Дарья ЛУПАНОВА, Екатерина ПОЛОБОК,
Молдавская экономическая академия

КОНЦЕПЦИЯ РИСК-МЕНЕДЖМЕНТА ДЛЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

This work describes the risk-management system, defines risks, their classification, instruments and also describes stages of risk-management.

Предпринимательская деятельность тесно связана с понятием «риск». Для успешного существования в условиях рыночной экономики предпринимателю необходимо решаться на внедрение технических новшеств и на смелые, нетривиальные действия, что усиливает риск. Поэтому необходимо правильно оценивать степень риска и уметь управлять риском, чтобы добиваться более эффективных результатов на рынке.

Риск-менеджмент представляет собой систему управления риском и экономическими, точнее, финансовыми отношениями, возникающими в процессе этого управления.

В основе риск-менеджмента лежат целенаправленный поиск и организация работы по снижению степени риска – искусство получения и увеличения дохода (выигрыша, прибыли) в неопределенной хозяйственной ситуации.

Главная цель риск-менеджмента – содействие достижению стратегических и тактических целей компании с помощью постоянного сокращения рисков (угроз) до приемлемого уровня, а также времени использование риска как возможности для дальнейшего развития компании и достижения конкурентных преимуществ.

Основная задача риск-менеджмента – идентификация, оценка, анализ и управление рисками. Риск-менеджмент представляет собой постоянный и развивающийся процесс, который анализирует развитие организации в движении, а именно прошлое, настоящее и будущее организации в целом.

Наиболее распространеннымпи инструментами риск-менеджмента являются:

- система ограничений (лимитов);
- диверсификация;
- аналитическая работа;
- хеджирование.

Для эффективного управления информационными рисками разработаны специальные методики, например, методики международных стандартов ISO 27000, ISO/IEC 27005 (BS7799), BSI; а также национальных стандартов NIST 80030, SAC, COSO, SAS 55/78 и некоторые другие, аналогичные им.

Риск характеризуется как опасность возникновения непредвиденных потерь ожидаемой прибыли, дохода или имущества, денежных средств в связи со случайным изменением условий экономической деятельности, неблагоприятными обстоятельствами. Его величина измеряется частотой, вероятностью возникновения того или иного уровня потерь.

Хозяйственные, финансовые и инвестиционные риски представляют собой обязательные атрибуты функционирования субъектов рыночной экономики. Само по себе наличие риска, сопровождающего деятельность того или иного предприятия, не является ни достоинством, ни недостатком. Наоборот, отсутствие риска, то есть опасности наступления непредсказуемых и нежелательных для субъекта последствий его действий, как правило, в конечном счете, вредит экономике, подрывает ее динамичность и эффективность.

Одна из проблем риск-менеджмента – классификация и идентификация рисков. Классификация рисков означает систематизацию множества рисков на основании каких-то признаков и критериев, позволяющих объединить подмножества рисков в более общие понятия.

Наиболее важными элементами, положенными в основу классификации рисков, являются:

- время возникновения;
- основные факторы возникновения;
- характер учета;
- характер последствий;

- сфера возникновения и другие.

По времени возникновения риски распределяются на ретроспективные, текущие и перспективные риски. Анализ ретроспективных рисков, их характера и способов снижения дает возможности более точно прогнозировать текущие и перспективные риски.

По факторам возникновения риски подразделяются на: политические, экономические (коммерческие) риски, социальные, демографические, географические, экологические.

По характеру учета риски делятся на внешние и внутренние.

По характеру последствий риски подразделяются на:чистые риски (иногда их еще называют простые или статические) и спекулятивные риски (иногда их еще называют динамическими или коммерческими).

Классификация рисков ***по сфере возникновения***, в основу которой положены сферы деятельности, является самой многочисленной группой. В соответствии со сферами предпринимательской деятельности обычно выделяют: производственный, коммерческий, финансовый и страховой риск.

По последствиям различают допустимые, критические, катастрофические риски.

Угроза – возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и/или потери информации.

Угрозы бывают преднамеренные и непреднамеренные, внутренние и внешние. Внешние риски составляют около 25% от всех рисков проекта (портфеля проектов) в целом. Остальные 75% – риски внутренние, находящиеся внутри команды проекта и компании, такие как: недисциплинированность, неформализованность процессов, неэффективная система мотивации, нарушенные внутренние коммуникации, неквалифицированный персонал. Наибольшую обеспокоенность вызывают кража конфиденциальной информации и халатность сотрудников, но теперь в этот ряд добавился еще информационный саботаж. Сравнение индексов обеспокоенности внутренними и внешними угрозами показывает, что именно инсайдерские риски превалируют в списке наиболее опасных угроз. Более того, наибольший рейтинг опасности приходится на утечку конфиденциальной информации. Как показало исследование, респонденты очень хорошо осведомлены о негативных последствиях таких инцидентов: о прямых и косвенных финансовых убытках, долгосрочном ущербе для репутации, потере имеющихся клиентов и трудностях в привлечении новых.

Анализ угроз информационной системы

Организация управления рисками должна носить комплексный характер. Она должна основываться на глубоком анализе негативных всевозможных последствий. Анализ негативных последствий предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению (уязвимостей) и, как следствие, определение актуальных угроз информационной безопасности. Исходя из этого, моделирование и классификацию источников угроз и их проявлений, целесообразно проводить на основе анализа взаимодействия логической цепочки: источники угроз – уязвимости – угрозы – последствия.

Управление рисками проекта включает в себя процессы, относящиеся к планированию управления рисками, их идентификации и анализу, реагированию на риски, мониторингу и управлению рисками проекта. Большинство из этих процессов подлежат обновлению в ходе проекта. Цели управления рисками проекта – повышение вероятности возникновения и воздействия благоприятных событий и снижение вероятности возникновения и воздействия неблагоприятных для проекта событий. Процессы управления рисками проекта включают в себя следующие этапы:

I. Планирование управления рисками – выбор подхода, планирование и выполнение операций по управлению рисками проекта.
II. Идентификация рисков – определение того, какие риски могут повлиять на проект, и документальное оформление их характеристик.
III. Качественный анализ рисков – расположение рисков по степени их приоритета для дальнейшего анализа или обработки путем оценки и суммирования вероятности их

возникновения и воздействия на проект.

IV. Количественный анализ рисков – количественный анализ потенциального влияния идентифицированных рисков на общие цели проекта.
V. Планирование реагирования на риски – разработка возможных вариантов и действий, способствующих повышению благоприятных возможностей и снижению угроз для достижения целей проекта.
VI. Мониторинг и управление рисками – отслеживание идентифицированных рисков, мониторинг остаточных рисков, идентификация новых рисков, исполнение планов реагирования на риски и оценка их эффективности на протяжении жизненного цикла проекта. Эти процессы взаимодействуют как друг с другом, так и с процессами из других областей знаний.

Заключение

Риск, как неотъемлемый элемент экономической, политической и социальной жизни общества, неизбежно сопровождает все направления и сферы деятельности любой организации, функционирующей в рыночных условиях.

Нестабильность уровня спроса и предложения, постоянно ужесточающаяся конкуренция, опережающие темпы развития техники и технологии, резкие изменения валютных курсов, неконтролируемая инфляция, непостоянство законодательной базы, а также многие другие негативные факторы, характерные для текущего состояния экономики, создают условия, при которых ни одна (даже самым тщательным образом спланированная) коммерческая операция не может быть осуществлена с заведомо гарантированным успехом. Вследствие этого основным и непременным условием нормального функционирования и развития любой современной организации является умение ее высшего руководства на строго научной основе осуществлять прогнозирование, профилактику и управление рисками. Вследствие чего риск-менедмент является и будет актуальным.

Литература:

1. http://md-management.ru/articles/html/article32511.html
2. http://www.iteam.ru/publications/project/section_40/article_3578/
3. Руководство к Своду знаний по управлению проектами (Руководство PMBOK®) Третье издание 2004 Project Management Institute, Four Campus Boulevard, Newtown Square, PA 19073-3299 USA / США 269
4. Managing Information Security Risks: The OCTAVE^{SM} approach. Addison Wesley. 2002.
5. Steve Purser. A Pracrical Guide to Managing Informational Security. Artech House Inc. 2004.
6. Inside Network Perimeter Security. Sams Publishing. 2005.
7. http://www.tekora.ru/project/35/49/
8. http://www.artkmv.ru/page.php?p=manag_081