Классификация рисков

Операционный и финансовый риски. Риски, связанные с информацией для принятия решений

Операционный риск касается операционной деятельности компании. Началом научного подхода к изучению операционных рисков можно считать 1967 г. Именно тогда начался большой всплеск турбулентности: доллар перестал быть привязанным к золоту. Это напрямую затронуло сразу все отрасли экономики.

Из теоремы Модильяни-Миллера (1963 г.) нам известно, что стоимость компании не зависит напрямую от величины заемного капитала.

Авторы теоремы высказали предположение о независимости рыночной цены предприятия от структуры корпоративных ценных бумаг (соотношения собственного (акционерного) и заемного (эмиссия облигаций) капитала, условий выплат по выпущенным ценным бумагам и т. п.) для заданного потока дивидендов, при условии рациональности экономических субъектов и совершенстве рынка капитала.

Обоснование состоит в следующем: если финансирование деятельности предприятия более выгодно за счет заемного капитала, а не за счет собственных источников средств, то владельцы акций предприятия со смешанной структурой капитала предпочтут продать часть акций своего предприятия, использовав вырученные средства на покупку акций предприятия, не пользующегося привлеченным финансированием, и восполнив недостаток в финансовых ресурсах за счет заемного капитала. Одновременные операции с ценными бумагами предприятий с относительно высокой и относительно низкой долей заемного капитала приведут в конце концов к тому, что цены таких предприятий будут примерно совпадать.

Вся деятельность компании разбивается на операционную, инвестиционную, финансовую. При учете информации о рисках в операционной деятельности берется период менее одного года. При учете информации о рисках в инвестиционной деятельности период

составляет в среднем один год. При этом учитывается информация о внеоборотных активах, рисках их владения и доходах в будущих периодах. При планировании финансовых рисков рассматриваются открытые источники информации за период свыше одного года. Безусловно, следует пользоваться только проверенными источниками информации, чтобы снизить риски недостоверности и неполноты данных для принятия решений.

Финансовый риск компании заключается в вероятности возникновения неблагоприятных финансовых последствий в форме потери дохода или капитала при неопределённости условий осуществления его финансовой деятельности. Под финансовым понимается риск, возникающий при осуществлении финансового предпринимательства или финансовых сделок, исходя из того, что в финансовом предпринимательстве в роли товара выступают либо ценные бумаги, либо денежные средства в рублях или валюте. Финансовые риски можно разделить на валютный, кредитный, инвестиционный.

Риски подразделяют по совокупности финансовых инструментов на индивидуальные и портфельные.

Индивидуальный финансовый риск характеризует все виды рисков, присущие отдельным финансовым инструментам.

Портфельный финансовый риск характеризует все виды рисков, присущие комплексу финансовых инструментов, объединённых в портфель (например, кредитный портфель предприятия, инвестиционный портфель и т.п.).

По характеризуемому объекту риски подразделяются на риск отдельной финансовой операции, риск различных видов финансовой деятельности, риск финансовой деятельности предприятия в целом.

Риск отдельной финансовой операции характеризует в комплексе все финансовые риски, присущие определённой финансовой операции (например, все риски, связанные с приобретением конкретных акций).

Риск различных видов финансовой деятельности – это, например, риск инвестиционной или кредитной деятельности предприятия.

Риск финансовой деятельности предприятия в целом – это комплекс всех видов рисков, присущих финансовой деятельности предприятия. Он определяется спецификой организационно-правовой формы деятельности предприятия, структурой капитала, составом активов, соотношением постоянных и переменных издержек и т.п.

Операционные риски являются внутренними рисками компании. К ним относятся риск рентабельности и потеря ликвидности, т.е. способности расплачиваться по краткосрочным обязательствам.

Так же как и операционные, риски инвестиционной деятельности относятся к внутренним рискам компании. К ним относятся риск потери права собственности на актив, неспособность актива зарабатывать доходы в будущем.

Например, в России на 2018 год эксперты рынка продуктов питания прогнозировали рост продаж индейки. Некоторые компании понадеялись на это, построили дополнительные производственные мощности в расчете на бурный рост продаж этого вида продукции. Прогноз не оправдался и компании пережили жесткий кризис – в результате остались с построенными производственными мощностями, которые больше никому не нужны. Некоторые игроки были вынуждены уйти с этого рынка продукции.

Финансовые риски относятся к внешним рискам. Например, существует проблема риска смены валютного курса, в основе которого нередко лежат вопросы идеологии. Компании могут быть подвержены дефолту.

Операционная деятельность является основной в деятельности компании и приносит основную часть дохода. Это та деятельность, ради которой создана компания.

Операционная деятельность – это деятельность, связанная с организацией, управлением и совершенствованием производственных систем, на основе которых производятся продукция или услуги компании.

Особенности операционной деятельности определяются, прежде всего, отраслевыми особенностями и характерными особенностями вида деятельности компании: торговая, производственная, финансовая, инвестиционная и другие виды деятельности.

Операционная деятельность имеет следующие особенности:

- является приоритетной по отношению к другим видам деятельности, поскольку обеспечивает производство и доставку потребителю продукции или услуг, производимых компанией;
- ориентирована в основном на товарный рынок и рынок услуг;
- носит регулярный характер;
- связана с операционными рисками.

Операции являются элементом любой деятельности, связанной с созданием продукта, услуги, работы, т.е. любой деятельности, которой свойственны организованность и продуктивность.

Все организационные функции являются операциями, и любая управленческая деятельность включает в себя операционную деятельность. К операционным процессам (операциям) относятся, например, поставки сырья, хранение запасов, производство, техническое обслуживание и ремонт оборудования. От эффективности управления операциями зависит результат производственной деятельности и успех развития компании, поэтому часто понятия «производство» и «операции» используют как взаимозаменяемые, а управление производством называют управлением операциями, или операционной деятельностью.

Управленческий риск

Признаки низкой культуры управления в топ-менеджменте:

- нацеленность на результат по принципу «цель оправдывает средства»;
- неадекватность экономическим условиям;
- нет отчетности, посвященной рискам.

В случае если руководство компании работает по принципу «цель оправдывает средства», могут возникнуть репутационные риски – компания стремится получить прибыль любой ценой, не учитывая интересы потребителей товаров и услуг, что при дальнейшем развитии событий может привести к финансовому краху и уходу с рынка.

В случае неадекватной оценки экономической ситуации резко возрастают риски финансовых потерь уже в ближайшем будущем.

Если в компании отсутствует достоверная финансовая отчетность, это лишает возможности выстраивать долгосрочную стратегию развития компании и понижает привлекательность данного бизнеса в глазах инвесторов или кредиторов, а также возможных партнеров.

По уровню управления можно выделить следующие виды риска:

- федеральный (требует оказания управляющего воздействия на федеральном уровне);
- региональный и межрегиональный (требует оказания управляющего воздействия на региональном и межрегиональном уровнях; прогнозирование наступления рисковых событий на региональном и межрегиональном уровне и принятие мер по их нейтрализации);
- отраслевой (требует оказания управляющего воздействия на отраслевом уровне; сокращение риска за счет мер косвенного воздействия на объективные и прямого влияния на субъективные факторы в отрасли);
- компании (подразделения) (требует оказания управляющего воздействия на уровне предприятия; целенаправленное

воздействие на субъективные факторы, ведущие к потерям, позволяющее максимизировать прибыль);

- рабочего места (анализ, выявление причин риска, зависящих от качества работы менеджера и принятие мер по их устранению).

Современные компании работают в условиях неопределенности, повышенного социального, хозяйственного, финансового, техногенного, природного и других видов риска. Это накладывает большую ответственность на руководителей.

От их работы зависит либо успех компании, либо ее крах. Другими словами, работа руководителей часто обусловливает высокий уровень риска в компании. Риски целесообразно рассматривать, как сумму вероятности совершить ряд ошибок при принятии решений, которые может допустить конкретный руководитель и размер последствий этих ошибок.

Риски, связанные с несоответствием масштаба мышления руководителя масштабам проблемы, резко возрастают при увеличении масштабов проблем.

В любой компании наибольшие риски вызывают руководители, находящиеся на ключевых должностях. Здесь действует правило, что знает, умеет и не боится делать старший руководитель, то знают и умеют делать его подчиненные.

Риски резко возрастают при передаче решений с нижестоящего уровня на вышестоящий.

Риски, связанные с некомпетентностью нескольких руководителей, находящихся на одном уровне управления, многократно возрастают при передаче их решений на более высокий уровень.

Главными виновниками повышения уровня риска в деятельности компании можно считать руководителей высшего уровня управления, принявших на работу ограниченных и недостаточно компетентных руководителей подразделений.

Рассмотрим основные риски, связанные с личностью руководителя компании:

- авантюрность личности – это склонность или способность руководителя к рискованным в смысле честности действиям, которые рассчитаны не на знания и опыт, не на учет возможностей и условий, а на случайный успех. Как правило, руководитель-авантюрист принимает решения при большом дефиците информации в надежде на удачу.
- комплекс вседозволенности – это присвоение руководителем права на нарушение законов, приказов, правил в процессе управленческой деятельности, которое он оправдывает служебной необходимостью. Такие ситуации встречаются, когда руководители считают, что они всегда правы, а всю ответственность перекладывают на подчиненных. И чем выше ранг руководителя, тем чаще встречается этот комплекс;
- склонность к обману, искажению информации, передаваемой на более высокие ступени управления, чтобы, например, представить свою работу в более выгодном свете.

Эта склонность выражается в приукрашивании статистических данных, которые затем становятся базой для искаженной оценки деятельности компании, разработки и принятия необоснованных управленческих решений.

Риск информационных технологий

Развитие бизнеса идет циклически, а IT – по экспоненте либо линейно.

Риск информационных технологий заключается в несоответствии информационных технологий компетенциям компании.

Технология управления проектными рисками не может быть полной, а значит, и приносить ожидаемый эффект, без учета рисков, привносимых ею самой. Факторами риска информационных технологий являются:

- низкая надежность компьютерных носителей данных в сравнении с традиционными бумажными носителями, обусловленная их технической сложностью;
- зависимость от энергоснабжения;
- низкая отказоустойчивость компьютерных систем, обусловленная их многокомпонентностью и многообразием вероятных причин отказа;
- сложность и дороговизна логистики компьютерных систем, обусловленная разнообразием расходуемых и комплектующих материалов, запчастей, требованиями высокой квалификации для определения их взаимной заменимости;
- высокие требования к квалификации кадров (как специалистов в области информационных технологий, так и пользователей), обратной стороной которых является высокая вероятность ошибочных действий, приводящих к утере или повреждению данных.

Любой из этих факторов может моментально разрушить всю систему управления рисками, сосредоточившую значительные затраты рабочего времени и финансовых ресурсов, либо воспрепятствовать ее работе именно в тот момент, когда актуализовался какой-либо проектный риск и требуется развернутая программа действий по его компенсации.

Полностью исключить такую возможность нельзя в принципе. В наибольшей степени это касается кадровых рисков: даже при эталонно отлаженной системе защиты информации и проработанной кадровой политике человеческий фактор остается главным узким местом в любой человеко-машинной системе. Если информация, хранимая на бумажном носителе, требует для своего уничтожения затрат времени и усилий, сопоставимых с затратами на ее считывание и восприятие, то данные в памяти компьютера могут быть уничтожены с той же легкостью и скоростью, с какой они вводятся и обрабатываются. Речь может идти лишь о сведении вероятности отказа информационной системы управления проектными рисками к разумному минимуму.

Как же предупреждать риски информационных технологий? Общие принципы, которые нужно соблюдать для обеспечения работоспособности информационной системы риск-менеджмента, следующие:

- ограничение прав доступа пользователей системы к ее информационным ресурсам и аппаратным средствам строго обоснованным минимумом;
- протоколирование всех действий пользователей системы, связанных с одномоментным изменением значительных объемов данных;
- строгая ответственность за сохранение в тайне параметров учетных записей пользователей, в особенности паролей, и за их соответствие принятому на фирме регламенту компьютерной безопасности;
- видеоконтроль доступа к наиболее ответственным компонентам аппаратного обеспечения информационной системы;
- проведение учебных мероприятий по действиям персонала в нештатных ситуациях (например, при выявлении признаков несанкционированного доступа в корпоративную вычислительную сеть);
- использование распределенной архитектуры баз данных, содержащих информацию о выполняемых проектах, проектных рисках и мерах по их преодолению, и обеспечение избыточности при хранении этой информации;
- функциональное дублирование аппаратных компонентов информационной системы;
- страхование информационных ресурсов, создаваемых в процессе функционирования информационной системы;
- регулярное резервное копирование данных с заранее продуманной и апробированной процедурой их гарантированного восстановления в течение регламентированного промежутка времени в случае необходимости;

- шифрование данных во избежание их попадания в руки конкурентов или злоумышленников;
- постоянное поддержание неприкосновенного запаса расходуемых материалов и комплектующих всех используемых в информационной системе наименований на случай возникновения экстренной потребности в них; своевременное обновление запаса по истечении регламентного срока их хранения, в течение которого они могут прийти в негодность;
- применение специализированных инструментальных средств анализа рисков информационных систем, в числе которых RiskWatch, CRAMM, COBRA и др.

Для большинства компаний, исключая особо крупные, наиболее выгодным решением оказывается аутсорсинг вспомогательных бизнес-процессов, связанных с обеспечением информационной безопасности и сведением рисков к минимуму.

Рассмотрим примеры, демонстрирующие значимость информационных рисков при компьютерных технологиях проектного риск- менеджмента и возможные действия при возникновении рисковых ситуаций.

ПРИМЕР 1

В крупной венчурной компании вышла из строя ЭВМ, на которой функционировал Microsoft Office Project Server. В результате временно утерян контроль над рисками всех выполняемых инновационных проектов при том, что связанные с ними рисковые ситуации возникают ежедневно.
Предложенные меры апостериорного управления риском состоят в срочном приобретении двух компьютеров требуемого класса (3 часа), установке на один из них операционной системы и серверного программного обеспечения (8 часов), восстановлении резервной копии базы данных (6 часов), повторном вводе данных мониторинга и других изменений, сделанных позже последнего резервного копирования (24 часа рабочего времени). Второй приобретенный компьютер в течение двух недель будет тестироваться с помощью специализированных программных средств для проверки его надежности, после чего серверное программное обеспечение и базы данных будут перенесены на него, а

высвободившийся компьютер будет протестирован аналогично, после чего на нем также будет функционировать EPM-сервер в синхронном с первым сервером режиме, что обеспечит наличие двух копий всех данных. Если же в процессе тестирования будут выявлены сбои, ненадежный компьютер будет возвращен поставщику. В течение 41 часа рабочего времени управление проектами и проектными рисками будет осуществляться без информационной поддержки, что приведет к задержке выполняемых проектов в среднем на 1 рабочий день и к финансовым потерям в размере порядка 1 млн руб.
Если бы резервная копия данных EPM-сервера оказалась дефектной (что не исключено, так как для ее изготовления использовались дешевые несертифицированные диски DVD-R вместо надежных, но дорогих и медленных магнитооптических носителей данных), средняя задержка проектов из-за трудности приведения базы данных в рабочее состояние составила бы около 6-8 дней, а финансовые потери составили бы десятки миллионов рублей.

ПРИМЕР 2

В небольшой фирме, реализующей напряженный по времени и технически сложный строительный проект, предусматривающий несколько тысяч работ и использующий около сотни разнообразных ресурсов (включая человеческие), заболел генеральный менеджер проекта. Его заместитель не имеет достаточных навыков работы с программой Primavera Project Planning, в которой реализована информационная модель проекта, вследствие чего мониторинг проекта не проводится. В течение недели проектные работы выполняются почти без отклонений от графика, и существенных проблем не возникает. Но затем по логистическим причинам оказывается невозможным выполнение одной из критических работ, и требуется пересмотреть план, чтобы свести к минимуму допущенное отставание. Заместитель генерального менеджера вынужден ограничиться переносом сроков критических работ на месяц – по истечении этого срока предполагалось возобновление поставки недостающего расходуемого материала. Впоследствии оказалось, что данный план не сбалансирован по персоналу, так как требует присутствия некоторых работников на двух работах одновременно. Руководство фирмы, опасаясь нарастающего отставания от графика, потребовало от своих специалистов отвечать за параллельно выполняемые работы, не считаясь с отсутствием физической возможности для

этого. Специалисты, работая в условиях перегрузки и стресса, не смогли обеспечить требуемое качество работ, и двое из них, опасаясь ответственности, уволились по собственному желанию. Это привело к окончательному срыву проекта и в конечном счете – к банкротству фирмы.
Правильная стратегия фирмы в отношении информационных технологий управления проектами состояла бы в том, чтобы передать услуги по управлению проектами на аутсорсинг. Если это не было сделано изначально (что уже было ошибкой при недостаточном человеческом потенциале команды управления проектом), следовало бы принять такое решение немедленно после заболевания генерального менеджера. Это обошлось бы дорого, но спасло бы фирму от банкротства.

Информационно-технологический риск (ИТ-риск) – вид операционного риска, связанный с несоразмерностью (недостаточностью) функциональных возможностей (характеристик) применяемых информационных, технологических и других систем и (или) их отказов (нарушений функционирования), а также в результате воздействия внешних событий.

ИТ-риск может быть классифицирован по нескольким критериям с учетом уязвимостей, которые могут привести к прерыванию или нарушению бизнес-процессов, таким как:

- риск доступности (недоступность информации или приложений в результате сбоев в работе систем, стихийных бедствий/природных катастроф или ошибки сотрудника, включая период восстановления);
- риск производительности (ухудшение характеристик работоспособности систем/приложений/специалистов или информационных технологий в целом приводит к снижению бизнес-результатов и их ценности);
- риск несоответствия нормативным требованиям (регуляторный риск) (несоответствие системы обработки информации требованиям регулятора, ИТ- или бизнес-политикам, что приводит к штрафам, судебным издержкам или потере репутации в связи с

несоблюдением законодательных норм или последствиям несоответствия политике в области ИТ-безопасности);

- риск безопасности (потеря важных данных или получение доступа и раскрытие конфиденциальной информации в результате мошеннических действий)