МЕТОДЫ УПРАВЛЕНИЯ БИЗНЕС-РИСКАМИ И ЭКСПЕРТНЫЕ МЕТОДЫ ИХ ОЦЕНКИ

BUSINESS RISK MANAGEMENT TECHNIQUES AND EXPERT METHODS OF THEIR EVALUATION

УДК 330.131

Мансуров Р. Р. Магистрант 2 курс, кафедра «Вычислительная техника и защита информации» Уфимский государственный авиационный технический университет Россия, г. Уфа

Mansurov R. R. robert.mansurov@gmail.com

Аннотация

В статье рассматривается проблема оценки рисков в бизнес-процессах. Данная проблема носит самостоятельное прикладное значение, как составляющая системы управления безопасностью информационных объектов. Целью исследования являлось изучение существующих подходов к формализации рисков, методик управления рисками, их преимуществ и недостатков. Перспектива дальнейших исследований заключается в разработке экспертной системы как инструмента поддержки принятия решений.

Summary

The article deals with the problem of risk assessment in business processes. This problem is of independent applied value as a component of the security management system for information objects. The purpose of the study was to study the existing approaches to formalizing risks, risk management techniques, their

advantages and disadvantages. The prospect for further research is to develop an expert system as a decision support tool.

Ключевые слова: риск, бизнес-риски, бизнес-процессы, методика, управления, экспертные методы.

Key words: risk, business risks, business processes, methodology, management, expert methods.

В настоящее время, IT играет важную роль во всех областях деятельности человека. Таким образом, следует учитывать не только бизнес-риски, но и IT-риски как их неотъемлемую часть. При разработке стратегий и планов, направленных на минимизации бизнес-рисков, следует сосредоточить внимание на особенностях того или иного коммерческого предприятия или бизнес-процесса и степени влияния информационных технологий на них.

Поэтому важным фактором в повышении уровня информационной безопасности является использование математических методов и моделей в подготовке решений для оценки рисков и их возможной профилактики. Однако применение этих методов в решении различных проблем часто затруднено из-за их сложности. Таким образом, широкое распространение получили экспертные методы оценки рисков.

В условиях нынешней нестабильности экономики разработка и создание экспертной системы для реализации процессов бизнес-планирования, основанной на использовании современных информационных технологий, поможет провести маркетинговые исследования для отрасли или производства услуг, составить финансовый план, а также обеспечить эффективное управление рисками и оценку.

Цель данной статьи заключается в определении методов управления бизнес-рисками, а также методы экспертных оценок их.

Мы живем в веке, когда технологии определяют будущее. Любой, кто занимается бизнесом в реальном времени, знает, насколько важны для бизнеса технологии. На начальных этапах развития бизнес полностью зависел от кадров, но с развитием технологий бизнес старается не отставать от них. Для любого бизнеса технологии важны для повышения его эффективности и достижения успеха. Поскольку технологии имеют неотъемлемое значение для бизнеса, бизнес-риски включают IT-риски.

Рассматривая предпринимательские риски, можно сказать, что не существует единого взгляда на риски и их взаимосвязь (или идентичность) с бизнес-рисками [1].

Бизнес-риск – это риск неадекватной прибыли или даже убытков, связанных с неопределенностью – усилением конкуренции, предпочтениями клиентов, забастовками, изменениями в государственной политике и т. д. Бизнес-риск возникает из-за конкуренции, рыночных условий, ассортимента товаров и т.

Два риска, которые приводят к бизнес-риску:

1. Внутренний риск, возникающий внутри организации. Эти риски управляемы. Они вызваны такими факторами, как забастовки, остановки работы, несчастные случаи на производстве, халатность сотрудников, неисправность оборудования, технологическое устаревание, повреждение товаров, возникновение пожаров и т. д.;

2. Внешний риск, который возникает извне компании и поэтому не поддается контролю. Это может быть вызвано колебаниями цен, изменением вкусов потребителей или государственных норм, форс-мажорными обстоятельствами и т. д. [2; 3].

Исследование IT-рисков позволяет разделить их на три категории:

1) кадровые риски (к ним относятся управление доступом к ресурсам, предоставление его в строгом соответствии с функциями, выполняемыми сотрудником, и мониторинг использования ресурсов.;

2) риски, связанные с отказом или неисправностью оборудования;

3) риски при применении «пиратского» программного обеспечения [4].

Наиболее распространенными в мире методиками управления IT-рисками являются CRAMM, COBIT for Risk, FRAP, OCTAVE; у них есть как определенные преимущества, так и ограничения [5-6].

Метод CRAMM (CCTA Risk Analysis and Management Method) основан на стандартах управления информационной безопасностью и описывает корреляцию между уязвимыми IT-активами и угрозами, которые могут повлиять на IT-активы через эти уязвимости.

Методология COBIT при реализации функции и процесса управления IT-рисками в организации выделяет компоненты, которые оказывают существенное влияние на риски и управление ими [5;7].

Процесс упрощенного анализа рисков (FRAP) описывает подход к качественной оценке рисков. Цель методологии состоит в том, чтобы идентифицировать, оценивать и регистрировать состав информации о безопасности рисков для заранее определенной области исследования.

Для анализа и оценки информационной безопасности создается команда проекта; Результаты мозгового штурма, проведенного командой проекта во время сеанса анализа и оценки рисков ложатся в основу отчёта [6-8].

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) описывает подход к качественной оценке рисков. Текущая версия этого фреймворка - OCTAVE Allegro. Данная методология предназначена для формализации и оптимизации оценки рисков информационной безопасности и обеспечения возможности получения необходимых для организации результатов с минимальными затратами времени и ресурсов.

Подходы к управлению рисками могут различаться в зависимости от методологии, используемой для анализа и управления рисками; все они содержат подробное описание инструкций по реализации каждого из перечисленных этапов управления рисками, а также рекомендации по выбору оптимальной методологии в зависимости от специфики организации.

В современной экономике бизнес-планирование – неотъемлемая часть функционирования любого субъекта, а современная система управления бизнес-процессами – инструмент, необходимый для его успешного функционирования. Система управления проектами субъекта – это сложная IT-система, разработанная на основе соответствующей экономико-математической модели. Решением может стать разработка и создание экспертной системы бизнес-планирования.

Предлагается использовать результаты исследований искусственного интеллекта, а именно технология разработки и создание экспертных систем для предоставления информации и принятием поддержки в качестве методов экономического и математического моделирования для оптимизации управления процессов бизнес-планирования.

Для формализации знаний в экспертных системах следует использовать определенные правила; эти правила устанавливают взаимосвязь между данными и фактами для вывода логических выводов («когнитивных результатов»), подобных тем, которые используются человеком при решении аналогичных проблем.

Такая экспертная система представляет собой интеллектуальную систему предоставления информации и поддержки принятия решений при бизнес-планировании, предназначенную для субъектов хозяйствования в различных отраслях экономики.

Широко используемые экспертные методы – это методы экспертной оценки, которые проводятся группой экспертов в условиях неопределенности или риска. Методы, которые наиболее часто используются в управлении рисками – это метод экспертной оценки, ранжирование, метод Дельфи.

Метод экспертной оценки обычно подразумевает обработку мнений опытных экспертов (квалифицированных специалистов). То есть этот метод предполагает сбор и изучение оценок вероятности потерь разными специалистами на основе собственной интуиции, знаний и опыта. Эти оценки сделаны с учетом всех факторов риска, а также статистики.

Реализация метода экспертной оценки намного сложнее, если количество оценочных показателей невелико. Этот метод часто применяется при разработке современных систем управления информационной безопасностью, а также при прогнозировании и долгосрочном планировании.

Поэтапный подход к оценке рисков основан, прежде всего, на выявлении рисков для каждой стадии проекта отдельно, а затем суммируется общий результат по проекту.

Существуют и другие методы экспертной оценки рисков. Один из них – метод ранжирования. На первом этапе обработки информации все оценки следует расположить в порядке убывания. Далее вычисляется среднее значение всех оценок по формуле среднего арифметического. Полученные значения разделены на четыре равных интервала. В случае, если оценки экспертов попадают в крайние интервалы, этих экспертов просят обосновать свое мнение. Остальные эксперты знакомятся с их обоснованием (при полной конфиденциальности). В следующих раундах обсуждения учитываются те факторы, которые были случайно потеряны экспертами в первом раунде опроса. В результате во втором туре расхождения во мнениях меньше.

Метод Дельфи предполагает отказ от прямого общения экспертов в процессе исследования. Таким образом, суть этого метода заключается в индивидуальном опросе всех членов группы с помощью анкет для выяснения их мнений на основе личного опыта и знаний о будущих гипотетических событиях.

Таким образом, можно сделать вывод, что экспертная оценка рисков – очень эффективный и простой метод анализа возникновения неблагоприятных событий, особенно в области систем управления информационной безопасностью. Более того, благодаря своей простой организации этот метод позволяет охватить широкий круг исследуемых факторов.

Однако из-за исключительной субъективности ответов экспертов необходимо придерживаться определенных правил при проведении экспертизы, а также анализировать степень совпадения мнений экспертов, чтобы определить качество этой экспертизы.

IT-риски являются основным источником бизнес-рисков, поскольку основные процессы предприятия выполняются с использованием информационных технологий. Минимизация рисков и обеспечение максимальной информационной безопасности требует управления IT-рисками с учетом специфики предприятия.

В исследовании описаны методики управления IT-рисками. Были изучены методы CRAMM, COBIT, FRAP и OCTAVE, которые широко используются правительственными и бизнес-организациями по всему миру. Изученные методы имеют как преимущества, так и недостатки для управления рисками и не обеспечивают решения для устранения последствий рисков, которые не были минимизированы или предотвращены.

В статье предлагается применение экспертных систем для решения сложных для человека-эксперта задач оценки рисков. В большинстве случаев экспертные системы эффективны для задач, которые сложно формализовать или не имеют алгоритмического решения.

Таким образом, можно сделать вывод, что при разработке экспертной системы реализована информационная поддержка и оптимизация процессов бизнес-планирования. В свою очередь, использование таких экспертных систем для оценки рисков субъектами позволит им иметь эффективные инструменты для формирования бизнес-планов реализации различных производственных и коммерческих проектов.

Использованные источники

1. What board members need to know – and do. Information technology risks in financial services. URL: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ccg-information-technol¬ogy-risk-in-fs.pdf
2. Сингина А. А. Взгляд на управление рисками информационных систем. Молодой ученый. 2011. № 6. Т. 1. С. 101–105. URL: https://moluch.ru/archive/29/3284
3. Песоцкая Е. Ю. Необходимость управления рисками в области информационных технологий. Современные проблемы науки и образования. 2007. № 6. Ч. 3. С. 48–52. URL: http://www.science-education.ru/ ru/article/view?id=821
4. Пастоев А. Методологии управления ИТ-рисками. Открытые системы СУБД. 2006. № 08. URL: https:// www.osp.ru/os/2006/08/3584582/
5. Коротнев К. Методики управления рисками информационной безопасности и их оценки (ч. 1). 14.05.2018. URL: https://safe-surf.ru/specialists/ article/5193/587932/
6. Коротнев К. Методики управления рисками информационной безопасности и их оценки (ч. 2). 22.05.2018. URL: https://safe-surf.ru/specialists/ article/5194/587935/
7. Управление ИТ рисками. 20.02.2018. URL: https:// www.itexpert.ru/rus/newsline/articles/detail. php?ID=8936.
8. Алексеев А. Управление рисками. Метод CRAMM / ЗАО «ИТ Эксперт». 2010. URL: https://www.itexpert. ru/rus/ITEMS/ITEMS_CRAMM.pdf
9. Аникин И. В. Метод оценки рисков для уязвимостей информационных систем, основанный на нечеткой логике. Информация и безопасность. 2014. Т. 17. № 3. С. 468–471.

Sources used

1. What board members need to know – and do. Information technology risks in financial services. URL: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ccg-information-technol¬ogy-risk-in-fs.pdf

2. Singina A. A. View on risk management of information systems. Young scientist. 2011. no. 6. Vol. 1. Pp. 101-105. URL: https://moluch.ru/archive/29/3284
3. Pesotskaya E. Yu. the Need for risk management in the field of information technology. Modern problems of science and education. 2007. No. 6. Part 3. Pp. 48-52. URL: http://www.science-education.ru/ ru/article/view?id=821
4. The pastoi A. methodology of management of it risk. Open DBMS systems. 2006. No. 08. URL: https:// www.osp.ru/os/2006/08/3584582/
5. Korotnev K. Methods of information security risk management and assessment (part 1). 14.05.2018. URL: https://safe-surf.ru/specialists/ article/5193/587932/
6. Korotnev K. Methods of information security risk management and assessment (part 2). 22.05.2018. URL: https://safe-surf.ru/specialists/ article/5194/587935/
7. It risk management. 20.02.2018. URL: https:// www.itexpert.ru/rus/newsline/articles/detail. php?ID=8936.
8. Alekseev A. risk Management. CRAMM method / it Expert CJSC. 2010. URL: https://www.itexpert. ru/rus/ITEMS/ITEMS_CRAMM.pdf
9. Anikin I. V. risk assessment Method for information system vulnerabilities based on fuzzy logic. Information and security. 2014. Vol. 17. No. 3. Pp. 468-471.