УДК 005.334:004

Т. И. Хитрова
кандидат экономических наук, доцент,
Байкальский государственный университет экономики и права
А. Н. Власов
Байкальский государственный университет экономики и права

МЕТОДИКИ И ТЕХНОЛОГИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

В статье авторы дают определение понятию «информационный риск» как специфический вид риска, возникающий при реализации проектов разработки, внедрения и эксплуатации информационных систем. Информационные риски определяются как важная проблема организации процесса эффективного управления современным предприятием. Отмечаются особенности используемых организационных мер и технических средств контроля и уменьшения риска: противоречие между регламентированностью методик и отсутствием средств формализации и структурирования экспертных знаний, реализуемых в процессе управления. Рассматриваются этапы процесса управления информационными рисками в аспекте исполняемых ими функций, приводится анализ реализации функций процесса управления рисками в методиках и информационных технологиях, присутствующих на российском и зарубежном рынках. Формулируются базовые требования к построению системы управления информационными рисками.

Ключевые слова: информационный риск; управление информационными рисками; функции процесса управления рисками; методики управления рисками; системный анализ; OLAP-технологии; Data Mining; интеллектуальный анализ данных; система поддержки принятия решений.

T. I. Khitrova
PhD in Economics, Associate Professor,
Baikal State University of Economics and Law
A. N. Vlasov
Baikal State University of Economics and Law

METHODS AND TECHNOLOGIES OF INFORMATION RISK MANAGEMENT

The authors of the article give a definition of the concept «information risk» as a specific type of risk arising in implementation of development, introduction and maintenance of information systems. Information risks are determined as an important problem in process structuring of effective management of a modern enterprise. The authors specify the features of the used managerial procedures and technical means of control and risk reduction: a contradiction between method due processes and absence of means for formalization and structuring of expert knowledge implemented in the management process. A consideration is given to the process stages for information risk management in context of their functions used, with an analysis brought forward to implementation of process functions for risk management in methods and information technologies present in the Russian and foreign markets. Basic requirement are formulated concerning building the system of information risk management.

Keywords: information risk; information risk management; process functions for risk management; methods of risk management; systems analysis; OLAP-technologies; Data Mining; intellectual analysis of data; system of decision-making support .

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2014. № 3
http://eizvestia.isea.ru

Мировой опыт и опыт ведущих отечественных предприятий показывает, что решение проблемы невозможно без реализации проектов внедрения и последующей организации информационных систем и технологий. Их использование является обязательным условием успешного функционирования современного предприятия. Реализация проектов разработки, внедрения и эксплуатации информационных систем связана с возникновением специфических рисков различной природы: риски потери информационных активов предприятия, риски невозможности эффективного отображения бизнес-процессов предприятия в автоматизированной информационной системе, риск осуществления преобразований, риски исполнения (связанные с персоналом) и т. п.

В связи с этим их идентификация, выявление особенностей, использование специальных методик и технологий управления рисками становятся существенными проблемами как для предприятия или организации, внедряющей и эксплуатирующей информационную систему, так и для компаний-вендоров, реализующих проект внедрения на условиях аутсорсинга. Наблюдается повсеместное усиление зависимости успешной бизнес-деятельности отечественных компаний от используемых организационных мер и технических средств контроля и уменьшения риска.

Традиционно процесс управления риском слабоформализован, но, имея в качестве объекта задачи разработки, внедрения и эксплуатации информационных систем и технологий, естественно стремиться к регламентации и автоматизации процедур управления риском, связанных с этими процессами. Формализация, как известно, предполагает наличие определенных алгоритмов исполнения процесса и программных систем, реализующих эти алгоритмы. В качестве первых, в данном случае, выступают методики и программы оценки рисков. Их недостатком является невысокий уровень формализации процессов.

К недостаткам программных систем отнесем, прежде всего, невысокий уровень интеллектуализации, выражающийся в отсутствии возможности накопления опыта экспертов, т. е. изменения параметров и структуры системы в процессе ее эксплуатации. В то время как на каждой стадии процесса стандарты и методики управления рисками рекомендуют ведение записей, позволяющих регистрировать информацию о функционировании процесса управления рисками, необходимую для контроля и совершенствования этого процесса, формализация экспертных знаний, содержащихся в этих записях, не предусматривается, инциденты, описывающие ситуации и результаты их разрешения, программными системами не фиксируются.

Понятия «информационный риск» и «управление информационными рисками» появились сравнительно недавно и сегодня вызывают постоянный интерес специалистов в области бизнеса информационных технологий.

Самое узкое определение информационных рисков — это риски утраты, несанкционированного изменения информации из-за сбоев в функционировании информационных систем или их выхода из строя, приводящие к потерям. Наиболее широкое определение информационного риска учитывает возникновение убытков из-за неправильной организации или умышленного нарушения информационных потоков и систем организации. В любом случае последствия информационного риска носят экономический характер, а, следовательно, информационный риск может быть определен как возможность случайного возникновения нежелательных убытков, измеряемых в денежном выражении [1].

Такое расширенное понимание информационного риска совершенно оправданно, если, например, задаться целью оценки риска в широком контексте информационной безопасности компании, включая организацию работ службы безопасности, PR-центра, информационных технологий и др. Однако при этом в круг рассмотрения попадают довольно разнородные риски, подходы к оценке и управлению которыми должны быть разными.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2014. № 3
http://eizvestia.isea.ru

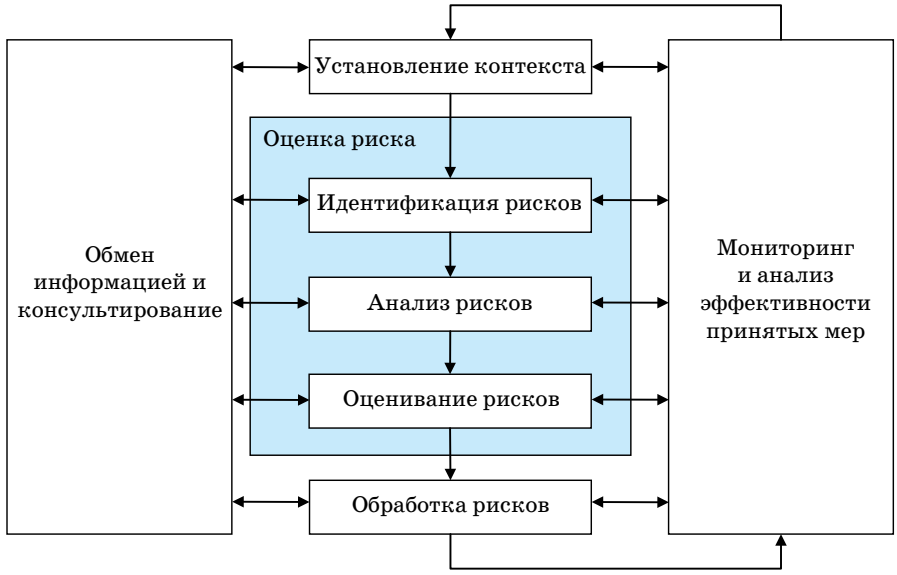
http://eizvestia.isea.ru
2014. № 3
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ

Наиболее целесообразными можно считать комбинированные подходы, сочетающие количественные и качественные методы оценки риска. Интегральный показатель в этом случае включает в себя результаты оценки различных видов риска, представленные в виде численных оценок, полученных на основе объективных значений, так и субъективных качественных значений, соотнесенных заранее с определенными критериями и шкалами [3].

Под термином «управление информационными рисками» обычно понимают комплекс мер по идентификации, анализу и устранению выявленных в структуре информационной безопасности недостатков, которые связаны с разработкой, эксплуатацией и утилизацией информационно-вычислительных комплексов, в соответствии с существующей нормативно-правовой базой и корпоративной политикой безопасности [2]. Считается, что качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации, адекватные текущим целям и задачам бизнеса компании.

Для эффективного управления информационными рисками разработаны специальные методики, например методики международных стандартов ISO 31010, AS/NZS 4360, FERMA, ISO 15408, ISO 17799; а также национальных стандартов ГОСТ Р 51901, NIST 800-30, SAC, COSO ERM, SAS 55/78 и некоторые другие, аналогичные им.

Согласно международному стандарту ISO 31010:2009 процесс управления рисками представляет собой семь взаимосвязанных и взаимодополняющих основных функций (рис.): обмен информацией и консультирование, установление контекста, идентификация рисков, анализ рисков, оценивание рисков, обработка рисков, мониторинг и анализ эффективности принятых мер[1].



Структурная схема процесса управления рисками

Помимо международного стандарта ISO 31010:2009 существуют и другие методики процесса управления рисками, например, такие как:

– американский национальный стандарт ANSI/PMI 99-001-2004[2];

[1] ISO/IEC 31010:2009 «Risk management — Risk assessment techniques». URL : www.iso.org/iso/?csnumber=51073.

[2] Руководство к Своду знаний по управлению проектами (Руководство PMBooK). URL : www.uapa.ru/.../source/2012/12/PMbok4.pdf.

– стандарт «Управление рисками» Австралии и Новой Зеландии AS/NZS 4360:1999[1];

– британский стандарт FERMA[2];

– стандарт COSO ERM[3].

Перечисленные стандарты в определенной степени схожи, но в то же время достаточно различны с точки зрения возможности их использования, которая определяется рядом факторов.

Стандарт FERMA, австралийский стандарт AS/NZS 4360:1999 и международный стандарт ISO разработаны риск-менеджерами для построения системы управления рисками организации любого размера вне зависимости от вида деятельности. Стандарт COSO ERM ориентирован на повышение достоверности отчетности предприятий и удобен для внутренних аудиторов. Стандарт FERMA содержит четко определенную последовательность действий и конкретные рекомендации по построению системы управления рисками. Это упрощает его использование неподготовленным пользователем. Термины американского и австралийского стандартов определены явно, они содержат практические рекомендации по внедрению. Интерпретации стандарта COSO ERM по сравнению с другими стандартами нечетки. Для его применения требуется привлечение к работе подготовленного специалиста, обладающего специальными экспертными знаниями.

У каждого из этих стандартов разные пользователи и разные законодательные требования. Так, американский и австралийский стандарты используются лицами, ответственными за управление рисками в организациях, и носят рекомендательный характер. FERMA предназначен (ориентированы) для риск-менеджеров и фактически представляет собой необязательные рекомендации. Стандарт COSO является обязательным для публичных компаний в США.

Представленные стандарты по разделению процесса управления рисками на отдельные функции способствуют пониманию общемировой тенденции развития механизма управления рисками, но не дают однозначного ответа на вопросы о целях и задачах функций процесса управления рисками. Относительная определенность существует только для функций планирования и идентификации рисков. В отношении остальных функций проявляется главная на сегодня проблема в процессе управления рисками — это определение понятийного аппарата управления рисками, т. е. отсутствие общепризнанных названий и определений. Следующая проблема состоит в том, что ни один из стандартов не содержит рекомендаций по выработке процедур управления рисками.

Комплексный анализ названных методических подходов показал общие моменты в содержании и структуре процесса управления рисками. Во-первых, процесс управления рисками начинается с планирования всего комплекса составляющих его действий. Как и в любом другом случае, планирование является начальной функцией процесса управления, выполняющей в нем важнейшую роль. Во-вторых, следующая функция в процессе управления рисками — идентификация рисков, т. е. определение тех событий и ситуаций, где возможно отрицательное воздействие. Сложность и уникальность процесса в том, что объект управления и его характеристики рассматриваются изначально только в предположении возможности негативных ситуаций.

[1] Совместный стандарт «Управление рисками» Австралии и Новой Зеландии был подготовлен техническим комитетом и опубликован 12 апреля 1999 г.

[2] Federation of European Risk Management Association — Европейская Федерация Ассоциаций риск-менеджмента. В 2002 г. был опубликован Стандарт по управлению рисками (Risk Managment Standart).

[3] Enterprise Risk Management — Integrated Framework Committee of Sponsoring Organizations of the Treadway Commission) — принципы риск-менеджмента, разработанные Комитетом спонсорских организаций Комиссии Тредвея совместно с компанией «PricewaterhouseCoopers».

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2014. № 3
http://eizvestia.isea.ru

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
2014. № 3
http://eizvestia.isea.ru

Анализ позволяет сделать вывод: в понимании начальных функций управления рисками среди во всех рассмотренных подходах противоречия отсутствуют.

На следующем этапе после идентификации объекта управления (т. е. рисков) выполняется оценка их основных характеристик: вероятности наступления негативных ситуаций и последствий их проявления — возникновения и величины возможных потерь. Это ключевой момент в процессе управления рисками.

Полученные данные после идентификации и оценки рисков позволяют определить уровень каждого из них, что является основанием для выбора решений в ситуациях, связанных с рисками. Это может быть одна из альтернатив решения, приводящая к некоему исходу.

В большинстве из названных методических подходов эта, следующая за оценкой рисков, функция управления называется «обработка рисков», которая включает действия по выбору и осуществлению тех или иных мероприятий в соответствии с установленным приемлемым уровнем для каждого идентифицированного риска.

Чтобы обеспечить правильность всех действий в процессе управления рисками вводится функция контроля. Осуществление контролирующих воздействий на мероприятия по обработке рисков одновременно позволяет обеспечивать обратной связью систему управления рисками, что предполагает передачу информации о состоянии объекта управления, а это является базисом для проведения повторных идентификаций и оценок рисков, а также пересмотра способов обработки рисков.

Функция документирования результатов всех действий в настоящее время считается однозначно сложившейся, стандартной функцией, присущей любой из методик процесса управления, в том числе и управления рисками в процессе реализации проекта информатизации.

Таким образом, для проведения полного анализа рисков имеется ряд методик, в том числе реализованных с использованием CASE-средств. Для построения системы управления информационными рисками важно использовать программные продукты, адаптированные к России, которые основываются на структурных методах системного анализа и проектирования.

Методики полного анализа информационных рисков реализуются как зарубежными, так и российскими программными продуктами. Из наиболее известных российских программных продуктов можно выделить программный комплекс «Гриф», разработанный санкт-петербургской компанией «Digital Security», и продукт «Авангард», созданный в Лаборатории системного анализа проблем информатизации Института системного анализа РАН. К сожалению, последний продукт не получил должного распространения в силу проблем, связанных с его поддержкой, развитием и продажей. Из зарубежных программных продуктов наиболее известными являются комплексы CRAMM[1] британской компании «Insight Consulting» и RiskWatch[2] американской компании «RiskWatch». Каждый основывается на своей собственной методике и каждый имеет свои недостатки и достоинства. Один является слишком сложным, другой нельзя адаптировать под конкретную ситуацию, третий формирует слишком много бумажной документации, часто являющейся бесполезной, т. е. перед разработчиками программных продуктов и специалистами в обла-

[1] CRAMM UK — Government's Risk Analysis and Management Method.

[2] В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности: RiskWatch for Physical Security (для физических методов защиты ИС); RiskWatch for Information Systems (для информационных рисков); HIPAA-WATCH for Healthcare Industry (для оценки соответствия требованиям стандарта HIPAA); RiskWatch RW17799 for ISO17799 (для оценки требованиям стандарта ISO 17799).

сти информационной безопасности стоит задача проектирования и разработки программного продукта, который будет лишен всех упомянутых недостатков.

Современные методики и технологии управления информационными рисками позволяют оценить существующий уровень информационных рисков в отечественных компаниях. Это особенно важно в тех случаях, когда к информационной системе компании предъявляются повышенные требования в области защиты информации и непрерывности бизнеса. Существенно, что качественно выполненный анализ информационных рисков позволяет провести сравнительный анализ «эффективность — стоимость» различных вариантов защиты, выбрать адекватные контрмеры и средства контроля, оценить уровень остаточных рисков.

Программная система должна строиться на основе концепции системы поддержки принятия решений: разрабатываться как инструментальное средство анализа рисков, основанное на результатах аналитических исследований с применением технологий OLAP и Data Mining, интеллектуального анализа данных, современных баз знаний и процедурах логического вывода, которые позволяют построить структурные и объектноориентированные модели информационных активов компании, модели угроз и модели рисков, связанных с отдельными информационными бизнес-транзакциями и, следовательно, выявлять такие информационные активы компании, риск нарушения защищенности которых является критическим, т. е. неприемлемым.

Список использованной литературы

1 Зинкевич В. Информационные риски: анализ и количественная оценка / В. Зинкевич, Д. Штатов // Бухгалтерия и банки. — 2007. — № 1. — С. 50–55 ; № 2. — С. 48–53.

2. Тюрин М. Национальные особенности управления информационными рисками / М. Тюрин // BYTE Россия. — 2006. — № 3 (91). — URL : http://www.bytemag.ru/numbers/index.php?ID=11525.

3. Хитрова Е. М. Методы оценки регионального риска и управления им / Е. М. Хитрова // Известия Иркутской государственной экономической академии. — 2008. — № 2 (58). — С. 56–59.

References

1. Zinkevich V., Shtatov D. Information risks: analysis and quantitative evaluation. *Bukhgalteriya i banki – Accounting and Banks*, 2007, no. 1, pp. 50–55; no. 2, pp. 48–53 (in Russian).

2. Tyurin M. National peculiarities of information risk management. *BYTE Rossiya – BYTE Russia*, 2006, no. 3 (91). Available at: http://www.bytemag.ru/numbers/index.php?ID=11525 (in Russian).

3. Khitrova E. M. Evaluation and regional risk management methods. *Izvestiya Irkutskoy gosudarstvennoy ekonomicheskoy akademii – Izvestiya of Irkutsk State Academy of Economics*, 2008, no. 2 (58), pp. 56–59 (in Russian).

Информация об авторах

Хитрова Татьяна Исхаковна — кандидат экономических наук, доцент, кафедра информатики и кибернетики, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: khitra@isea.ru.

Власов Алексей Николаевич — аспирант, кафедра информатики и кибернетики, Байкальский государственный университет экономики и права, 664003, г. Иркутск, ул. Ленина, 11, e-mail: vlasov_an@bk.ru.

Authors

Tatyana I. Khitrova — PhD in Economics, Chair of Computer Science and Cybernetics, Baikal State University of Economics and Law, 11 Lenin St., 664003, Irkutsk, Russia, e-mail: khitra@isea.ru.

Aleksey N. Vlasov — PhD student, Chair of Computer Science and Cybernetics, Baikal State University of Economics and Law, 11 Lenin St., 664003, Irkutsk, Russia, e-mail: vlasov_an@bk.ru.

http://eizvestia.isea.ru
2014. № 3
ИЗВЕСТИЯ ИРКУТСКОЙ ГОСУДАРСТВЕННОЙ ЭКОНОМИЧЕСКОЙ АКАДЕМИИ (Байкальский государственный университет экономики и права)
ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ