью эффективного выполнения плана управления рисками,

между менеджерами проекта и командой управления рисками должно осуществляться постоянное взаимодействие.

В заключении можно сказать, что управление рисками ИТ-проектов - это определение, оценка и контроль эффекта, внутренних и внешних факторов, которые могут негативно повлиять на стоимость и процесс внедрения новых информационных технологий в компании. Таким образом, задачей управления рисками проектов ИТ является своевременное определение факторов, связанных с внедрением информационной системы или системы автоматизации, которые могут негативно повлиять на реализацию проекта внедрения, а также оптимальное планирование действий по минимизации этих факторов.

Использование общедоступной корпоративной системы управления рисками, включающей в себя набор методологий, стандартов и шаблонов документов, имеющий организационную поддержку

руководства, порядок взаимодействий и систематизированный подход к управлению рисками, позволит избежать множества ошибок, которые терпят многие руководители ИТ-проектов.

СПИСОК ЛИТЕРАТУРЫ:

1. Коршунов Г.И. Обеспечение качества сложных систем. СПГУВК. С-Петербург. 2002
2. Найт Ф. Х. Риск, неопределенность и прибыль. М.: Дело, 2003
3. Рогов М. А. Риск-менеджмент. М.: Финансы и статистика, 2001. – 120 с.
4. Черкасов В.В. Проблемы Риска В Управленческой Деятельности, 2-е издание, переб. и допол. М.: "Рефл-бук", К.: "Ваклер", 2002. — 320 с.
5. Project Management Body of Knowledge (PM BOK), Project Management Institute, Drexel Hill, Pennsylvania, 2004. – 401 p.

RISK MANAGEMENT IN INFORMATION TECHNOLOGY

Pesotskaya Ye.Yu.

Moscow state regional university, Moscow

The role of Information Technologies (IT) in organizations nowadays is becoming more and more critical to maintain successful operational management and keep its market competitive advantage. Implementation of new information system and business process automation appears to be highly complicated and tough process for the organization and faces many issues and risks.

To avoid many problems, typical for managers of IT-projects, it is reasonable to use corporate risk management system, which includes set of organizational principles, methodology and standards, document templates and specialized risk management procedures.

