ФИНАНСОВЫЙ ДИРЕКТОР

Дата: 08.04.09
Издание: FD.ru

Некоторые аспекты управления информационными рисками в бизнесе

Нижникова Елена (старший менеджер Департамента ИТ-консалтинга и системной интеграции ЗАО «АКГ «РБС»)

Сегодня мы живем в эпоху перемен, в период нарастающего уплотнения событий во времени, усложнения социально-экономических систем, ускорения протекающих в них информационных потоков. Для удержания данных процессов под контролем специалисты все активнее привлекают информационные технологии, а в период кризисных явлений в мировой экономике еще никогда не были так востребованы понятные и надежные системы поддержки принятия решений.

Мировой финансовый кризис поставил предприятия перед необходимостью искать способы выживания в новых условиях. Каждый раз, принимая управленческое решение, хороший руководитель задумывается, к каким последствиям оно приведет, какие возможные риски оно имеет. И как показывает мировой опыт, в будущем вопреки финансовому кризису, а может быть, и благодаря ему, принятие оптимальных управленческих решений будет базироваться на широком применении систем поддержки принятия решений. Одним из ключевых компонентов таких систем является подсистема управления рисками. В статье мы сконцентрируемся на вопросе управления информационными рисками на предприятиях.

Для начала несколько слов о моделировании управления рисками в компании

Есть такой афоризм, что управление – это действие из будущего в настоящем. А моделирование – это задание образа будущего. Именно моделирование различных ситуаций может помочь управленцу определить ресурсы и резервы, которые есть у организации для собственного развития. И именно модель можно применять для управления рисками.

Моделирование рисков позволяет определить вероятное воздействие разного рода событий на деятельность организации, вырабатывать адекватную стратегию управления рисками. Создание моделей рисков помогает заранее определить, как при помощи оперативных мер наилучшим образом минимизировать ущерб и обеспечить действенную защиту компании.

Моделирование может быть использовано для идентификации, количественного анализа рисков, присутствующих в различных ситуациях. Кроме того, оно позволяет определить причинно-следственные связи между рисковыми факторами. Можно также анализировать проблемные области, связанные с риском, и набор соответствующих альтернативных ответных мер.

Если говорить о более высоком уровне управления – стратегическом, то оно также тесно связано с моделированием и анализом, со способностью компаний заблаговременно выявлять основные тенденции, происходящие во внешней и внутренней среде. На отслеживании и выявлении основных тенденций в макро и микро среде строится небезызвестное управление по слабым сигналам. Примером слабых сигналов могут быть слияние и поглощение двух крупных компаний-конкурентов, изменение законодательства в отрасли, в которой функционирует ваша компания, прогнозы о преобразовании мировой финансовой системы, конфиденциальные сведения об изменениях, которые могут затронуть ваш бизнес, и так далее. Имея информацию о слабых сигналах среды, руководство компании получает возможность предпринять ответные меры еще до возникновения так называемых рисковых событий, у компании появляется время для маневра, для накопления гибкости при адаптации к новым условиям. Управление по слабым сигналам особенно важно при антикризисном управлении.

Как правило, редко какая организация может себе позволить осуществлять полный анализ и внешней, и внутренней среды. В этом случае для анализа внешней среды используют результаты научных исследований, прогнозы. Согласно негласной статистике состав информации для обработки слабых сигналов на 60 % состоит из открытых источников (СМИ, Интернет, публикации) и на 40% из агентурной информации.

Выявление слабых сигналов требует применение систем моделирования и интеллектуальной обработки данных. Для выявления ключевых тенденций во внешней среде: в мировой экономике, геополитике, для прогнозов развития технологий созданы целые корпорации, например, американская корпорация RAND, Национальный научный фонд США, Национальный институт научно-технической политики Японии, Департамент науки и инноваций Великобритании. В России тоже есть подобные структуры.

Как говорится, руководитель может знать бухгалтерский учет, но понимание того, как развивается отрасль, какие возможности и угрозы существуют во внешней и внутренней среде организации часто определяет успех в бизнесе. Умение руководства на научной основе осуществлять прогнозирование и управление рисками в современной компании является одним из условий достойного ее развития.

Что такое информационные риски?

Перейдем к рассмотрению информационных рисков компании. Информационные риски – это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий, включая потери значимой для компании информации. Информационные риски связаны с созданием, передачей, хранением и использованием данных с помощью электронных носителей и иных средств связи. Наличие системы управления информационными рисками является обязательным компонентом общей системы обеспечения информационной безопасности компании.

Существует целый ряд стандартов и подходов к обеспечению информационной безопасности компании и управлению информационными рисками. Наибольшую известность в мировой практике управления информационными рисками имеют такие международные спецификации и стандарты как ISO 17799–2002 (BS 7799), GAO и FISCAM, SCIP, COBIT, NIST 800–30, SAC, COSO, SAS 55/78 и некоторые другие аналогичные им.

Основополагающими считаются стандарты серии ISO 27000, включающие шесть стандартов информационной безопасности (по аналогии с другими стандартами системы менеджмента качества ISO 9000). Фактически эти стандарты представляет собой технологию управления информационной безопасностью.

Если говорить о том, что должна включать в себя технология управления режимом информационной безопасности, то следует отметить следующие ключевые элементы:

- Документирование информационной системы с позиции информационной безопасности компании;
- Классификация информационных рисков и профилирование пользователей;
- Качественная и количественная оценка информационных рисков, их анализ;
- Управление информационными рисками на всех этапах жизненного цикла информационной системы, возможно с применением специального программного инструментария;
- Аудит в области информационной безопасности.

Найти и обезвредить, или выявление информационных рисков

В рамках статьи мы рассмотрим один из аспектов управления информационными рисками – это процесс их выявления.

Выявление рисков осуществляется с применением различных методов экспертных опросов:

- Анкетирование;
- Интервьюирование;
- Метод комиссии;
- Мозговой штурм;
- Delfy

В рамках комплексной диагностики рисков могут использоваться при необходимости все методы выявления рисков. Методы экспертных опросов делятся на очные и заочные. К заочным относится анкетирование, к очным – интервью, комиссии, мозговой штурм, Delfy. Очные методы являются более точными, чем заочные, однако требуют больших затрат времени и труда.

Несколько слов о каждом методе.

Анкетирование: заключается подготовке и заполнении экспертами специальных форм (анкет) с целью выявления рисков.

Интервьюирование: относится к индивидуальным методам экспертных опросов и заключается в проведении беседы интервьюером (лицом, проводящим интервью) с экспертом по заранее подготовленным темам и вопросам.

Метод комиссии: заключается в открытой дискуссии по обсуждаемым рискам в рамках специально созданного Комитета по управлению рисками. В процессе проведения обсуждения в Комитете эксперты (участники) высказывают мнения относительно значимости рисков и методов их снижения, приводя аргументы за и против. Окончательное решение выносится голосованием или единолично ведущим дискуссии.

Мозговой штурм: заключается в коллективном обсуждении и выявлении новых идей, ни одна из которых не отвергается в ходе дискуссии. Метод особенно эффективен для выявления рисков, которые могут не выявить другие методы. При

проведении мозгового штурма должен быть участник, письменно фиксирующий и формулирующий идеи, высказываемые другими участниками, после чего зафиксированное обсуждается методом комиссии.

Метод Delfy: не подразумевает прямых дебатов и является комбинацией метода анкетирования и проведения групповых обсуждений. Первая фаза является проведением анкетирования экспертов. Однако после обработки результатов опросов проводится повторное анкетирование экспертов, но уже с имеющейся у экспертов в распоряжении полученной по результатам предыдущей фазы информацией. Данная процедура повторяется несколько раз до достижения приемлемой степени точности (разброса) мнений.

Выявленные риски могут быть оформлены в виде таблицы.

НАИМЕНОВАНИЕ ПОДРАЗДЕЛЕНИЯ										
ID риска	Формулировка риска	Описание рискового события	Источник (причина) риска	Описание последствия рискового события	Бизнес-процесс	Предв. оценка вер-сти риска	Предв. оценка существ. риска	Предв. оценка знач-ти риска	Возможные мероприятия по упр. риском	Лицо, выявившее и оценившее риск

При выявлении рисков, как правило, можно обнаружить более сотни рисков. В качестве примера представляем усеченный реестр информационных рисков на этапе проектирования системы. В реестре информационных рисков определяются факторы риска, которые могут возникать, возможные рисковые события и последствия их наступления, с которыми может столкнуться компания, мероприятия по управлению информационными рисками. Как правило, в рамках постановки системы управления рисками реестр прорабатывается достаточно подробно для всех видов рисков, включая причинно-следственные связи между ними.

Далее каждый риск, приведенный в реестре, необходимо ранжировать исходя из вероятности наступления рискового события и оценки возможного ущерба. Такое ранжирование служит базой создания карты информационных рисков. Вообще карта риска является мощным инструментом для их анализа и группировки по приоритетам. Карта рисков, включая и информационные риски, выполняет важную роль в оценке стратегических действий компании, в прогнозировании и планировании ее деятельности. Процесс ее создания является сложным и зачастую требует привлечения внешних консультантов.

Фактор риска	**Рисковое событие**	**Последствия наступления рискового события**	**Мероприятия по управлению рисками**
1. Разработка и проектирование системы			
Проектные риски (неэффективный план внедрения, отсутствие поддержки со стороны руководства и пользователей, низкая скорость принятия решений по проектным вопросам, отсутствие механизма контроля качества работ проектной команды)	Ошибки расчетов (заложенных планов, методик и алгоритмов)	Срыв сроков реализации проекта. Невозможность достижения планируемых результатов проекта, дополнительные затраты, финансовые потери	Разработка проектного решения на автоматизируемую систему, технического задания на разработку и внедрение программного обеспечения (ПО) в соответствии со стандартами (ГОСТ 34.602-89). Составление детального плана-графика работ по проекту с последующим контролем его исполнения. Наличие Методики внедрения и следование ей при выполнении работ по проекту. Проведение организационных мероприятий по управлению изменениями. Внешний аудит проекта.
2. Программно-аппаратное обеспечение, целостность			
Отсутствие концепции обеспечения технической защиты информации, недостаточное проведение мероприятий по профилактике работы и поддержанию работоспособности комплекса программно-аппаратных средств	Отсутствие/недоступность требуемой информации, сбои в работе аппаратной части ИТ-инфраструктуры	Невозможность своевременного формирования отчётности в системе. Отсутствие возможности оперативного формирования документов в системе. Возможные коммерческие и производственные потери, упущенная выгода, связанные с потерей данных, вынужденной остановкой работы ИВС на время устранения неполадок.	Использование современных средств защиты и дублирования информации, создание резервных копий баз данных. Наличие квалифицированного системного администратора, обеспечивающего бесперебойную работу информационных систем, оперативное восстановление утерянной информации из резервных копий. Разработка концепции обеспечения технической защиты

			информации.
Оборудование размещено в несоответствующем месте	Несанкционированный доступ к информации	Возможная утечка информации, проведение актов информационного вандализма и диверсии, потеря данных. Связанные с этим коммерческие потери, упущенная выгода.	Разработка, реализация и контроль требований к размещению оборудования
Оборудование передачи данных не защищено от перехвата или повреждения	Выход из строя оборудования, потеря данных	Потеря данных, простои сотрудников, финансовые потери	Защита оборудования от перехвата и повреждений
Не ведется учет всех неисправностей и мероприятий по обслуживанию оборудования	Выход из строя оборудования, потеря данных	Невозможно предъявить претензии ответственным за обслуживание сотрудникам, поставщикам оборудования, дополнительные расходы, потери данных, простои	Разработать и вести реестр учета всех неисправностей и мероприятий по обслуживанию оборудования
3. Данные, целостность / пригодность			
Не за каждым информационным активом закреплен ответственный владелец, определена процедура защиты, его месторасположение	Потеря данных, ошибки при вводе данных, несанкционированный доступ	Возможная утечка информации, проведение актов информационного вандализма и диверсии, потеря данных. Связанные с этим коммерческие потери, упущенная выгода.	Разработать регламенты и закрепить ответственных за актуализацию информации по информационным активам
Отсутствие единых стандартов на хранение и предоставление данных для всех систем ИТ-инфраструктуры	Отсутствие/недоступность требуемой информации	Невозможность своевременного формирования отчётности. Отсутствие возможности формирования документов при помощи ПО.	Использование современных средств защиты и дублирования информации, создание резервных копий баз данных. Наличие квалифицированного системного администратора, обеспечивающего бесперебойную работу информационной системы, оперативное восстановление утерянной информации из резервных копий.
4. Функционирование, взаимодействие			
Отсутствие единой политики (документ) по информационной безопасности	Потеря данных, ошибки при вводе данных, несанкционированный доступ	Нарушения регламентов информационных потоков, дополнительные затраты на восстановление целостности данных, снижения качества предоставляемых услуг, финансовые потери	Разработка единой Политики информационной безопасности, доведение ее положений до каждого сотрудника, проведение регулярных внутренних семинаров по принципам информационной безопасности и изменений в них
Не существует (или не покрывает все области) механизма авторизации обращений к информации на ее изменения	Потеря данных, ошибки при вводе данных, несанкционированный доступ	Невозможно установить причину, ответственность и штрафы за нарушения информационной безопасности, целостности и достоверности данных, увеличение количества инцидентов, возрастающие дополнительные затраты на устранение последствий	Внедрить механизмы авторизации, покрывающие все существующие программно-аппаратные средства.
Не осуществляется аудит систем безопасности на независимой регулярной основе	Потеря данных, ошибки при вводе данных, несанкционированный доступ	Снижение эффективности мероприятий по информационной безопасности, понижение уровня информационной безопасности компании затраты, потери	Проводить аудит систем безопасности на независимой регулярной основе.
Нарушение пользователями регламента занесения данных в систему	Отсутствие/недоступность требуемой информации	Искажение информации о текущем состоянии дел. В результате возможны потери, связанные с принятием неправильных управленческих решений, основанных на неполной информации, отсутствием возможности получения достоверной оперативной отчётности.	Создание регламентов, описывающих требования по полноте и срокам регистрации информации в системе. Добавление этих требований в должностные инструкции сотрудников, занимающихся непосредственным вводом информации в систему. Разработка Положения о

		Возможные коммерческие потери, упущенная выгода, связанная с отсутствием достоверной информации.	персональной ответственности за несвоевременный ввод данных в систему.
5. Патентная чистота			
Использование нелицензионного программного обеспечения.	Сбои в работе программного обеспечения, Невозможность добавить новый функционал в систему	Невозможность предъявления претензий фирме-производителю в случае ошибок и сбоев в работе по вине программного продукта. Отсутствие возможности получения поддержки и сопровождения ПО со стороны фирмы разработчика или системного интегратора, обучения сотрудников компании работе в среде данного ПО.	Использование лицензионного ПО. Использование услуг по поддержке и сопровождению ПО со стороны фирмы разработчика или официальных партнёров разработчика.
Использование нелицензионного программного обеспечения.	Отсутствие/недоступность требуемой информации	Потери, связанные с начислением штрафов, конфискации нелицензионного ПО в связи нарушением Закона о защите авторских прав. Нанесение ущерба имиджу компании в связи с распространением информации об использовании компанией "пиратского" ПО.	Использование лицензионного ПО.
6. Несанкционированный доступ			
Не проведена идентификация возможных путей доступа к информации третьих лиц, не установлены возможные основания доступа	Несанкционированный доступ к информации, потеря информации, использование информации третьими лицами в своих целях	Возможная утечка информации, проведение актов информационного вандализма и диверсии, потеря данных. Связанные с этим коммерческие потери, упущенная выгода.	Идентификация возможных путей доступа к информации третьих лиц, установление возможных оснований доступа.
Недостаточный уровень защиты информации	Несанкционированный доступ к информации	Возможная потеря данных, заражение компьютерными вирусами вследствие проведения актов диверсии и саботажа со стороны агентов конкурентов и прочих сторон, заинтересованных в нарушении нормального функционирования компании. Серьёзные финансовые потери, упущенная выгода, связанная со сбоями в работе системы и потерей данных. Усиление позиций конкурентов, связанных с нарушениями нормального функционирования служб и подразделений компании	Использование современных средств защиты информации и средств разграничения прав доступа пользователя к данным информационной системы. Реализация в системе протоколирования и мониторинга действий и операций всех пользователей системы. Контроль за нахождением в АРМ системы несанкционированных пользователей.
7. Ошибки конечного пользователя			
Не подписывается соглашение о конфиденциальности при приеме на работу сотрудников	Ошибки пользователей, Потеря данных, Несанкционированный доступ	Возможная утечка информации, проведение актов информационного вандализма и диверсии, потеря данных. Связанные с этим коммерческие потери, упущенная выгода.	Разработать типовое соглашение о конфиденциальности.
Отсутствует процедура информирования об инцидентах и сбоях в системе информационной безопасности	Ошибки пользователей, Потеря данных, Несанкционированный доступ	Возможная утечка информации, проведение актов информационного вандализма и диверсии, потеря данных. Связанные с этим коммерческие потери, упущенная выгода.	Разработать и внедрить процедуру информирования об инцидентах.
Недостаточный уровень квалификации пользователей. Отсутствие необходимой пользовательской документации на	Ошибки при вводе данных, сбои в работе программного обеспечения	Искажение информации о текущем состоянии дел. Возможные потери, связанные с принятием неправильных управленческих решений, основанных на неполной	Необходимо наличие актуальной эксплуатационно-технической документации, детально предписывающей пользователю его действия при работе с системой. Наличие регламентных

эксплуатируемые ИС.		информации, отсутствием возможности получения достоверной оперативной информации.	и организационных процедур, обеспечивающих своевременный контроль правильности и полноты занесения информации в систему.
8. Неограниченный доступ в Интернет			
Отсутствие антивирусной защиты. Отсутствие регулярного обновления базы данных компьютерных вирусов	Сбои в работе программного обеспечения, отсутствие/недоступность требуемой информации	Невозможность своевременного формирования отчётности. Отсутствие возможности формирования документов при помощи ПО. Практически полная парализация тех видов деятельности предприятия, в которых используется вычислительная техника. Возможность утечки информации, несанкционированного доступа в результате деятельности вирусов - "троянов".	Использование современных средств антивирусной защиты, дублирование информации, создание резервных копий баз данных. Наличие квалифицированного системного администратора, обеспечивающего своевременное обновление антивирусных баз данных, оперативное восстановление утерянной информации из резервных копий. Разработка регламентов по использованию персональных компьютеров работниками компании. Обязательное наличие на каждом компьютере, а также серверах приложений, баз данных и почтовых серверах компании антивирусных программ (мониторов и сканеров).
Отсутствие контроля доступа в Интернет	Несанкционированный доступ к информации	Возможная утечка информации, проведение актов информационного вандализма и диверсии, потеря данных. Связанные с этим коммерческие потери, упущенная выгода.	Использование современных средств защиты информации, дублирование информации, создание резервных копий баз данных. Разработка регламентов описывающих требования к информационной безопасности при использовании персональных компьютеров работниками компании и работе в Internet. Ограничение доступа в Internet.

Фундамент системы управления рисками

Итак, мы коротко затронули тему выявления информационных рисков, но отдельно хотелось бы сказать про тот фундамент, который необходим для системы управления рисками в компании.

Как правило, создание комплексной системы управления рисками, в том числе информационными, в компании не может обойтись без разработки и принятия следующих мер:

1. Разработка нормативной базы функционирования системы управления рисками:

1.1. Политика информационной безопасности, доведение ее положений до каждого сотрудника.

1.2. Политика в области управления рисками.

1.3. Регламенты и методики проведения работ по управлению рисками.

1.4. Дополнения в положения о подразделения и должностные инструкции для подразделений и должностных лиц, принимающих участие в работе по управлению рисками в компании.

2. Создание органов управления, контролирующих и координирующих общую работу по управлению рисками, в частности Комитета по рискам.

3. Внедрение в практику работы подразделений компании (в том числе в Службе контроллинга) современных методов управления рисками (идентификации, оценки рисков, а также контроля эффективности управления рисками).

4. Постепенный переход в долгосрочной перспективе от фрагментарного управления рисками к комплексной системе, в рамках которой управление всеми рисками будет осуществляться на постоянной и регулярной основе.

В заключение отметим, что обязательным условием успешного управления информационными рисками является его непрерывность. Поэтому оценка информационных рисков, а также разработка и обновление планов по их минимизации должны производиться в компании с определенной периодичностью, например раз в квартал. Периодический аудит системы управления рисками, проводимый независимыми экспертами, будет дополнительно способствовать минимизации рисков.

Кейс:

Проблема: Крупная телекоммуникационная компания обратилась в Аудиторско-консультационную группу «Развитие бизнес-систем» с просьбой провести анализ и усовершенствование существующей системы управления рисками.

Результаты внедрения системы управления рисками (ОАО «Сибирьтелеком»).

Во-первых: осознание рисков на всех уровнях компании.

Так, по мнению экспертов, одним из важных моментов проекта по управлению рисками является осознание того, что фактор риска может быть в одном подразделении, рисковое событие – в другом, а последствие – в третьем.

При проведении работы по проекту каждый увидел работу смежных подразделений, потому что основные проблемы возникают на стыке.

Во-вторых, повышение значимости и необходимости управления рисками.

Так, по мнению экспертов, проведение оценки рисков экспертами представляет очень большой интерес. Например, ранее считалось, что в компании велик риск неправильного введения (не введения) информации в учетную систему по первичным документам. По результатам оценки оказалось, что этот риск находится далеко не на первом месте.

Перечень рисков теперь составлен более качественно: рисков стало меньше, риски лучше «привязаны» к деятельности компании.

В-третьих, становление риск-менеджмента стало составной частью корпоративного управления. В ОАО «Сибирьтелеком» создан и действует Комитет по рискам, в который вошли члены высшего руководства компании.

Эксперты также отмечают, что управление рисками дает действенную обратную связь в управлении и способствует повышению рейтинга корпоративного управления.