Министерство образования Республики Беларусь

Учреждение образования
«Гомельский государственный технический университет имени П. О. Сухого»

Кафедра «Менеджмент»

М. В. Заренин

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ РИСКОВ В ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ И КОМПАНИЙ

НАУЧНО-АНАЛИТИЧЕСКИЙ ОБЗОР МАТЕРИАЛОВ
по курсу «Менеджмент»
для студентов экономических специальностей

Гомель 2006

УДК 004.77(075.8)
ББК 65.050я73
З-34

Рекомендовано научно-методическим советом
гуманитарно-экономического факультета ГГТУ им. П. О. Сухого
(*протокол № 9 от 29.06.2005 г.*)

Заренин, М. В.

З-34 Использование информационных технологий рисков в деятельности предприятий и компаний : науч.-аналит. обзор материалов по курсу «Менеджмент» для студентов экон. специальностей / М. В. Заренин. – Гомель : ГГТУ им. П. О. Сухого, 2006. – 22 с.– Систем. требования: PC не ниже Intel Celeron 300 МГц ; 32 Mb RAM ; свободное место на HDD 16 Mb ; Windows 98 и выше ; Adobe Acrobat Reader. – Режим доступа: http://gstu.local/lib. – Загл. с титул. экрана.

Научно-аналитический обзор материалов посвящен теме информационных рисков. Предлагаются вниманию выступления практиков, теоретиков, руководителей и специалистов по вопросам появления рисков и возможных способов их избежания или преодоления.

Для студентов экономических специальностей.

УДК 004.77(075.8)
ББК 65.050я73

Предисловие

Предлагаемый обзор материалов посвящен теме информационных рисков. Под риском, по нашему мнению, понимается «состояние неопределенности в стремлении получить желаемый результат, который может оказаться условным или неудачным».

Проблема IT – рисков рассматривается во многих учебниках и учебных пособиях (См. Деловое планирование. Под ред. В.М. Попова. М., «Финансы и статистика», 1997; М.В. Заренин. Менеджмент. Организация управленческой деятельности, 2000 г.; Т.В. Никитина. Банковский менеджмент. С.Петер. 2002 г. и др.).

В данном обзоре собраны выступления 12[и] практиков и теоретиков, руководителей и специалистов по вопросам IT – рисков на конференциях, и др. «Финансового директора» на протяжении ряда лет. Появление рисков и возможных способов их избежания или преодоления представляет интерес как для студентов, так и для всех интересующихся проблемами управления предприятиями и банками.

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ

Мишель Мур, *партнер компании «Эрнст энд Янг»*

Обеспечение информационной безопасности – одна из главных задач современного предприятия. Угрозу могут представлять не только технические сбои, но и несогласованность данных в различных учетных системах, которая встречается едва ли не у каждой второй компании, а также неограниченный доступ сотрудников к информации.

Информационные риски – это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий. Иными словами, IT – риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи.

IT – риски можно разделить на две категории:

- риски, вызванные утечкой информации и использованием ее конкурентами или сотрудниками в целях, которые могут повредить бизнесу;
- риски технических сбоев работы каналов передачи информации, которые могут привести к убыткам.

Работа по минимизации IT – рисков заключается в предупреждении несанкционированного доступа к данным, а также аварий и сбоев оборудования. Процесс минимизации IT – рисков следует рассматривать комплексно: сначала выявляются возможные проблемы, а затем определяется, какими способами их можно решить.

Выявление IT – рисков

На практике способы выявления IT – рисков ничем не отличаются от способов определения любых других рисков: составляются карты рисков (См. «Финансовый директор» № 10-12 2004 г.), проводится сбор экспертных мнений и т.п.

Выявить наиболее критические информационные риски можно и более простым способом – ответив на следующие вопросы.

1. Способна ли компания контролировать доступ к информационным системам, в которых формируется и хранится финансовая отчетность?

2. Обеспечены ли клиенты компании необходимой информационной поддержкой, то есть могут ли они в нужный момент дозвониться до компании или же связаться по электронной почте?

3. Сможет ли компания в короткий срок интегрировать существующие технологии работы с информацией в системы предприятия, являющегося объектом слияния или приобретения?

Например, в компании установлена одна или несколько учетных систем, с помощью которых финансисты получают данные для составления консолидированной отчетности. При покупке нового предприятия выясняется, что у него установлена другая учетная система. Поэтому у компании должен быть четкий план трансформации такой отчетности в стандарты, принятые на головном предприятии. В противном случае она может потерять оперативный контроль над ситуацией.

4. Позволяет ли организация документооборота компании в существующих системах продолжить ее деятельность в прежнем режиме в случае ухода ключевых сотрудников?

Эта проблема чрезвычайно актуальна для российских компаний, поскольку даже финансовая и бухгалтерская информация зачастую вводится и хранится в произвольном виде, не говоря уже о сведениях, касающихся клиентов и т.п. Это ведет к дополнительным затратам времени новых сотрудников на «вхождение» в курс дела и повышает вероятность возникновения ошибок.

5. Обеспечена ли защита интеллектуальной собственности компании и ее клиентов?

6. Имеет ли компания четкий алгоритм действий в критической ситуации, например в случае сбоев в работе компьютерных сетей или вирусной атаки?

7. Соответствует ли способ работы информационных систем общим задачам компании? (Если перед компанией стоит задача иметь общий центр управления денежными потоками, а учетные системы, установленные в разных филиалах, не связаны между собой, то поставленная задача не будет решена).

Точно определить возможный ущерб от большинства IT – рисков довольно сложно, но примерно оценить их вполне возможно.

Личный опыт

Владимир Исаев, *генеральный директор компании «Фармстер» (Москва)*

При защите проекта бюджета перед Советом директоров мне нужно было обосновать рентабельность установки антивирусной системы. Для этого я подсчитал приблизительные убытки, которые понесет компания при проникновении вируса в компьютерную сеть. Учитывая уровень компьютерной грамотности персонала компании, вероятность того что сотрудник откроет «подозрительное» письмо и запустит вирус, равна 30 %. Частоту, с которой приходя письма с вирусами, тоже можно определить – такие данные публикуются во многих компьютерных изданиях. Для полного же восстановления компьютерной сети после вирусной атаки

нашей IT – службе потребуется один - два дня. Таким образом, издержки на восстановление работы складываются из заработной платы IT – специалиста за эти два дня, операционных издержек, связанных с остановкой работы, а также из средней прибыли, которую компания недополучит за это время. Когда члены Совета директоров увидели, насколько такие расходы превышают стоимость антивирусного программного обеспечения, вопрос о целесообразности покупки отпал.

Как минимизировать IT – риски

Как показывает опыт многих российских компаний, наиболее успешные стратегии предупреждения IT – рисков базируются на трех основных правилах.

Минимизация IT – рисков компании ТНК

Александр Блох, *руководитель Блока информатизации и связи Тюменской нефтяной компании*

В ТНК входит множество территориально удаленных предприятий, поэтому для повышения управляемости IT – инфраструктуры, а также для снижения информационных рисков в компании несколько лет назад были внедрены методология и программное обеспечение ITSM[1]. В результате мы получили централизованную структуру управления информационными технологиями, контроль за работой которой ведется в Москве. С помощью программного обеспечения SAP R/3 были автоматизированы ключевые бизнес-процессы (разведка, добыча, обслуживающие процессы, материально-техническое обеспечение, логистика, финансы, поддержка) в наиболее важных регионах присутствия, а также центральный офис компании. Остальные системы автоматизации бухгалтерского учета и других второстепенных функций также были интегрированы с SAP R/3. Связь с офисами во всех ключевых регионах осуществляется с помощью выделенных линий. Кроме того, единая сервисная служба, в которую поступают все звонки о неисправностях, связанных с работой IT – инфраструктуры, может отслеживать состояние критических точек и заблаговременно предупреждать возможные проблемы. Таким образом, наш топ-менеджмент имеет доступ в режиме он-лайн ко всей финансовой и производственной информации предприятий ТНК, вплоть до отдельной скважины.

При утверждении бюджета проекта по внедрению ITSM инвестиционным комитетом мы не анализировали его эффективность, так

[1] Подробнее об этом см. «Финансовый директор», 2003, № 7-8, с.140

как не могли точно подсчитать экономический эффект. Но все понимали, что с такими сложными процессами и географической удаленностью предприятий, как у нас, необходимо иметь инструмент, который снижает риски операций и улучшает управление ресурсами. В настоящее время на поддержание инфраструктуры уходит приблизительно 40 % всего IT – бюджета компании.

Правило № 1. Доступ сотрудников к информационным системам и документам компании должен быть различен в зависимости от важности и конфиденциальности содержания документа.

Правило № 2. Компания должна контролировать доступ к информации и обеспечивать защиту уязвимых мест информационных систем.

Правило № 3. Информационные системы, от которых напрямую зависит деятельность компании (стратегически важные каналы связи, архивы документов, компьютерная сеть), должны работать бесперебойно даже в случае кризисной ситуации.

Личный опыт

Вадим Корнеев, *начальник отдела внедрения факторинговых технологий АБ «ИБГ НИКойл» (Москва)*

Защита информации в нашем подразделении – это обеспечение непрерывности внутренних бизнес-процессов и безопасности обмена данными с нашими клиентами при использовании информационных систем собственной разработки. На случай возникновения чрезвычайных ситуаций , таких как атаки на основной сервер или сбои в его работе, журнал транзакций (то есть перечень операций, производимых в системе. – *Примеч. редакции*) периодически копируется на резервный сервер, находящийся в другом помещении, поэтому максимальный объем информации, который мы можем потерять, - это данные за последний час работы.

Для организации доступа наших клиентов к данным через сети общего пользования, например Интернет, мы выделили отдельный сервер. На него копируются данные с основного сервера, так что даже если мы не сможем отразить атаку взломщиков, они не получат доступа к внутренней информации компании, а также к электронным архивам, которые хранятся на носителях, не имеющих выхода в интернет. Доступ клиентов к данным обеспечен различными степенями защиты, которые гарантируют конфиденциальность и достоверность.

ФИНАНСЫ: СТРАТЕГИЯ И ТАКТИКА

КАК УПРАВЛЯТЬ РИСКАМИ

Владимир Шаповалов, *директор по управлению рисками компании «Объединенная финансовая группа», канд. экон. наук*

Деятельность любого предприятия неразрывно связана с понятием «риск»: банк, в котором вы держите свои денежные средства, может обанкротиться, деловой партнер, с которым заключена сделка, - оказаться недобросовестным, а сотрудник, принятый на работу, - некомпетентным. Не стоит забывать и о стихийных бедствиях, компьютерных вирусах, экономических кризисах и других явлениях, способных нанести урон компании. Вместе с тем рисками можно управлять так же, как процессами производства или закупки материалов

Для того чтобы компания могла принимать обоснованные решения в условиях неопределенности, она должна выработать политику по управлению рисками. Управление рисками следует регламентировать специальным внутренним документом – программой по управлению рисками. Как правило, она включает следующие разделы:

- определение понятия «риск», принятое на предприятии;
- цели управления рисками;
- классификация и подробное описание основных видов рисков, с которыми может столкнуться компания;
- принципы управления различными видами рисков;
- организация управления рисками.

Политика по управлению рисками должна быть одобрена и принята высшим руководством или акционерами компании. Рассмотрим более подробно все разделы этого документа.

Определение понятия «риск»

Каждый финансовый менеджер имеет свое представление о риске, методах его оценки и способах определения его размеров. В толковом словаре русского языка С. Ожегова риск определяется как «возможная опасность; действие наудачу в надежде на счастливый исход».

Классификация основных видов риска

Для достижения вышеуказанных целей необходимо подробно раскрыть суть основных видов риска, с которыми сталкивается компания. Автор предлагает следующую классификацию рисков: кредитные, рыночные, риски ликвидности, операционные, юридические.

Мнение эксперта

Юрий Костин, *риск-менеджер Департамента корпоративных финансов ОАО «Сибнефть» (Москва)*

На практике существует много различных классификаций рисков. Помимо кредитных, рыночных, операционных, правовых и других рисков нередко выделяют стратегические и информационные.

Стратегические риски представляют собой опасность убытков из-за неопределенности, обусловленной долгосрочными стратегическими решениями компании.

Под информационными рисками понимают вероятность ущерба в результате потери значимой для компании информации.

Кредитный риск

Под кредитным риском подразумевают вероятные потери, связанные с отказом или неспособностью контрагента полностью или частично выполнить свои кредитные обязательства. Доверяя кому-либо свои средства, компания принимает на себя кредитный риск. Например, покупатель может не выполнить обязательства по оплате товаров, после того как они были ему поставлены. Размер ущерба в результате наступления рискового события определяется как стоимость всех непокрытых обязательств контрагента перед компанией в денежном выражении, включая возможные расходы, связанные с возвратом его долга.

Рыночные риски

Рыночные риски характеризуют возможные потери, возникающие в результате изменения конъюнктуры рынка. Они связаны с колебаниями цен на товарных рынках и обменных курсов валют, курсов на фондовых рынках и т.д. К примеру, компания заключила договор на поставку товаров покупателю через определенное время и зафиксировала в договоре цену поставки. Когда подошел срок исполнения обязательств по договору, покупатель отказался от выполнения условий сделки. К этому времени цена на рынке на этот товар значительно снизилась, в результате из-за

реализации товаров по более низкой цене другому покупателю компания понесла убытки.

Рыночным рискам в наибольшей степени подвержены самые ликвидные активы компании (товары, денежные средства, ценные бумаги и т.д.), так как их стоимость во многом зависит от сложившихся рыночных цен.

Риски ликвидности

Риски ликвидности – вероятность получения убытка из-за нехватки денежных средств в требуемые сроки и, как следствие, неспособность компании выполнить свои обязательства. Наступление такого рискового события может повлечь за собой штрафы, пени, ущерб деловой репутации фирмы, вплоть до объявления ее банкротом. К примеру, компания должна рассчитаться по своим кредиторским обязательствам в течение двух недель, но из-за задержки платежа за отгруженную продукцию она не располагает наличными денежными средствами. Очевидно, что со стороны кредиторов к предприятию будут применены штрафные санкции.

Как правило, риск ликвидности наступает по причине непрофессионального управления денежными потоками, дебиторской и кредиторской задолженностями.

Операционные риски

Под операционными рисками подразумеваются потенциальные потери компании, вызванные ошибками либо непрофессиональными (противоправными) действиями персонала компании, а также сбоями в работе оборудования. В качестве примера можно привести риск выпуска бракованной продукции в результате нарушения технологического процесса. По словам риск-менеджера компании «РУСАЛ-УК» **Дениса Камышева,** к операционным рискам промышленной компании необходимо относить и так называемые форс-мажорные риски (например, риски воздействия природных катастроф).

Базельский комитет по надзору за банковской деятельностью[1] характеризует операционный риск как «риск прямых или косвенных потерь из-за неэффективных или разрушенных внутренних процессов, действий людей и систем».

[1] Базельский комитет по надзору за банковской деятельностью (Basel committee on Banking Supervision) – совещательный орган, созданный в 1975 году и объединяющий представителей органов банковского надзора и центральных банков тринадцати развитых государств.

Юридические риски

Юридические риски представляют собой возможные потери в результате изменения законодательства, налоговой системы и т.д. Юридический риск может возникнуть из-за несоответствия внутренних документов компании (клиентов и контрагентов) существующим законодательным нормам и требованиям. К примеру, сделка будет признана недействительной, если договор между организациями оформлен с нарушением юридических норм и правил.

Принципы управления различными видами рисков

Общие принципы управления рисками

Управление рисками начинается с выявления и оценки всех возможных угроз, с которыми компании сталкивается в процессе своей деятельности. Затем осуществляется поиск альтернатив, то есть рассматриваются менее рискованные варианты осуществления деятельности с возможностью получения тех же доходов. При этом необходимо сопоставлять затраты на реализацию менее рискованной сделки и размеры риска, который удастся снизить. Другими словами, не должно получиться так, что компания избежала риска потерять 100 тыс.долл.США, потратив на это 200 тысяч.

После того как риски выявлены и оценены, руководство должно решить, принимать эти риски или уклоняться от них. Принятие рисков подразумевает, что компания берет на себя ответственность по самостоятельному предотвращению и ликвидации последствий этих рисков.

Управление кредитными рисками

Основным инструментом для снижения кредитного риска стало использование банковских гарантий при организации продажи авиаперевозок через агентскую сеть компании. То есть банк гарантирует исполнение части обязательств, принятых на себя контрагентом. Такой подход позволил нам как значительно снизить кредитный риск и потери компании, так и дать нашим контрагентам удобный инструмент для осуществления взаиморасчетов, поскольку отпадает необходимость в отвлечении из оборота значительных денежных средств на осуществление предоплаты, что в результате стимулирует продажу авиаперевозок.

Для эффективного управления кредитными рисками не достаточно установить кредитные лимиты для клиентов – необходимо осуществлять

регулярный мониторинг клиентской кредитоспособности, периодически корректировать рейтинговые таблицы и пересматривать установленные лимиты. Делать это целесообразно раз в квартал либо при наступлении любого значительного события, которое прямо или косвенно может повлиять на кредитоспособность клиента.

Управление рыночными рисками

Управление рыночными рисками, как и кредитными, осуществляется с помощью системы лимитов. Иными словами, при реализации продукции, формировании валютного или инвестиционного портфеля вероятные максимальные потери не должны превышать установленных лимитов.

При определении лимитов за основу берется максимально допустимый единовременный размер потерь, который не повлечет за собой нарушения нормальной деятельности компании. Размер возможных потерь по конкретному активу компании (готовая продукция, валютные портфели, инвестиционные портфели и т.д.), подверженному влиянию рыночного риска, может быть определен как на основании «исторического» анализа, так и путем экспертных оценок.

При управлении рыночными рисками можно установить следующие виды лимитов:

- на сумму сделки по приобретению или реализации продукции, если она заключается на таких условиях, при которых результат ее проведения зависит от колебания рыночных цен;
- на размер валютной составляющей активов, которые снижают вероятность потерь в случае изменения курса какой-либо валюты;
- на совокупный размер собственного инвестиционного портфеля компании.

Пример.

Рассчитаем лимит на сумму сделки по реализации продукции. По условиям сделки компания должна поставить продукцию покупателю через несколько месяцев после заключения договора по заранее оговоренной цене. Капитал компании составляет 100 млн.долл. США; максимально допустимый утвержденный размер единовременных потерь компании – 20 % от капитала, то есть 20 млн. долл. США. На основании исторического анализа, проведенного риск-менеджером, было определено, что максимальный размер потерь при заключении подобной сделки может составлять 50 % от дохода по сделке.

Лимит сделки будет равен 40 млн.долл. США (100 млн.долл. США х 20 % : 50 %).

Таким образом, максимальный размер потерь по сделке в случае наступления наихудшего из возможных рыночных сценариев мы

определили как 50 %. Другими словами, при максимально допустимом размере потерь в 20 млн. долл. США мы можем заключить сделку на сумму 40 млн.долл.США.

Окончательный размер лимита корректируется высшим руководством компании исходя из стратегии развития, наличия свободных денежных средств и отношения компании к риску.

Необходимо также регулярное проведение так называемых стресс-тестингов, то есть моделирование последствий наиболее неблагоприятных событий. К примеру, моделируется ситуация значительного роста цен на сырье и материалы и проводится анализ последствий такого роста для предприятия, делаются выводы и разрабатываются соответствующие меры.

Управление рисками ликвидности

Основой управления рисками ликвидности является анализ планируемых денежных потоков компании. Данные о сроках и размерах поступлений и выплат при составлении бюджета движения денежных средств корректируются с учетом выявленных рисков. Например, при выявлении кассовых разрывов менеджмент компании должен ликвидировать их путем перераспределения денежных потоков либо запланировать получение краткосрочного кредита или займа на покрытие таких разрывов.

Управление операционными рисками

Операционные риски неразрывно связаны с деятельностью предприятии, и управляют ими, как правило, руководители структурных подразделений. К примеру, начальник производственного подразделения контролирует изношенность оборудования и определяет необходимые мероприятия для предотвращения сбоев, связанных с выходом из строя оборудования. По мнению Андрея Новицкого, служба по управлению рисками не может и не должна полностью заменять ту часть работы по управлению рисками, которую фактически осуществляют другие структурные подразделения компании в процессе своей ежедневной деятельности. Риск-менеджер не только сам управляет рисками, но и помогает в этом другим менеджерам.

Личный опыт

Михаил Рогов, *риск-менеджер автопромышленного холдинга «РусПромАвто» (Москва), член GARP (Global Association of Risk Professionals), член правления российского отделения PRMIA (The*

Professional Risk Managers International Association), канд. экон. наук, доцент

В отличие от инвестиционных и банковских учреждений на промышленных и торговых предприятиях преобладают операционные риски. Управление рисками осуществляет руководство – генеральный и финансовый директора, главный бухгалтер, а при постепенном росте компании функции по управлению рисками распределяются между службами безопасности, юридическим отделом, контрольно-ревизионными службами или отделом внутреннего аудита. В любом случае вопросы управления рисками должны контролироваться топ-менеджерами компании, финансовым директором или представителями собственника.

Принципы управления операционными рисками аналогичны способам управления другими видами рисков: выбор критерия управления (установление лимитов или нормы соотношения риска к доходу), идентификация и измерение рисков, а также проведение мероприятий по их оптимизации. В процессе анализа операционных рисков могут использоваться «деревья вероятностей», то есть детальные сценарии возможных исходов событий, которые помогают рассчитать количественные оценки рисков.

Для управления операционными рисками необходимо контролировать сигналы о рисках. в качестве таких сигналов могут выступать и служебные записки об осложнившейся обстановке на каком-либо участке, о частых поломках различных узлов одно и того же станка, свидетельствующие о высокой вероятности его выхода из строя.

Управление юридическими рисками

Управление юридическими рисками основано на формализации процесса юридического оформления и сопровождения деятельности компании. Для того чтобы минимизировать юридические риски, любые бизнес-процессы компании, подверженные этим рискам (например, заключение договора поставки), должны проходить обязательную юридическую проверку.

Для минимизации юридических рисков при осуществлении большого количества одинаковых операций целесообразно использовать типовые формы документов, разработанные юридическим отделом.

Личный опыт

Михаил Рогов

Одна из задач риск-менеджера в процессе управления любыми рисками – отслеживать их концентрацию. Так, для управления юридическими рисками следует ежемесячно запрашивать у юридического отдела реестр незакрытых юридических дел, исков и проблем с указанием

«цены вопроса». Таким образом, у риск-менеджера будет не только информация о проблемах, но и данные о возможных убытках из-за несвоевременного решения этих проблем. Для снижения юридических рисков в компании необходима отлаженная процедура прохождения документов (визирование и согласование), а также разделение полномочий сотрудников.

Организация управления рисками

По мнению Игоря Тарасова, успех программы управления рисками во многом зависит от правильной организации службы управления рисками и разграничения полномочий по оценке, управлению и контролю рисков между подразделениями. Осуществлять эффективное управление рисками, описанное выше, должно специальное подразделение или сотрудник (риск-менеджер). В обязанности подразделения по управлению рисками входит:

- разработка детального плана управления рисками;
- сбор информации о рисках, которым подвержена организация, их оценка и ранжирование, а также информирование о них руководства;
- консультирование подразделений компании по вопросам управления рисками.

Важным моментом организации управления рисками на предприятии является разграничение полномочий риск-менеджера и топ-менеджмента компании или собственников бизнеса. Как правило, полномочия разделяются в зависимости от величины наиболее вероятных потерь в случае наступления рискового события или размера лимита. К примеру, лимит, не превышающий 10 тыс. долл. США, может быть утвержден риск-менеджером, а лимит свыше этой суммы – финансовым директором.

Для обеспечения непрерывности бизнес-процессов при отсутствии или недостаточности какого-то лимита в программе по управлению рисками необходимо прописать полномочия соответствующих лиц компании (а также лиц, замещающих их в случае отсутствия) на одобрение превышения лимитов, сроки ответа на запрос о превышении лимитов, формы соответствующей заявки и т.д.

Также необходимо определить место подразделения по управлению рисками в организационной структуре предприятия и принципы его взаимодействия с другими подразделениями.

Личный опыт

Денис Камышев

На мой взгляд, существуют два основных подхода к организации управления рисками. Первый – так называемая концентрированная модель: все вопросы управления рисками концентрируются в рамках одного структурного подразделения, в которое входят юристы, экономисты, производственники, страховщики и т.д. Второй подход – управление рисками в рамках «распределенной» системы, когда создается

относительно небольшое подразделение мониторинга рисков, а функции по непосредственному управлению рисками передаются в другие отделы. При таком подходе отдел мониторинга рисков разрабатывает корпоративную политику и специфические методики управления рисками компании и передает функции по оперативному управлению в структурные подразделения компании, которые на основании разработанных методик управляют характерными для своего направления деятельности рисками, что часто позволяет избежать дублирования функций в рамках компании.

Андрей Шабанов, *Глава Представительства компании Scala (сотрудничество с соперниками) в России и странах СНГ*

«Мы часто работаем в тендеме с партнерами. Проекты по внедрению ERP-систем, как правило, включают в себя оптимизацию и перестройку существующих бизнес-процессов, интеграцию с другими системами и создание большой корпоративной информационной системы. С 1991 года *Scala* продвигает в России финансовые модули, а с 1996 года и модуль Управления Производством. Мы были первыми на российском рынке, кто предложил своим клиентам полномасштабную ERP-систему. Сейчас наш новый продукт Collaborative ERP – это следующая ступень после ERP-II. Уже в самом названии заложен ответ, в чем отличие системы Collaborative от системы ERP-II, поскольку слово Collaborative означает «сотрудничество с соперниками».

Мы готовы помочь сделать Ваш бизнес успешным. Мы видим себя не просто поставщиком ERP-системы, мы стремимся стать партнером для наших заказчиков».

Приступая к разработке политики по управлению рисками, необходимо быть готовым к кропотливой и сложной работе, в процессе которой предстоит тесно взаимодействовать с различными структурными подразделениями компании. Поэтому руководители всех служб компании должно хорошо понимать цели разработки системы управления рисками.

1. Направить действия персонала компании на предотвращение IT – рисков, а также обеспечить резервные мощности для работы в критической ситуации.

2. Разработать единые стандарты информационных систем в рамках организации, то есть перейти к единым отчетным формам, а также единым правилам расчета показателей, которые будут применяться во всех программных продуктах компании, используемых для этой цели.

3. Классифицировать данные по степени конфиденциальности и разграничить права доступа к ним.

4. следить за тем, чтобы любые документы, обращающиеся внутри организации, создавались с помощью систем, централизованно установленных на компьютерах. Установка любых других программ должна быть санкционирована, иначе риск сбоев и вирусных атак резко возрастет.

5. Внедрить средства контроля, позволяющие отслеживать состояние всех корпоративных систем: в случае несанкционированного доступа система должна или автоматически запрещать вход, или сигнализировать об опасности, чтобы персонал мог принять меры.

Помимо перечисленных мер необходимо подготовиться к последствиям возможных кризисных ситуаций и описать действия компании по выходу из кризиса. Для этого следует:

- проанализировать сценарии проникновения посторонних лиц или не имеющих соответствующих полномочий сотрудников компании во внутреннюю информационную сеть, а также провести учебные мероприятия с целью отработки модели поведения сотрудников, ответственных за информационную безопасность, в кризисных ситуациях;
- разработать варианты решения проблем, связанных с кадрами, включая уход из компании ключевых сотрудников, например составить и ознакомить персонал с планом преемственности управления на предприятии;
- подготовит запасные информационные мощности (серверы, компьютеры), а также резервные линии связи.

Если бизнес компании во многом зависит от состояния ее информационных сетей (например, у фирм, занимающихся разработкой компьютерных программ), необходимо назначит ответственного за разработку, внедрение и контроль исполнения корпоративных правил, направленных на снижение IT – рисков. Желательно, чтобы такой координатор не имел отношения к IT – структуре компании (например, исполнительный директор).

Считается, что сотрудник, который не связан напрямую с информационными технологиями, будет наиболее объективен при организации мероприятий по риск-менеджменту. Его работа должна оцениваться с помощью измеряемых показателей, скажем, время устранения сбоев в работе сервера не должно превышать 30 минут или же частота таких сбоев должна быть не выше, чем два раза в год.

Обязательным условием успешного риск-менеджмента в области информационных технологий является его непрерывность. Поэтому оценка IT – рисков, а также разработка и обновление планов по их минимизации должны производиться с определенной периодичностью, например раз в квартал. Периодический аудит системы работы с информацией (информационный аудит), проводимый независимыми экспертами, будет дополнительно способствовать минимизации рисков.

В заключение отметим, что разработка и реализация политики по минимизации IT – рисков не приносит пользы, если рекомендуемые стандарты и правила неверно используются, например, если сотрудники не обучены их применению и не понимают их важности. Поэтому работа по обеспечению IT – безопасности должна быть комплексной и продуманной.

«Создание системы риск-менеджмента позволит обеспечить стабильность бизнеса и максимизировать прибыль»

Интервью с начальником Управления анализа кризисных ситуаций и рисков компании «Норильский никель» **Шамилем Курмашовым**

- Какие задачи решает риск-менеджер?

На мой взгляд, риск-менеджер должен выявлять и анализировать возможные проблемы предприятия, а также определять, в какой области искать пути их решения (математика, экономика, логика). Основные задачи риск-менеджера – обеспечение руководства компании объективной и полной информацией о ее бизнес-позиционировании, разработка эффективных управленческих решений, направленных на предотвращение кризиса или минимизацию воздействия риск-факторов, что реализуется в корпоративной системе управления рисками.

Для чего разрабатывается система управления рисками?

- Основная цель – это обеспечение оптимального для акционеров компании и инвесторов баланса между максимизацией прибыли и долгосрочной стабильностью бизнеса. Я считаю, что для достижения этой цели освой системы управления рисками должны стать принципы комплексности, непрерывности и интеграции.

Принцип комплексности подразумевает взаимодействие всех подразделений компании в процессе выявления и оценки рисков по направлениям деятельности. При этом передача функций управления подразделению, риски которого контролируются, может нейтрализовать положительный эффект от внедрения процедур управления рисками. Например, отдел сбыта не должен устанавливать лимиты на кредитование покупателей. Такая ситуация создает массу возможностей для злоупотреблений и аналогично той, когда человек сам у себя спрашивает разрешение и сам его дает.

Не менее важным принципом системы управления рисками предприятия является непрерывность, то есть постоянный мониторинг и контроль рисков предприятия. Это необходимо, поскольку условия, в которых работает предприятие, постоянно меняются, появляются новые риски, которые тоже требуют тщательного анализа и контроля.

Также следует соблюдать принцип интеграции, то есть оценивать интегральный риск компании – давать взвешенную оценку воздействия на бизнес всего спектра рисков, начиная от вероятного снижения цен на продукцию и заканчивая возможным ущербом от технологических аварий. На наличие такого риска может указывать неустойчивость ключевых показателей деятельности компании: прибыль, денежный поток и т.д.Этот принцип позволяет учесть взаимосвязь отдельных рисков. Как показывает

практика, выявление таких связей между рисками дает возможность сформировать более взвешенную оценку ситуации и соответственно оптимизировать потребность в объеме средств, необходимых для обеспечения сбалансированной непрерывной деятельности компании.

Помимо этого руководство компании, как правило, интересует, на сколько может снизиться , например, денежный поток от основной деятельности по сравнению с принятым на год планом и что нужно предпринять для устранения негативного эффекта. Для ответа на этот вопрос необходимо оценить все риски компании и в первую очередь интегральный.

- Какие шаги необходимы для построения системы риск-менеджмента?

- Основываясь на опыте нашей компании, могу выделить следующие этапы.

Во-первых, путем анализа бизнес-процессов компании следует выявить риски и отразить их на карте рисков. При анализе бизнес-процессов важно учитывать производственную специфику, уникальность вспомогательных и обеспечивающих производств, а также географическое расположение подразделений компании, так как эти факторы в значительной степени влияют на характер рисков.

Во-вторых, для контроля текущими рисками нужно создать и внедрить систему текущего мониторинга рисков, основанную на системе операционных риск-индикаторов в разрезе всех направлений деятельности компании.

В-третьих, необходимо разработать принципы оценки и прогнозирования рисков и протестировать их на достоверность методом бэк-тестинга, который заключается в следующем. К реальным историческим данным применяются разработанные принципы оценки и прогнозирования рисков, а полученные результаты сопоставляются с реальными событиями, произошедшими в компании. На основания такого сопоставления делается вывод об адекватности системы.

В-четвертых, разрабатываются системы управления рисками, позволяющие осуществлять профилактику их возникновения. Создаются кризис-сценарии – алгоритм действий подразделений компании в кризисных ситуациях. Хочу отметить, что не следует смешивать риск-менеджмент и кризис-менеджмент. Если риск – это возможность наступления какого-нибудь события, то кризис – результат уже состоявшегося события.

И наконец, в-пятых, следует отслеживать, насколько хозяйственная деятельность предприятия с учетом внедрения системы риск-менеджмента соответствует стратегическим целям, определенным руководством предприятия (приводить параметры хозяйственной политики в соответствие с принятой стратегией).

В итоге сотрудники, которые занимаются созданием системы риск-менеджмента, должны выработать четкую политику по управлению рисками, которая обеспечит прозрачность, устойчивость и непрерывность бизнеса.

Дмитрий Волов, *IT-директор ЗАО «Эмпилс» (Ростов-наДону)*

Менеджеры нашего предприятия еще в 1998 году начали рассматривать вопросы, связанные с обеспечением информационной безопасности, в качестве одного из важнейших направлений деятельности наравне с закупками, управлением материальными потоками, планированием производства и т.п. Меры, принимаемые для реализации данного направления, и бюджет, который выделяется для этого, постоянно пересматриваются в соответствии с текущими потребностями компании.

KIT- риска мы относим потери данных из-за сбоя в работе информационных систем, хищение информации, а также передачу информации третьим лицам сотрудниками предприятия. Работа по минимизации таких рисков делится на организационную и техническую. Организационные меры связаны с ограничением доступа к данным. Для этого вся информация классифицируется на общедоступную, для служебного пользования и секретную. Кроме того, содержание информационных потоков можно разделить по назначению:

- данные, которые циркулируют внутри рабочей группы (по определенному проекту);
- данные, предназначенные для исполнителей и руководителей подразделений (заработная плата, индивидуальные задачи);
- данные для руководителей подразделений и топ-менеджмента (планы стратегического развития).

Разработкой регламентов, касающихся информационной безопасности, занимается отдел реинжиниринга и стандартизации бизнес-процессов. Основываясь на этих регламентах, каждый руководитель подразделения формирует для своих сотрудников должностные инструкции и назначает ответственных за соблюдение информационной безопасности в рамках своего подразделения.

Техническая работа по обеспечению информационной безопасности заключается в дублировании важных функций, от которых зависят сохранность и целостность информации, а также непрерывность работы компании (например, установка запасных серверов, систем резервного копирования). Чтобы минимизировать риск сбоев, мы используем только технику от надежных производителей. Затраты на нее окупаются, так как убыток от простоя информационных систем в течение нескольких часов многократно превысит их стоимость, а потеря информации может вообще парализовать работу предприятия.

Обеспечение информационной безопасности – это, в первую очередь, вопрос эффективности затраченных средств, поэтому расходы на защиту не должны превышать суммы возможного ущерба.

поскольку любые расходы на предотвращение рисков должны быть обоснованы, необходимо обязательно рассчитывать их экономическую эффективность. Расчетом эффективности и обоснованием расходов на заседании бюджетного комитета занимается менеджер направления, которое заинтересовано в снижении риска.

Заренин Марат Владимирович

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ РИСКОВ В ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ И КОМПАНИЙ

Научно-аналитический обзор материалов по курсу «Менеджмент» для студентов экономических специальностей

Подписано в печать 29.11.06.
Формат 60x84/16. Бумага офсетная. Гарнитура Таймс.
Цифровая печать. Усл. печ. л. 1,39. Уч. - изд. л. 1,43.
Изд. № 151.
E-mail: ic@gstu.gomel.by
http://www.gstu.gomel.by

Отпечатано на МФУ XEROX WorkCentre 35 DADF
с макета оригинала авторского для внутреннего использования.
Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого».
246746, г. Гомель, пр. Октября, 48, т. 47-71-64.