На правах рукописи

Завгородний Виктор Иванович

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ

Специальность: 08.00.13 – Математические и инструментальные методы экономики

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора экономических наук

Москва – 2009

Работа выполнена на кафедре «Информационные технологии» ФГОУ ВПО «Финансовая академия при Правительстве Российской Федерации»

Научный консультант: доктор экономических наук, профессор **Чистов Дмитрий Владимирович**

Официальные оппоненты: доктор экономических наук, профессор **Емельянов Александр Анатольевич**

доктор экономических наук, профессор **Лагоша Борис Александрович**

Заслуженный деятель науки РФ

доктор экономических наук, профессор **Чеботарёв Станислав Стефанович**

Ведущая организация: **Федеральное государственное унитарное предприятие «Российский научно-технический центр информации по стандартизации, метрологии и оценке соответствия»**

Защита состоится « 24 » февраля 2010 г. в 10-00 на заседании совета по защите докторских и кандидатских диссертаций Д 505.001.03 при ФГОУ ВПО «Финансовая академия при Правительстве Российской Федерации» по адресу 125993, Москва, Ленинградский проспект, д. 55, аудитория 213.

С диссертацией можно ознакомиться в диссертационном зале библиотечно-информационного комплекса ФГОУ ВПО «Финансовая академия при Правительстве Российской Федерации» по адресу: 125993, Москва, Ленинградский проспект, д. 49, комн. 203.

Автореферат разослан « 19 » января 2010 года и размещен на официальном сайте Высшей аттестационной комиссии Министерства образования и науки Российской Федерации http://vak.ed.gov.ru.

Ученый секретарь совета Д 505.001.03,
кандидат экономических наук,
доцент — О.Ю. Городецкая

1. Общая характеристика работы

Актуальность избранной темы. Процесс повсеместного внедрения новых информационных технологий в бизнес-процессы предприятий является одним из основных факторов существенного повышения эффективности современной экономики. Информатизация экономики требует значительных инвестиций в информационную сферу. По данным исследовательской фирмы International data corporation,[1] мировые расходы на информационные технологии в 2009 году даже в условиях экономического кризиса составят 1,8 триллиона долларов.

Возрастание значения информации и информационных технологий для каждого предприятия сопровождается усложнением задач управления информационной сферой. Важнейшими из них являются рациональное использование инвестиций в информационные технологии и снижение рисков, связанных с информационными процессами предприятия. В современной научной литературе, в национальных и международных стандартах уделяется большое внимание проблемам управления рисками, связанными с использованием информации в деятельности предприятий. Вместе с тем остается нерешенным целый ряд проблем.

Главная из них – отсутствие методологий управления информационными рисками предприятий, обеспечивающих системный подход к управлению информационной сферой предприятия, ориентированных на достижение конечного результата бизнес-процессов, согласованное использование методов и моделей.

Как правило, проблемы управления качеством и безопасностью информации не интегрируются в единую проблему управления информационной сферой предприятия, с едиными показателями качества и эффективности, ориентированными на конечные результаты деятельности предприятия. Под управлением информационными рисками понимается только процесс обеспечения безопасности информации. Такой подход затрудняет создание методического аппарата комплексного решения задачи обеспечения качества и безопасности информации, ведет к снижению эффективности управления рисками всей информационной сферы предприятия.

Недооценка важности комплексного подхода к управлению информационными рисками не позволяет установить взаимосвязи информационных и экономических рисков, сказывается на организационном и технологическом уровнях управления информационными рисками. Управлением занимаются, в основном, специалисты отделов информационной безопасности и отделов информационных технологий. Существующие организационные структуры предприятий и технологии управления не позволяют использовать в полной мере возможности руководства и менеджмента различных уровней в процессе управления информационными рисками.

Степень разработанности проблемы. Различные аспекты управления информационными рисками нашли отражение в работах отечественных и зарубежных ученых. Проблемы, связанные с экономическими рисками, исследова-

[1] http://www.idc.com

ны в работах многих ученых, среди которых Балабанов И.Т., Бернстайн П., Бланк И.А., Блек Ф., Дункан Р., Ильенкова Н.Д., Красс М.С., Лаврушин О.И., Лагоша Б.А., Лиис Ф., Луман Н., Маркович Г., Мертон Р., Мильнер Б., Найт Ф.Х., Салин В.Н, Самуэльсон П., Сенчагов В.К., Фомичев А.Н., Чеботарев С.С., Шоулс М. Учеными разработаны общие закономерности и принципы управления экономическими рисками, проведен анализ, классификация и систематизация рисков, а также даются научно-методические и практические рекомендации по управлению рисками в различных областях экономики. Вместе с тем информационные риски как разновидность экономических рисков рассматриваются лишь в работах отдельных ученых. Результатом такого подхода является недооценка важности управления информационными рисками и экономических методов управления информационными рисками.

Современная информатика является теоретическим базисом построения информационных систем, обеспечения качества и безопасности информации. Основы информатики заложили следующие выдающиеся ученые: Берг А.И., Винер Н., Глушков В.М., Ершов А.П., Канторович Л. В., Келдыш М.В., Колмогоров А. Н., Лебедев С.А., Ляпунов А.А., Марчук Г.И., Мочли Д.У., Джон фон Нейман, Семенихин В.С., Соболев С.Л., Трапезников В.А., Экерт Д.П. и другие.

Методологической базой исследования сложных систем, к которым относятся информационные системы, является теория систем и системный анализ. Наибольший вклад в развитие этого научного направления внесли Акофф Р., Берталанфи Л., Волкова В.Н., Денисов А.А., Дрогобыцкий И.Н., Емельянов А.А., Клейнер Г.Б., Макол Р.Е., Месарович М., Оптнер С., Перегудов Ф.И., Поспелов Д.А., Прангишвили И.В., Черняк Ю.И., Черчмен У. и другие. Методы и нотации структурного системного анализа, а также поддерживающие их CASE-системы представлены в трудах Буча Г., Гейна К., Йордана Э., Калянова Г.Н., Росса Д., Сарсона Т., Шеера А.-В., Якобсона И. и др.

Проблемы оценки качества информации и надежности аппаратных и программных средств рассматриваются в трудах Байхельта Ф., Герасименко В. А., Липаева В.В., Майерса Г., Ушакова И.А., Франкена П., Ясина Е.Г. и др.

Математические методы, модели и инструментарий анализа и оценки рисков представлены в работах Емельянова А.А., Костогрызова А.И., Кульбы В.В., Степанова П.В., Хрусталева Е.Ю. и многих других.

Тематика обеспечения информационной безопасности нашла отражение в работах таких ученых как Бородакий Ю.В., Галатенко В.А., Герасименко В.А., Грушо А.А., Зегжда П.Д., Кастельс М., Конявский В.А., Мафтик С., Мун С., Петренко С.А., Росс Г.В., Стенг Д.И., Тимонина Е.Е., Хоффман Л.Дж., Щербаков А.Ю. и др.

В настоящее время теория и практика создания аппаратно-программных средств и технологий их применения успешно развиваются. Сложнее решаются вопросы, связанные с обеспечением качества первичной информации, формальным представлением и оценкой эффективности взаимодействия человека с техническими системами. Не решена задача интегральной оценки влияния качества и безопасности информации на развитие других экономических рисков, на конечные результаты деятельности предприятий.

В последние годы особую остроту приобрели проблемы обеспечения безопасности информации. Этим и объясняется внимание к вопросам информационной безопасности со стороны отечественных и зарубежных ученых и специалистов. Наибольшее внимание ученые уделяют развитию механизмов обеспечения информационной безопасности, основанных на использовании аппаратных, программных и криптографических средств защиты. Следует также отметить отдельные исследования в области теории построения систем защиты информации, создания методического и инструментального аппарата анализа отдельных рисков. В то же время не развита методология оценки безопасности информации с позиций достижения конечных целей бизнеса и применения экономических методов управления информационными рисками.

Пока еще не создана концепция управления информационными рисками, в которой бы с системных позиций рассматривались все составляющие качества и безопасности информации, влияющие на эффективность ее использования в бизнес-процессах.

Существующие методы и средства анализа информационных рисков не объединены в рамках единой методологии, и могут применяться, как правило, только для исследования отдельных вопросов безопасности и качества информации. Не уделяется должного внимания использованию методов мягких вычислений для решения проблем анализа и синтеза систем управления информационными рисками.

В целом можно сделать вывод об актуальности и недостаточной степени разработанности проблемы управления информационными рисками на теоретическом, методологическом и методическом уровнях, что и обусловило выбор темы настоящего исследования и определило его цели и задачи.

Целью диссертационной работы является решение научной проблемы развития методологии управления информационными рисками.

В рамках поставленной цели выделено три основные подцели с соответствующими им задачами.

Подцель 1 – системное исследование основных свойств информационных рисков, определение их содержания и места среди экономических рисков.

Для достижения этой цели поставлены и решены следующие основные задачи:

- определение основного содержания информационных рисков, случайности и неопределенности;
- уточнение понятийного аппарата управления информационными рисками;
- определение взаимосвязи информационных и экономических рисков.

Подцель 2 – разработка концепции информационного риск-менеджмента.

Для достижения этой цели поставлены и решены следующие основные задачи:

- определение целей и задач информационного риск-менеджмента, обоснование структуры информационного риск-менеджмента;

- обобщение и адаптация методологии системного подхода к исследованию информационных рисков;
- определение целей, задач и стратегий управления информационными рисками, формирование методологических принципов анализа и создания систем управления информационными рисками;
- построение таксономии информационных рисков;
- классификация и характеристика механизмов управления информационными рисками предприятия.

Подцель 3 – разработка методологии управления информационными рисками.

Для достижения этой цели поставлены и решены следующие основные задачи:

- разработка методики системного анализа информационных рисков;
- разработка методов и моделей выбора механизмов управления информационными рисками и подсистем информационной системы с применением экономических методов управления;
- структуризация расходов и определение полных расходов предприятия на управление информационными рисками;
- определение эффективности затрат на управление информационными рисками.

Объект и предмет исследования. Объектом исследования является процесс управления предприятиями и организациями различных отраслей и организационно-правовых форм собственности.

Предметом исследования являются методы и модели управления информационными рисками хозяйствующих субъектов.

Теоретические и методологические основы работы. Проведенные исследования базируются на применении системного структурного анализа, теории множеств, теории нечетких множеств и нечеткой логики, теории графов, нечетких сетей Петри, генетических алгоритмов, марковских процессов, теории вероятностей, теории рисков.

В процессе исследования были проанализированы и использованы нормативные и методические документы, стандарты, специальная и периодическая литература, справочно-статистические материалы, результаты разработок отечественных и зарубежных ученых, материалы периодической печати, информация официальных веб-сайтов, материалы научных и научно-практических конференций, семинаров в области теории информации, информационных систем, информационной безопасности и риск-менеджмента.

Содержание работы соответствует основным положениям п. 1.4. Разработка и исследование моделей и математических методов анализа микроэкономических процессов и систем: отраслей народного хозяйства, фирм и предприятий, домашних хозяйств, рынков, механизмов формирования спроса и потребления, способов количественной оценки предпринимательских рисков и обоснования инвестиционных решений и п. 2.6. Развитие теоретических основ методологии и инструментария проектирования, разработки и сопровождения ин-

формационных систем субъектов экономической деятельности: методы формализованного представления предметной области, программные средства, базы данных, корпоративные хранилища данных, базы знаний, коммуникационные технологии Паспорта специальности ВАК 08.00.13 – «Математические и инструментальные методы экономики».

Научная новизна исследования заключается в разработке теоретико-методологического базиса управления информационными рисками в рамках нового научного направления – информационного риск-менеджмента.

Научную новизну содержат следующие положения работы, которые выносятся на защиту:

1) расширено представление о научной категории «информационный риск»:
   - под информационным риском понимается возможность наступления случайного события в информационной сфере предприятия, оказывающего негативное влияние не только на безопасность, но и на качество управляющей информации;
   - изменение представления об информационном риске позволяет рассматривать управление информационными рисками как системное управление всеми рисками, связанными с получением, обработкой, хранением, передачей и использованием информации в управлении бизнес-процессами;
2) анализ информационного риска как случайного события, позволил обосновать следующие положения:
   - наряду с объективной случайностью существует субъективная случайность риска, которая вносится при использовании недостоверной, неактуальной, неполной информации в процессе управления любыми социально-экономическими или человеко-машинными системами (процессами);
   - информационный риск рассматривается как мегариск в социально-экономических системах, присутствующий в виде информационной составляющей во всех рисках, в том числе и в экономических;
   - понятие «управление информационными рисками» распространяется на область управления информационными рисками в условиях статистической неопределенности;
3) развиты основные теоретико-методологические положения информационного риск-менеджмента, как нового направления в риск-менеджменте:
   - сформирована концепция информационного риск-менеджмента, включающая понятийный аппарат, цели, задачи, принципы управления информационными рисками и построения систем управления информационными рисками;
   - разработана методика системного анализа информационных рисков, в основу которой положено представление процесса функционирования предприятия с помощью моделей потоков данных и событий. Она

включает частные методики и направлена на определение общих расходов на управление информационными рисками, которые складываются из затрат на управление рисками и суммарного ущерба от них;

– особое внимание уделяется получению и обеспечению качества входной информации, взаимодействию с внешней средой, связи информационных рисков с бизнес-процессами, изменению роли менеджмента предприятий в управлении информационными рисками;

4) предложена двухкомпонентная классификация информационных рисков, которая отличается от существующих классификаций:

– наличием индексированной схемы классификации и таблицы, обеспечивающих полноту представления характеристик рисков и удобство использования;

– возможностью автоматизированной обработки характеристик и дополнения таблицы новыми данными о результатах анализа рисков;

5) обобщены принципы построения систем управления информационными рисками и предложены новые принципы, учитывающие особенности целей и задач использования таких систем:

– анализ и создание системы управления информационными рисками (СУИР) осуществляется на основе представления информационной сферы предприятия в виде мегасистемы;

– обеспечение возможности активного воздействия информационной системы предприятия на внешнюю среду;

– создание новых информационных технологий, позволяющих специалистам и менеджерам предприятия перейти на системный уровень управления качеством и безопасностью информации;

6) разработан методический инструментарий анализа информационных рисков:

– иерархическая нечеткая модель и инструментальные средства оценки качества информационных ресурсов, основанные на применении лингвистических переменных и отличающиеся повышенной точностью и информативностью;

– модель для исследования динамических процессов систем управления информационными рисками, особенность которой заключается в использовании нечетких временных сетей Петри с ингибиторными связями;

– модель, построенная на основе нечетких сетей Петри, для получения нечетких заключений об эффективности системы управления информационными рисками или ее подсистем;

7) создан методический аппарат выбора механизмов управления информационными рисками и подсистемы хранения данных:

– методы и инструментальные средства выбора механизмов управления информационными рисками, которые отличаются возможностью учета совместимости механизмов и включают два метода, построенные на

основе модифицированного жадного алгоритма и генетического алгоритма;

- методы выбора механизмов управления информационными рисками, допускающие совместное использование отдельных и агрегированных механизмов, а также наличие условия об обязательном включении в СУИР определенных механизмов;
- модель выбора подсистемы эффективного хранения данных, основанная на использовании аппарата цепей Маркова;

8) разработано методическое обеспечение определения и оптимизации расходов на управление информационными рисками:

- модель оптимизации затрат на управление значимыми информационными рисками с применением механизмов страхования информационных рисков, которую отличает возможность моделирования без ограничения средств на управление и в условиях лимита денежных средств;
- структурированы расходы и предложена модель определения полных расходов предприятия на управление информационными рисками, которую отличает от известных учет затрат на обеспечение качества информации и системных затрат.

Практическая значимость исследования состоит в возможности широкого использования полученных методических и инструментальных средств в процессе анализа и оценки информационных рисков, а также при построении и совершенствовании систем управления информационными рисками предприятий.

Материалы исследований могут применяться также при подготовке и переподготовке кадров на занятиях по экономическим дисциплинам, при подготовке специалистов по экономической и информационной безопасности в процессе изучения таких дисциплин, как «Информационная безопасность компьютерных систем», «Информационная безопасность», «Информационная безопасность бизнеса», «Управление информационными рисками».

Самостоятельное практическое значение имеют:

1) методика и инструментальные средства выбора механизмов управления информационными рисками;
2) методика и инструментальные средства оценки качества информационных ресурсов;
3) методика получения нечетких заключений об эффективности системы управления информационными рисками;
4) методика исследования динамических процессов системы управления информационными рисками;
5) методика выбора системы хранения данных;
6) предложения по совершенствованию организационной структуры системы управления информационными рисками;
7) практические рекомендации по созданию компьютера защищенной архитектуры.

Апробация и внедрение результатов исследования. Материалы диссертационной работы внедрены в деятельность ряда научно-исследовательских

институтов и предприятий: НИИ автоматической аппаратуры им. академика В.С. Семенихина, Московского научно-исследовательского телевизионного института, Военной страховой компании, Горьковского автомобильного завода, Расчетной палаты Московской межбанковской валютной биржи. Результаты внедрения результатов работы подтверждены соответствующими документами.

Материалы исследований используются в образовательном процессе по дисциплинам «Информационная безопасность компьютерных систем», «Информационная безопасность», «Информационная безопасность бизнеса» в Финакадемии.

Полученные теоретические и методологические результаты докладывались на 20-ти международных, всероссийских и региональных конференциях и семинарах в том числе на IV Всесоюзном совещании по распределенным вычислительным системам массового обслуживания (Душанбе, 1991), на II научно-технической конференции Московского военного университета радиоэлектроники (Кубинка, 1997), на Международной конференции «Развитие вычислительной техники в России и странах бывшего СССР: история и перспективы» (Петрозаводск, 2006), на II Международной научно-технической конференции «Информационные технологии в науке, образовании и производстве» (Орел, 2006), на Национальном форуме по информационной безопасности «Инфофорум 2007» (Москва, 2007), на Международной конференции «Бизнес информатика» (София, 2007), на XV Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы» (Москва, МИФИ 2008), на Международной научно-практической конференции «Информационные технологии в образовании, науке и производстве» (Серпухов, 2009).

Публикации. Основные результаты диссертации отражены в 45-ти научных публикациях, авторский объем в которых составляет 54,28 п.л. В число опубликованных работ входят три монографии и 10 статей в периодических изданиях из Перечня ВАК, а также две публикации в зарубежных издательствах.

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИССЕРТАЦИИ

В соответствии с целью и задачами исследования в работе рассматриваются шесть групп проблем.

Первая группа проблем связана с системным исследованием основных свойств информационных рисков и определением их места среди экономических рисков.

Важной проблемой исследования информационных рисков является анализ понятия «риск». По мнению большинства ученых, оно означает возможность наступления событий с отрицательными последствиями в результате определенных решений или действий. Такой взгляд на сущность риска закреплен в Федеральном законе «О техническом регулировании»: «риск – вероятность причинения вреда жизни или здоровью граждан, имуществу физических или

юридических лиц, государственному или муниципальному имуществу...»[1]. Существует и другая распространенная точка зрения на содержание риска. Ее сторонники под риском понимают случайное событие, вызывающее негативные последствия.

При этом всеми признается, что рисковое событие – событие случайное. В соответствии с сущностью процессов, явлений и объектов, порождающих случайности, различают объективную и субъективную случайности. Объективная случайность связана с природой материи, ее сущностью. В наиболее явной форме объективная случайность проявляется в микромире на уровне молекул, атомов, элементарных частиц. Субъективная случайность определяется неполнотой информации о причинах и сущности случайных событий.

Таким образом, все рисковые события являются случайными событиями, и случайность определяется их случайной природой и недостатком качественной информации об этих событиях. Один из первых исследователей неопределенности Ф.Х. Найт разделял ее на измеряемую и не измеряемую. В современной интерпретации различают статистическую и нестатистическую неопределенность.

В условиях статистической неопределенности с необходимой точностью могут быть определены законы распределения случайных величин. Это позволяет успешно использовать методы теории вероятностей и математической статистики при управлении рисками. В отношении значительной части информационных рисков не удается получить статистическую информацию. В этом случае исследователи вынуждены прибегать к использованию «квазистатистики» или нестрогой статистики, которая основывается не только на частотном определении характеристик случайных величин, но и на широком применении экспертных оценок. Для работы с нестатистическими данными в последние годы успешно применяются методы мягких вычислений, такие, как интервальный метод, нейронные сети, нечеткие множества и нечеткая логика, генетические алгоритмы и др.

Некоторые ученые понятие «управление риском» относят только к управлению в условиях статистической информации, а если информация является нестатистической, употребляют термин «управление в условиях неопределенности». Автор считает, что понятие «управление рисками» должно применяться как при работе со статистической, так и нестатистической информацией. Различия заключаются лишь в методах управления. При наличии статистической информации следует использовать методы, основанные на теории вероятностей и математической статистике. В условиях вынужденного использования нестатистической информации необходимо снижать степень неопределенности данных и использовать методы мягких вычислений.

Информационная неопределенность является либо единственной основой случайности события для человека, либо сопровождающей и дополняющей объективную случайность. Следствие такого вывода – необходимость признания информационной составляющей рисков любой природы. В информацион-

[1] Федеральный закон «О техническом регулировании» от 27.12.2002 №184 – ФЗ.

ной составляющей могут быть выделены общие элементы, которые должны систематизироваться и учитываться в процессе управления рисками.

Центральной проблемой первой группы является исследование содержания информационных рисков. Системный подход к проблеме позволил предложить новую трактовку понятия «информационный риск». Основные отличия заключаются в учете не только свойств безопасности информации, но и ее качества, а также в расширении сферы реализации рисковых событий и более тесной связи информационных рисков с конечными результатами бизнес-процессов.

Понятие «качество информации» рассматривается применительно к использованию информации в бизнес-процессах. То есть исследуются потребительские свойства информации на выходе информационных процессов, которые оказывают непосредственное влияние на эффективность основных бизнес-процессов предприятия.

Для системного рассмотрения вопросов управления информационными рисками вводится понятие «информационная сфера предприятия». С позиций рассмотрения сущности информационных рисков предлагается выделить две системы: информационную систему предприятия (внутренняя среда) и внешнюю информационную среду. Объединение этих двух систем позволяет получить системный комплекс или мегасистему. Такую мегасистему и предлагается рассматривать как информационную сферу предприятия. Информационная сфера предприятия не может быть представлена в виде системы из-за наличия иррационального взаимодействия между информационной системой предприятия (ИСП) и внешней средой. Под иррациональным взаимодействием понимается наличие неупорядоченности, нецелесообразности, неопознаваемости, непредсказуемости и парадоксальности во взаимодействии систем.

Понятие «предприятие» рассматривается в широком смысле независимо от форм собственности, вида деятельности, организационно-экономической формы и т. д. При необходимости учета особенностей управления информационными рисками на определенных предприятиях это оговаривается особо.

С позиций системного анализа информационная система предприятия представляет собой открытую систему, образуемую множеством взаимосвязанных информационных элементов, которые обеспечивают получение, обработку, хранение и передачу необходимой информации в целях эффективного функционирования предприятия. В качестве информационных элементов рассматриваются сотрудники предприятия, информационные ресурсы, компьютерные системы различных классов, средства и системы сбора, обработки, хранения, передачи и представления информации, участвующие в информационном процессе или обеспечивающие информационный процесс.

Внешнюю информационную среду предприятия образуют объекты, субъекты, процессы и явления внешней среды, оказывающие влияние на элементы информационной системы предприятия и на информацию во внешней среде, имеющую отношение к предприятию, его бизнес-процессам.

На самом высоком уровне представления мегасистемы, с учетом целей исследования информационных рисков, понятие информационной сферы пред-

приятия может быть сформулировано следующим образом. *Под информационной сферой предприятия* следует понимать взаимосвязанные элементы информационной системы предприятия и внешней информационной среды предприятия, а также систему регулирования отношений субъектов информационных процессов во внутренней и внешней среде предприятия. Таким образом, к информационной сфере предприятия относятся все элементы внутренней и внешней среды в их взаимодействии, имеющие отношение к получаемой, используемой, обрабатываемой, хранящейся и распространяемой информации, влияющей на бизнес-процессы предприятия, независимо от форм представления информации, видов объектов и субъектов, а также временных и пространственных рамок информационных процессов.

Используя дефиницию информационной сферы предприятия понятие «информационный риск» может быть определено следующим образом: *информационный риск* – это возможность наступления случайного события в информационной сфере предприятия, в результате которого предприятию будет нанесен ущерб. Причем информационные риски рассматриваются как случайные события во внутренней или внешней среде предприятия, оказывающие негативное влияние не только на безопасность информации, но и на ее качество. При этом учитываются все события, которые могут произойти на всех этапах информационного процесса – от получения информации до ее использования в бизнес-процессах.

Информационные риски приводят к ущербам предприятия. Поэтому они с полным правом могут быть отнесены к экономическим рискам. При выделении информационных рисков в отдельный вид экономических рисков важно определить соотношение и взаимосвязи информационных и других экономических рисков.

Проведенный анализ содержания рисков любой природы позволил сделать вывод о наличии информационной составляющей в любом риске. Это утверждение полностью распространяется и на экономические риски. Отсюда следуют выводы:

1) при анализе любого экономического риска необходимо рассматривать информационные риски, которые являются возможными причинами и факторами экономических рисков;
2) управление экономическими рисками должно предполагать управление и информационными рисками.

Часть экономических рисков, по существу, является полностью информационными рисками. К ним относятся, например, управленческий и инвестиционный риски.

В значительной степени информационными являются такие риски, как банковский, валютный, процентный, производственный риск предприятий, оказывающих информационные услуги, и другие риски, в которых основное место занимает риск принятия управленческого решения или производственные процессы являются информационными процессами.

Вторая группа проблем связана с разработкой теоретико-методологического базиса информационного риск-менеджмента.

Управление информационными рисками осуществляется с учетом основных положений общего менеджмента, а также с использованием результатов, полученных в рамках риск-менеджмента. Вместе с тем управление информационными рисками имеет много особенностей и требует доработки методологии, принятой в риск-менеджменте. Учитывая особенности и значимость системного управления информационными рисками, предлагается выделить управление информационными рисками в отдельный раздел риск-менеджмента – информационный риск-менеджмент.

Кроме того, наличие информационной составляющей в любом экономическом риске позволяет сделать вывод о необходимости управления этой информационной составляющей. При всем многообразии и различии экономических рисков в информационной составляющей этих рисков могут быть выделены общие элементы, требующие применения единых методологических подходов к управлению рисками.

В качестве методологической основы информационного риск-менеджмента предлагается использовать системный подход. Системное управление информационными рисками в рамках информационного риск-менеджмента позволяет выйти на качественно новый уровень управления:

1) учитываются все негативные события, влияющие на безопасность и качество информации, которые могут произойти на всех этапах информационного процесса – от получения информации до ее использования в бизнес-процессах, независимо от форм представления информации, видов объектов и субъектов информационных процессов, а также временных и пространственных рамок использования информации;
2) появляется возможность согласованного применения всего комплекса механизмов управления, направленного на достижение конечных целей бизнес-процессов;
3) для исследования информационных рисков могут согласованно применяться научные методы из различных областей науки, которые не используются вне рамок системного подхода;
4) в полной мере становятся доступными экономические механизмы управления, повышается значение правовых и организационных методов управления;
5) рассматриваемый подход к пониманию информационных рисков позволяет сделать вывод о коренном изменении роли и значения менеджмента предприятия: менеджеры всех уровней принимают активное участие в управлении информационными рисками;
6) архитектура информационной системы предприятия и, прежде всего, архитектура системы управления информационными рисками должна быть адаптирована к управлению рисками на более высоком системном уровне.

Предлагается в информационном риск-менеджменте выделить три подраздела: управление информационной безопасностью; управление качеством информации; информационное взаимодействие с внешней средой предприятия.

Первые два подраздела информационного риск-менеджмента объединяют направления управления внутренней информационной сферой. В рамках этих направлений рассматриваются также вопросы взаимодействия с внешней средой, но они касаются, в основном, технологии информационных процессов. Это взаимодействие носит, как правило, пассивный характер по отношению к внешней среде.

Выделение проблем информационного взаимодействия с внешней средой предприятия в отдельное направление объясняется необходимостью активного информационного воздействия на внешнюю среду, которое осуществляется, в основном, с помощью правовых и организационных методов. Главными задачами такого воздействия являются информационное обеспечение бизнес-процессов во внешней среде, защита интеллектуальной собственности предприятия и других законных прав предприятия в информационной сфере, взаимодействие с государственными структурами, средствами массовой информации, потребителями продукции предприятия и партнерами по бизнесу.

В условиях становления информационного риск-менеджмента важное значение имеет решение концептуальных вопросов управления информационными рисками. Прежде всего, необходимо определить понятие «управление информационными рисками». Под управлением информационными рисками понимается система согласованных действий, операций и процедур, осуществляемых персоналом предприятия в целях минимизации расходов на противодействие информационным рискам и устранение их последствий.

Целью управления информационными рисками является минимизация суммы расходов предприятия на противодействие информационным рискам и суммарного ущерба от этих рисков.

Управление информационными рисками предполагает решение следующих *задач*: анализ рисков; выработка политики управления информационными рисками; создание системы управления информационными рисками; устранение причин и факторов значимых рисков; создание механизмов снижения ущерба от возможных рисков; оценка ущерба; ликвидация последствий рисковых событий; постоянный мониторинг и периодический аудит системы управления рисками; анализ эффективности системы управления информационными рисками; совершенствование системы управления информационными рисками.

На основании всестороннего анализа возможных стратегий управления информационными рисками предлагаются следующие *стратегии управления*: принятие риска; предотвращение риска; снижение возможного ущерба от риска; предотвращение риска и снижение возможного ущерба от него.

Применительно к задаче построения систем управления информационными рисками предлагается использовать следующие *методологические принципы*, основанные на принципах системного анализа и синтеза систем, а также на принципах разработки информационных систем. К ним могут быть отнесены: принцип соответствия целей создания каждой подсистемы общей цели создания СУИР; принцип создания СУИР как подсистемы информационной системы предприятия; принцип построения адаптивной СУИР, обеспечивающей ее эффективность и устойчивость; принцип синтеза многоуровневой, многозвенной,

комплексной системы защиты от информационных рисков; принцип централизованного иерархического управления; принцип открытости системы; итеративный процесс построения СУИР, основу которого составляют этапы анализа и синтеза.

Перечень приведенных общепринятых принципов построения информационных систем предлагается дополнить следующими принципами: анализ и создание системы управления информационными рисками осуществляется на основе представления информационной сферы предприятия в виде мегасистемы; обеспечение возможности активного воздействия информационной системы предприятия на внешнюю среду; создание новых информационных технологий, позволяющих специалистам и менеджерам предприятия перейти на системный уровень управления качеством и безопасностью информации.

Общий алгоритм системного анализа применительно к исследованию информационных рисков может быть представлен в виде следующей последовательности этапов: определение целей анализа информационных рисков; общая постановка задачи исследования; построение информационной модели; идентификация информационных рисков; определение механизма воздействия информационных рисков на ИСП; выявление источников, факторов рисков и причин их порождающих; определение взаимосвязи информационных рисков; классификация рисков; выбор показателей оценки рисков; выбор методов и средств оценки рисков; построение моделей; оценка рисков; определение тенденций развития информационных рисков.

Одной из наиболее важных проблем анализа информационных рисков является *проблема создания классификации информационных рисков*.

Информационные риски предлагается группировать в соответствии с их природой и механизмом действия. Это позволяет оптимально использовать средства и методы защиты информации для блокирования целой группы рисков, сходных по механизму действия.

Для классификации информационных рисков предлагается использовать индексированную схему классификации (рис.1) и таблицу 1. Схема показывает разделение информационных рисков на группы по одному из пяти классификационных признаков.

Каждой группе присваивается свой индекс. В таблицу сведены все основные риски. С помощью индексов для каждого информационного риска возможно определение его места в классификации по всем классификационным признакам.

При необходимости такая таблица может быть дополнена еще одним столбцом. В нем могут быть размещены индексы тех информационных рисков, наступлению которых способствует соответствующий риск из первого столбца.

Данная классификация обладает еще одним достоинством. Таблицу легко дополнить вычисленными значениями вероятности информационного риска, величинами ущерба и другими показателями риска, которые получаются в результате анализа информационных рисков. То есть таблица классификации, дополненная столбцами с вычисленными показателями отобранных значимых рисков, является таблицей результатов анализа информационных рисков.

Рис. 1. Индексированная схема классификации информационных рисков

Важной проблемой является *классификация и характеристика механизмов управления* информационными рисками предприятия. Управление информационными рисками предполагает согласованное комплексное применение методов и средств различной физической природы в рамках единой технологической цепи для достижения целей управления. В отношении средств и методов принято использовать общий термин – механизм управления информационными рисками. Многообразие методов и средств, сложные отношения взаимодействия, необходимость согласования по месту и времени их применения вызывают необходимость использования возможностей таксономии на концептуальном уровне исследования проблем управления информационными рисками.

Исходя из целей таксономии механизмов управления информационными рисками, предлагается классификация, в которой все множество механизмов разделено на два подмножества: средства и методы управления информационными рисками.

Методы, в свою очередь, могут быть разделены на нормативные правовые, организационные и экономические. К экономическим методам управления от-

носятся следующие методы: определения затрат на систему управления информационными рисками; оценки ущербов от информационных рисков; оптимизации общих расходов на управление информационными рисками; страхования информационных рисков; создания резервов для минимизации ущербов.

Таблица 1

Фрагмент классификационной таблицы информационных рисков

Информационный риск	Индекс				
	Механизм воздействия	Источник риска	Характер риска	Вид ущерба	Результат воздействия
Пожары	1	А В	σ	П К	$\alpha_3\ \alpha_4\ \alpha_5\ \alpha_2$
Наводнения	1	В	σ	П К	$\alpha_3\ \alpha_4\ \alpha_5\ \alpha_2$
Землетрясения	1	В	σ	П К	$\alpha_3\ \alpha_4\ \alpha_5\ \alpha_2$
Ураганы	1	В	σ	П К	$\alpha_3\ \alpha_4\ \alpha_5\ \alpha_2$
Взрывы	2	А В	σ	П К	$\alpha_3\ \alpha_4\ \alpha_5\ \alpha_2$
Аварии в системе электропитания, водоснабжения, отопления	2	А В	σ	П К	$\alpha_3\ \alpha_4\ \alpha_5\ \alpha_2$
…	…	…	…	…	…

Средства управления информационными рисками в соответствии с особенностями решаемых задач могут быть разделены на три группы средств: средства сбора и первичной обработки информации; средства обеспечения качества информации в информационной системе; средства обеспечения безопасности информации в информационной системе.

К третьей группе относятся проблемы создания методического аппарата анализа информационных рисков. Центральной проблемой этой группы является разработка методики системного анализа информационных рисков. Методика базируется на использовании системного структурного анализа и предполагает выполнение следующих шагов.

Шаг 1. Уточняются цели и задачи исследования, определяются исполнители и выполняется планирование работ.

Шаг 2. Проводится обследование предприятия.

2.1. Выделяются во внешней среде элементы (объекты, субъекты, процессы и явления), с которыми предприятие взаимодействует в процессе производственной деятельности. Все внешние элементы могут быть распределены по двум группам: элементы взаимодействия и элементы воздействия. К элементам воздействия следует относить те из них, которые оказывают одностороннее влияние на работу информационной системы предприятия.

2.2. Определяются все существенные информационные потоки и их характеристики как между предприятием и внешней средой, так и внутри предприятия.

2.3. Изучаются процессы преобразования, хранения и передачи информации.

2.4. Определяется перечень событий, оказывающих влияние на работу информационной системы предприятия.

Шаг 3. Создается модель потоков данных DFD. Могут использоваться как классические нотации Йордана, Гейна-Сарсона, так и нотации SSADM, ARIS и др. В результате получается иерархическая модель потоков данных, в которую входят диаграммы, словари данных и спецификации процессов.

Шаг 4. На основе построенной модели потоков данных создается модель состояний (рис.2). Состояния процессов на каждом уровне иерархии рассматриваются в соответствии с принятой нумерацией процессов в модели DFD. В дополнение к нотации ARIS предлагается при отображении события показывать показатели риска.

Шаг 5. Осуществляется определение показателей рисков на каждом уровне модели. Показатели рисков определяются с помощью частных методик, основу которых составляют модели различных видов.

Шаг 6. Анализ результатов моделирования.

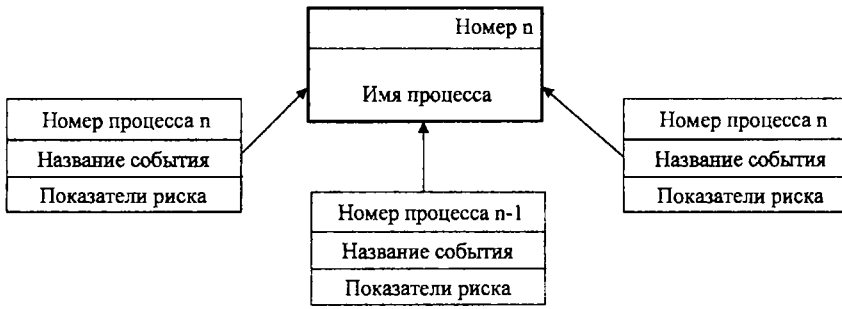

Рис. 2. Модель состояний

На шаге 5 продвижение по модели осуществляется с нижних уровней к верхним. Для каждого вида рисков выбираются модели, обеспечивающие необходимую точность и возможность получения характеристик, позволяющих вычислять прямые и косвенные ущербы. Данные о событиях, оказывающих воздействие на соответствующий процесс, обобщаются на уровне этого процесса и передаются для учета на верхних уровнях. Например, три события оказывают влияние на непрерывность процесса. Эти события обрабатываются, и на процесс следующего уровня иерархии передается сообщение с обобщенными характеристиками простоя процесса от воздействия всех рассматриваемых событий. Обрабатываются только данные о косвенных рисках. Значения величин прямых ущербов передаются на верхние уровни без изменения для их суммирования. Для этого в прямоугольниках-событиях отображаются величины ущербов от прямых рисков.

Методологии структурного анализа для исследования информационных рисков реализованы в целом ряде инструментальных CASE-систем (ARIS,

UML, CASE.Аналитик, BPwin и др.). Динамические процессы в системах моделируются в некоторых CASE-технологиях с помощью аппарата сетей Петри (Design/CPN, CPN-AMI, INCOME Mobile).

В диссертации порядок применения предложенного метода анализа информационных рисков показан на примере создания модели коммерческого банка. На основе типовой структуры бизнес-процессов банка создана модель потоков данных и для выбранной ветви модели выполнена детализация с построением модели событий на уровне банкомата.

Для анализа информационных рисков в условиях нестатистических данных с учетом динамики процессов предложено использовать модифицированные *нечеткие временные сети Петри с ингибиторными связями*. Формально нечеткая временная сеть Петри с ингибиторными связями может быть представлена следующим образом:

$NP_\tau = (P, T, I, I_d, O, m_0, Z, S)$,

где $P=\{p_1, p_2, ..., p_N\}$ – конечное множество позиций; $T=\{t_1, t_2, ..., t_K\}$ – конечное множество переходов; I– входная функция переходов, определяемая как отображение I: $P\times T\to R^0$; I_d – бинарная функция ингибиторных связей, которая определяется как отображение I_d: $P\times T\to\{0,1\}$; O – выходная функция переходов, определяемая как отображение O: $T\times P\to R^0$; $m^0=(m_1^0, m_2^0, ..., m_N^0)$ ($m_n^0\in R^0$, $n=\overline{1,N}$) – вектор начальной маркировки сети, компонент которого m_n^0 представляет собой некоторую неотрицательную нечеткую величину; $Z=(z_1, z_2, ..., z_N)$ – вектор параметров временных задержек маркеров в позициях, компонент которого z_n представляет собой некоторую неотрицательную нечеткую величину; $S=(s_1, s_2, ..., s_K)$ – вектор параметров времен срабатывания разрешенных переходов, компонент которого s_k представляет собой некоторую неотрицательную нечеткую величину; R^0 – множество натуральных чисел и ноль.

Динамика перемещения маркеров по сети определяется следующими правилами Π_i, $i=\overline{1,4}$.

Π_1 – правило определения текущей маркировки. Любое состояние сети определяется вектором $m=(m_1, m_2, ..., m_N)$, $n=\overline{1,N}$, компоненты которого задаются с помощью трапецеидальных нечетких интервалов $m_i=\langle a_1^i, a_2^i, a_3^i, a_4^i\rangle$ и означают функции принадлежности нечеткого наличия маркера в соответствующей позиции $p_i\in P$ относительно времени с момента запуска данной сети. Начальное состояние сети определяется вектором начальной разметки (маркировки) m^0.

Π_2 – правило активности перехода. Переход $t_k\in T$ является активным (разрешенным) при некоторой доступной маркировке m, если выполняются следующие условия:

$$m_i>0 \quad ((\forall p_i\in P)\wedge(I(p_i,t_k)>0))\wedge((\forall p_d\in P)\wedge(I_d(p_d,t_k)=1)).$$

Причем, $I_d(p_d,t_k)=1$, *если* $m_d=<0,0,0,0>$.

То есть, во всех входных позициях рассматриваемого перехода $t_k \in T$ в определенный момент времени должны быть маркеры с соответствующей функцией принадлежности, отличной от нуля, и на всех входящих ингибиторных дугах поддерживается режим разрешения срабатывания перехода.

$П_3$ – правило нечеткого срабатывания перехода. Если переход $t_k \in T$ является активным (выполняется условие $П_2$) по условиям маркировки, то переход срабатывает за время s_k и маркировка m изменяется на маркировку m^{ϕ} по следующему правилу:

1) для каждой входной позиции $p_i \in P$ при условии

$I(p_i, t_k) > 0$

маркировка позиции p_i изменяется на $m_i^{\phi} = <0, 0, 0, 0>$;

2) все выходные позиции $p_j \in P$ при условии $O(t_k, p_j) > 0$ изменяют состояние по формуле:

$$m_j^{\phi} = \min\Big\{ \max_{(i=\overline{1,N}) \wedge (I(p_i,t_k)>0)} \{m_i\} + s_k, m_j \Big\}$$

$$(\forall p_i \in P) \wedge (O(t_k, p_j) > 0) \wedge (m_j \neq <0, 0, 0, 0>)$$

(примечание: первая строка условий относится к max, а вторая – к min, то есть операция минимум применяется только если $m_j \neq <0, 0, 0, 0>$);

3) для позиций $p_i \in P$, не являющихся ни входными, ни выходными по отношению к переходу t_k, маркировка не изменяется:

$$m_i^{\phi} = m_i \quad \forall p_i \in P \mid I(p_i, t_k) = 0 \wedge O(t_k, p_i) = 0.$$

Если позиция является одновременно входной и выходной, то сначала производится расчет для входной позиции, а затем – для выходной.

$П_4$ – правило нечеткой задержки в позициях. После нечеткого срабатывания активных переходов по правилу $П_3$ новая разметка m^{ϕ} устанавливается с задержкой, которая определяется нечетким интервалом z_j для каждой позиции. Доступная маркировка определяется по формуле:

$$m_j^{\phi'} = m_j^{\phi} + z_j \quad \forall p_j \in P \mid O(t_k, p_j) > 0 \wedge m_j^{\phi} \neq <0,0,0,0>.$$

Исходные данные для моделирования процесса включают данные о начальной маркировке (разметке), о задержке маркеров в позициях и времени срабатывания переходов, которые представляются множествами трапецеидальных нечетких интервалов. Применение правил срабатывания переходов с учетом исходных данных позволяет получить информацию о времени начала и завершения событий в моделируемом процессе. Вычисленное значение времени в виде трапецеидального интервала при необходимости может быть приведено к обычному четкому значению с помощью одного из правил дефаззификации.

Методика определения нечетких временных характеристик динамических процессов может быть представлена следующей последовательностью шагов:

Шаг 1. Получение исходных данных для моделирования.

Шаг 2. Последовательное применение правил активных переходов, срабатывания переходов и изменений маркировки до достижения финальных состояний.

Шаг 3. Анализ результатов и их преобразование, при необходимости, к четкому виду.

Методика апробирована на примере моделирования динамических процессов работы банкомата.

Для *представления правил нечетких продукций может быть использована нечеткая сеть Петри* вида:

$NP_f=(N, f, \lambda, m^0)$,

где $N=(P, T, I, O)$ – структура нечеткой ординарной сети Петри с входной функцией $I: P\times T \to \{0,1\}$ и выходной функцией $O: T\times P \to \{0,1\}$; $f=(f_1, f_2, ...f_K)$ – вектор значений функции принадлежности нечеткого срабатывания переходов, при $f_k \in [0,1]$; $\lambda=(\lambda_1,\lambda_2,...\lambda_K)$ – вектор значений порога срабатывания переходов, при $\lambda_k \in [0,1]$; $m^0 = (m_1^0, m_2^0, ..., m_N^0)$ – вектор начальной маркировки сети, компонент которого m_n^0 представляет собой значение функции принадлежности нечеткого наличия одного маркера в n – й позиции сети, при $m_n^0 \in [0,1]$.

Маркировка сети меняется в соответствии с правилами.

$П_1$ – правило определения текущей маркировки. Текущее состояние сети определяется вектором $m = (m_1, m_2, ..., m_N)$, компонент которого $m_n \in [0,1]$ интерпретируется как функция принадлежности нечеткого нахождения одного маркера в позиции p_n. Начальное состояние сети определяется вектором начальной маркировки m^0.

$П_2$ – правило, определяющее условие активности перехода. Переход $t_k \in T$ считается активным (разрешенным), если при текущей маркировке m_n выполнено условие:

$$\min\{m_n\} \geq \lambda_k,$$
$$(n=\overline{1,N}) \wedge (I(p_n,t_k)>0)$$

где λ_k – значение порога срабатывания перехода $t_k \in T$.

$П_3$ – правило нечеткого срабатывания активного перехода. Если переход $t_k \in T$ является активным при текущей маркировке m_n, то осуществляется мгновенный переход к новому вектору маркировки $m_\eta^\gamma = (m_1^\gamma, m_2^\gamma, ..., m_N^\gamma)$, каждый компонент которого определяется в соответствии со следующим выражением:

$$m_j^\gamma = \max\{m_j, \quad \min\{m_n, f_k\} \quad\} \quad (\forall\ p_j \in P) \wedge (O(t_k, p_j)>0),$$
$$(n=\overline{1,N}) \wedge (I(p_n,t_k)>0)$$

где f_k – значение функции принадлежности или мера возможности срабатывания перехода $t_k \in T$. Значения функции f_k для всех переходов задаются

при определении параметров сети. Эта формула используется для определения маркировки как входных, так и выходных позиций.

Правила нечеткой продукции применительно к сетям Петри реализуются следующим образом. Правило нечеткой продукции «Правило i : Если A, то B» представляется как переход $t_k \in T$ сети NP_f. Входной позиции p_n этого перехода соответствует условие A, а выходной позиции p_j – заключение B.

Если условием правила нечеткой продукции определяется использование нескольких логически связанных подусловий или подзаключений, то это учитывается соответствующим образом в сети.

Методика получения нечетких продукций (нечетких заключений) предполагает выполнение следующих шагов.

Шаг 1. Устанавливаются правила нечетких продукций.

Шаг 2. Для каждого правила задаются веса или коэффициенты определенности F_i правил нечетких продукций, которые рассматриваются в нечетких сетях Петри как значения функций принадлежности нечеткого срабатывания переходов – f_i.

Шаг 3. Нечетким высказываниям ставятся в соответствие позиции сети NP_f.

Шаг 4. Для части позиций задаются исходные степени истинности высказываний, которые определяют начальную маркировку сети m^0.

Шаг 5. Используются правила срабатывания переходов для изменения маркировки сети до достижения финальных состояний.

Шаг 6. Анализируются результаты, в качестве которых рассматриваются степени истинности финальных высказываний.

Возможность использования моделей на основе нечетких сетей NP_f показана в диссертационной работе на примере анализа возможностей антивирусной подсистемы противостоять заражению информационной системы новым вирусом.

Экспертам и лицу, принимающему решение в условиях высокой степени неопределенности, удобно использовать лингвистические переменные. Использование *лингвистических переменных в моделях анализа* эффективности и качества механизмов управления информационными рисками позволяет получать интегрированный (агрегированный) показатель, опираясь на систему взаимосвязанных иерархических показателей.

Поэтому для оценки качества ресурсов, механизмов, подсистем системы управления информационными рисками предлагается использовать иерархическую нечеткую модель, основанную на применении лингвистических переменных.

Качество информационного ресурса описывается следующей нечеткой моделью:

$Q = <G, L, P, A>$, где G – граф дерева с вершинами g_i $(i = \overline{0, N})$, каждой из которых поставлено в соответствие одно из возможных лингвистических значений переменной $x_i \in L$, характеризующих показатель качества i-го меха-

низма; $L = \{L_i\ ,\ (i = \overline{0, N})\}$ – набор лингвистических значений (качественных оценок) каждого показателя; P – система отношений предпочтения одних показателей другим для одного уровня иерархии показателей; A – алгоритм агрегирования информации, позволяющий получать обобщенный показатель качества на текущем уровне иерархии путем обработки значений оценок качества подчиненных вершин.

Если в отношении всех лингвистических переменных принять пятиуровневый классификатор с L_i ={«Очень низкий» (ОН), «Низкий» (Н), «Средний» (С), «Высокий» (В), «Очень высокий» (ОВ)}, то каждому i-му значению лингвистической переменной можно поставить в соответствие трапецеидальную функцию принадлежности $\mu_i(x)$, определенную на 01 носителе с набором нейтральных точек с координатами (0,2; 0,4; 0,6; 0,8).

Агрегирование осуществляется по уровням, продвигаясь от нижних уровней графа G к верхним. Предварительно определяются значения лингвистических переменных x_i для конечных вершин графа G. Эта задача может быть решена с помощью экспертных методов оценивания.

По графу определяется подмножество вершин (показателей) $g_k \in G_k^u$ при $k = \overline{1, N_k}$ уровня u, которые связаны с k-той вершиной старшего уровня u-1. Для каждого подмножества вершин определяется взвешенная сумма соответствующих функций принадлежности. Для этого может быть использован OWA-оператор Ягера: $\mu_k(x) = \sum_{i=1}^{N_k} \mu_H(x)\rho_i$, где ρ_i – вес i- го показателя, N_k – количество показателей нижнего уровня, связанных с показателем k следующего по иерархии уровня. В качестве весов показателей качества использованы коэффициенты Фишберна.

Коэффициент Фишберна зависит от взаимного соотношения показателей качества, входящих в подмножество связанных показателей одного уровня. Показатели $П_{ui}^k$ и $П_{ui+1}^k$ u- го уровня, определяющие значение k-го показателя старшего уровня u-1, могут находиться друг к другу в отношении нестрогого предпочтения ($\succ$) или безразличия ($\approx$). Формально система предпочтений может быть представлена следующим образом:

$P = \{\ П_{ui}^k\ (\varphi)\, П_{ui+1}^k \mid \varphi \in (\succ, \approx)\}$.

Если $П_{u1}^k \succ П_{u2}^k \succ ... \succ П_{uN_k}^k$ для всех $П_{ui}^k$, то коэффициенты Фишберна определяются по формуле:

$$\rho_i = \frac{2(N_k - i + 1)}{(N_k + 1)N_k}, \quad i = \overline{1, N_k}.$$

Если $П_{u1}^k \approx П_{u2}^k \approx ... \approx П_{uN_k}^k$ для всех $П_{ui}^k$, то коэффициенты Фишберна равны и вычисляются следующим образом:

$$\rho_i = \frac{1}{N_k}, \quad i = \overline{1, N_k}.$$

При смешанном характере предпочтений показателей одного подмножества следует использовать выражения:

$$r_{i-1} = \begin{cases} r_i, \text{ если } \Pi^k_{ui-1} \approx \Pi^k_{ui}; \\ r_i + 1, \text{ если } \Pi^k_{ui-1} \succ \Pi^k_{ui}. \end{cases}, r_{N_k} = 1,\ i = \overline{N_k, 2};$$

$$\rho_i = r_i / \sum_{i=1}^{N_k} r_i .$$

При вычислении функции $\mu_k(x)$ используется возможность перехода от действий с трапецеидальными функциями принадлежности к операциям над абсциссами вершин трапеций (a_1, a_2, a_3, a_4):

$$\sum_{i=1}^{N_k} \rho_i \times (a_{i1}, a_{i2}, a_{i3}, a_{i4}) = (\sum_{i=1}^{N_k} p_i \times a_{i1}, \sum_{i=1}^{N_k} p_i \times a_{i2}, \sum_{i=1}^{N_k} p_i \times a_{i3}, \sum_{i=1}^{N_k} p_i \times a_{i4}).$$

Вычисленное значение функции принадлежности $\mu_k(x)$ необходимо сравнить с функциями принадлежности $\mu_i(x)$, $i = \overline{1,5}$ для получения оценки о лингвистическом уровне показателя g_k. Для показателя g_k выбирается лингвистическое значение $x_i \in L$, если $\mu_i(x)$ наиболее близка к $\mu_k(x)$. Близость функций принадлежности может определяться с помощью квадратичного расстояния Евклида или абсолютного (относительного) расстояния Хемминга.

Если использовать абсолютное расстояние Хемминга и учесть трапецеидальную форму функций $\mu_i(x)$ и $\mu_k(x)$, то близость функций δ_{ik} определяется следующим образом:

$$\delta_{ik} = \max \left\{ \left| a_1^k - b_1^i \right|, \left| a_2^k - b_2^i \right|, \left| a_3^k - b_3^i \right|, \left| a_4^k - b_4^i \right| \right\}, \quad i = \overline{1,5},$$

где δ_{ik} – абсолютное расстояние Хемминга; b_u^i, a_u^k – абсциссы соответственно функций $\mu_i(x)$, $i = \overline{1,5}$ и вычисленной функции $\mu_k(x)$. В качестве лингвистической переменной выбирается та из x_i, которой соответствует функция $\mu_i(x)$ с координатами, обеспечивающими $\min \delta_{ik}$.

Алгоритм вычисления обобщенного показателя сопровождается проверкой условия на допустимость частных показателей качества информационного ресурса. Если значение $x_i \notin L_i^*$, где L_i^* – множество разрешенных для i– го показателя значений лингвистической переменной, то качество информационного ресурса считается неудовлетворительным.

По сравнению с существующими методами нечеткого моделирования процесса определения агрегированных показателей качества предлагаются следующие изменения: решение о качестве информационного ресурса принимается не только на основании обобщенного показателя, но и с учетом ограничений на значения отдельных показателей, в том числе и показателей, вычисляемых в ходе моделирования; для повышения точности алгоритма координаты трапецеидальных функций принадлежности, вычисляемые на каждом шаге, проверяются на близость к одной из пяти «эталонных» функций с идентификацией значения лингвистической переменной, но в дальнейших расчетах используются полученные значения координат, а не координаты соответствующей «эталонной» функции; степень совпадения полученных функций характеризуется

не только близостью четырех координат с координатами «эталонных» функций, выраженной в процентах, но и направлением смещения этих функций относительно «эталонных» по 01 оси определения функций; применяется характеристика, показывающая степень совпадения (перекрытия) верхних оснований трапеций, соответствующих проверяемой и «эталонной» функциям. Предлагаемый подход к моделированию позволяет повысить информативность полученных данных, а также точность вычислений до 20%.

Разработанная программа «Агрегирование показателей» позволяет автоматизировать все процессы вычисления лингвистических переменных и приведенных выше характеристик точности.

Методика получения агрегированного показателя состоит из последовательности следующих шагов.

Шаг 1. Определяются показатели качества, для которых не требуется выполнение операции агрегирования.

Шаг 2. Строится граф иерархической зависимости показателей с указанием признаков предпочтения показателей.

Шаг 3. Вычисляются функции принадлежности на каждом уровне, и определяется значение агрегированного показателя на текущем уровне. Осуществляется продвижение к следующему по иерархии уровню вверх.

Шаг 4. Вычисляется агрегированный показатель первого уровня.

К четвертой группе относятся проблемы определения множества механизмов системы управления информационными рисками и построения подсистем информационной системы.

При создании системы управления информационными рисками и ее совершенствовании решается задача выбора рационального множества механизмов управления информационными рисками, обеспечивающего минимум суммы затрат на эти механизмы и общего ущерба от информационных рисков. Задача относится к нелинейным дискретным бинарным задачам переборного типа. Точное решение задач такого класса возможно методами полного перебора, ветвей и границ, динамического программирования. Результаты, приемлемые для практических целей, могут быть получены при использовании методов, позволяющих получать субоптимальные значения. К таким методам относятся методы, основанные на использовании жадных и генетических алгоритмов.

Формальная постановка задачи может быть представлена в следующем виде. Известно множество значимых рисков $R = \{ r_1, r,..., r_N \}$. Для каждого риска r_n определен ущерб в денежной форме u_{r_n}. Тогда множество ущербов может быть представлено в порядке убывания значения ущерба следующим образом: $U = (u_{r_1}, u_{r_2},..., u_{r_N})$. Каждый ущерб u_{r_n} определен при условии, что в отношении n- го риска не применяются никакие механизмы управления информационными рисками.

Определено множество механизмов управления информационными рисками $M = (m_1, m_2,..., m_K)$, элементы которого могут использоваться в системе управления информационными рисками. Каждый k- й механизм управления

информационными рисками характеризуется множествами параметров R_k и E_k, а также параметром c_k.

Множество $R_k = (r_1, r_2, ..., r_J)$ составляют информационные риски, которым противодействует k- й механизм управления информационными рисками.

С помощью множества показателей $E_k = (e_{k1}, e_{k2}, ..., e_{KN})$ оценивается эффективность k- го механизма. Элемент множества e_{kn} показывает какая часть ущерба от n- го информационного риска будет предотвращена при использовании k- го механизма. Величина e_{kn} изменяется в пределах $0 \le e_{kn} < 1$. Эффективность всех механизмов может характеризоваться с помощью матрицы E размерности $K \times N$.

При подсчете общей эффективности снижения ущерба от риска n, при условии включения в СУИР всех K рассматриваемых механизмов, может использоваться мультипликативный показатель:

$$\prod_{k=1}^{K}(1 - e_{kn}) = (1 - e_{1n})(1 - e_{2n})...(1 - e_{Kn}).$$

Этот показатель характеризует общую часть ущерба от риска n, которая сохранится при применении всех K механизмов управления информационными рисками.

Параметр c_k представляет собой затраты предприятия на приобретение или на изменение, разработку, создание, а также на внедрение и эксплуатацию k- го механизма. Часто руководство предприятия не может направить на совершенствование СУИР денежные средства, которые превышают определенную сумму C_{max}.

Известны также элементы матрицы совместимости механизмов управления информационными рисками D. Значение элемента матрицы d_{ij} определяется следующим условием:

$$d_{ij} = \begin{cases} 1, \textit{ если } i-\textit{й и } j-\textit{й механизмы совместимы}; \\ 0 - \textit{в противном случае.} \end{cases}$$

Несовместимыми считаются механизмы, которые не допускают совместного использования в одной системе управления информационными рисками механизмов без существенного изменения их структур.

Множество механизмов, входящих в систему управления информационными рисками, задается с помощью бинарного вектора конфигурации:

$$X = (x_1, x_2, \ldots, x_K).$$

Компоненты вектора принимают следующие значения:

$$x_k = \begin{cases} 1, \textit{ если } k-\textit{й механизм включен в СУИР}; \\ 0 - \textit{в противном случае.} \end{cases}$$

Механизмы управления информационными рисками $x_i, x_j \in X$ совместимы, если выполняется условие: $x_i x_j \le d_{ij}$, $i = \overline{1,K}$, $j = \overline{1,K}$.

Общий ущерб U^o, который ожидается после введения в СУИР механизмов управления информационными рисками, назовем остаточным. Остаточный ущерб определяется бинарным вектором конфигурации. С учетом введенных

обозначений выражение для вычисления остаточного ущерба может быть представлено в следующем виде:

$$U^o(x_1, x_2, ..., x_K) = \sum_{n=1}^{N} u_{r_n} \prod_{k=1}^{K} (1 - e_{kn} x_k).$$

С учетом выбранных обозначений и введенных зависимостей постановка задачи оптимального выбора механизмов управления информационными рисками может быть представлена следующим образом.

Определить бинарный вектор $X^* = (x_1^*, x_2^*, ..., x_K^*)$, обеспечивающий минимум суммы расходов на применение механизмов управления информационными рисками и остаточного ущерба от всех значимых рисков:

$$\sum_{k=1}^{K} (c_k x_k) + \sum_{n=1}^{N} u_{r_n} \prod_{k=1}^{K} (1 - e_{kn} x_k) \quad (1)$$

при выполнении условий:

$$x_i x_j \le d_{ij}, \; i = \overline{1, K}, \; j = \overline{1, K};$$

$$\sum_{k=1}^{K} (c_k x_k) \le C_{\max}.$$

Для решения поставленной задачи может быть использован *следующий модифицированный метод*, который относится к классу *жадных алгоритмов*. Сущность метода заключается в выборе на каждом шаге одного из возможных механизмов, обеспечивающего получение максимального эффекта. Эффект определяется величиной снижения затрат на управление рисками в результате применения очередного механизма и упущенной выгодой от невозможности использования на последующих шагах механизмов, несовместимых с включаемым в систему очередным механизмом. Таким образом, на каждом шаге анализируются не только локальный эффект от включения в систему механизма, но и рассматриваются последствия этого шага в дальнейшей работе алгоритма. В алгоритме учитываются ограничения на расходы, связанные с применением механизмов управления информационными рисками.

Для формального представления алгоритма вводятся следующие обозначения:

h – номер выполненного шага алгоритма;

$X_h(x_{h1}, x_{h2}, \ldots, x_{hK})$ – состояние вектора конфигурации после h-го шага алгоритма;

$W^l(h)$ – множество механизмов, включенных в число используемых на h-ом шаге алгоритма;

$S^l(h)$ – множество механизмов еще не включенных в число используемых на h-ом шаге алгоритма, но совместимых с механизмами множества $W^l(h)$;

$\Omega^l(h)$ – множество механизмов, несовместимых с множеством $W^l(h)$, т.е. исключаемых из дальнейшего рассмотрения;

$U_n^o(h)$ – остаточная величина ущерба от n-го риска после выбора механизмов на первых h шагах.

Таким образом, значения $x_{hk}=1$ соответствуют механизмам, уже отобранным на первых h шагах алгоритма, т. е. входящим в множество $W^l(h)$.

Пусть $m_{h+1} \in S^l(h)$– механизм, выбираемый на $h+1$- ом шаге из множества $S^l(h)$. Выбор механизма m_{h+1} означает, что соответствующий компонент в $X_h(x_{h1}, x_{h2}, \ldots, x_{hK})$ становится равным единице. Предположим, что выбранному механизму m_{h+1} в векторе X_h соответствует компонент с номером k.

Тогда величина, на которую уменьшится ущерб от n- го риска при выборе на шаге $h+1$ механизма m_{h+1}с номером k, равна $\Delta U_n(h+1,k)$ и определяется следующим образом:

$$\Delta U_n(h+1,k) = U_n^o(h) e_{kn}.$$

Оставшаяся величина ущерба от n- го риска при этом будет равна:

$$U_n^o(h+1,k) = U_n^o(h)(1-e_{kn}).$$

Суммарное уменьшение ущербов от рисков всех видов при выборе на h+1– ом шаге k- го механизма $\Delta U(h+1,k)$, равна:

$$\Delta U(h+1,k) = \sum_{n=1}^{N} \Delta U_n(h+1,k) = \sum_{n=1}^{N} U_n^o(h) e_{kn}.$$

Упускаемая возможность снижения ущербов на последующих шагах алгоритма $\Delta U_\tau^-(h+1,k)$, обусловлена исключением применения на следующих шагах механизма τ, несовместимого с механизмом k ($\tau \in \Omega^l(h)$).

Выражение для вычисления величины $\Delta U_\tau^-(h+1,k)$ имеет вид:

$$\Delta U_\tau^-(h+1,k) = \sum_{n=1}^{N} U_n^o(h)(1-e_{kn}) e_{\tau n} \bar{d}_{k\tau} s_{h\tau}^1,$$

где $\bar{d}_{k\tau}$ – инверсное значение $d_{k\tau}$ из матрицы совместимости D (если $d_{k\tau}=1$, то $\bar{d}_{k\tau}=0$ и наоборот); множитель $s_{h\tau}^1=1$, если $\tau \in S^l(h)$ и $s_{h\tau}^1=0$, если $\tau \notin S^l(h)$.

Присутствие множителя $s_{h\tau}^1$ в выражении позволяет учитывать на шаге $h+1$ механизм τ, который стал несовместным только на шаге $h+1$ в результате включения механизма k. Величина $U_n^o(h)(1-e_{kn})$ есть остаточный ущерб от n-го риска после применения механизма k на шаге h+1.

Суммарная упускаемая возможность снижения ущербов, в случае выбора на $h+1$- ом шаге k- го механизма, за счет исключения несовместимых с ним механизмов, равна:

$$\Delta U^-(h+1,k) = \sum_{\tau=1}^{K} \sum_{n=1}^{N} U_n^o(h)(1-e_{kn}) e_{\tau n} \bar{d}_{k\tau} s_{h\tau}^1.$$

Для оценки эффекта от включения на шаге h+1 k- го механизма управления информационными рисками введем величину $Э(h+1,k)$:

$$Э(h+1,k) = \Delta U(h+1,k) - (\Delta U^-(h+1,k) + c_k).$$

Эффект от включения механизма k в систему управления информационными рисками определяется как разность между суммарной величиной снижения ущербов за счет использования механизма k и суммой затрат на k - й механизм и общей величины ущерба, на которую не может быть уменьшен ущерб

предприятия из-за невозможности использования механизмов, несовместимых с механизмом k.

В соответствии с введенными обозначениями модифицированный жадный алгоритм состоит из следующих шагов. На каждом шаге h для $m \in S^l(h)$ вычисляется $Э(h+1,k)$ и выбирается такой механизм m^* с номером k^*, для которого $Э(h+1,k^*)$ имеет наибольшее значение и при этом не исчерпываются выделенные средства. Если такого механизма нет, то работа алгоритма прекращается и в качестве оптимального принимается вектор $X^*(x_1^*, x_2^*, ..., x_K^*)$.

Проведенные испытания точности модели показали, что с увеличением количества переменных точность метода снижается. Это объясняется тем, что величина $\Delta U_\tau^-(h+1,k)$ подсчитывается для всех механизмов, которые еще не включены в состав субоптимального подмножества. Причем учитываются и те механизмы, которые не попадут в окончательное субоптимальное подмножество механизмов.

Для повышения точности алгоритма изменен порядок расчета величины $\Delta U_\tau^-(h+1,k)$. При ее вычислении используется величина gl, получившая название «глубина просмотра». Она определяет максимальное количество механизмов, которые участвуют в подсчете величины $\Delta U_\tau^-(h+1,k)$. На каждом шаге определяется gl механизмов, которые могут стать несовместимыми после выбора механизма k. Причем в число механизмов, характеристики которых будут использованы при подсчете величины $\Delta U_\tau^-(h+1,k)$, включаются не более gl механизмов с наилучшими значениями $\Delta U(h+1,k) - c_k$. Глубина просмотра ограничивает количество анализируемых механизмов сверху. При выполнении алгоритма количество несовместимых с k механизмов может быть меньше gl.

Переменная величина gl зависит от количества механизмов K. Экспериментально было установлено, что наивысшая точность метода достигается, если величина gl находится в интервале $\frac{1}{4}K < gl < \frac{1}{3}K$.

В диссертации приводится также две разновидности рассмотренного метода: при совместном использовании отдельных и комплексных (агрегированных) механизмов управления информационными рисками, а также при условии обязательного включения в систему отдельных механизмов.

Задача в представленной постановке может быть решена также с помощью *генетического алгоритма*. Теория генетических алгоритмов определяет лишь общие положения построения алгоритмов такого класса. Конкретный вид алгоритма определяется условиями решаемой задачи. Для решения задачи выбора механизмов управления информационными рисками предложен метод на основе генетического алгоритма, включающий следующие шаги.

Шаг 1. Формируются исходные данные для моделирования. Целевая функция, матрицы совместимости и коэффициентов снижения рисков, а также ограничения полностью соответствуют приведенным в постановке задачи выбора механизмов управления информационными рисками. Применительно к терминологии генетических алгоритмов в качестве особи рассматривается век-

тор $X=(x_1, x_2, \ldots, x_K)$. Задается также число повторений и мощность начального множества особей (популяции).

Шаг 2. Случайным образом генерируется исходная популяция.

Шаг 3. Производится операция скрещивания особей (выполняется оператор кроссовер). Сначала случайным образом образуются пары особей. В соответствии с классическим оператором кроссовера используется одна, случайно выбранная, точка разрыва n. Биты с номерами с 1 по n одной особи в паре замещаются битами с соответствующими номерами другой особи. Обмен битами не выполняется в паре особей с номерами битов, большими n, то есть они остаются без изменений.

Шаг 4. Выполняется оператор мутации. Значение каждого бита особи изменяется на инверсное с установленной вероятностью. Для каждой особи вычисляется целевая функция (1), называемая функцией приспособленности.

Шаг 5. Отбираются особи для нового поколения. Из множества возможных принципов отбора выбран элитный принцип формирования новой популяции. Особи в популяциях сортируются в порядке возрастания функции приспособленности особей. Новая популяция формируется из особей, входящих в первую половину предыдущей и текущей популяций. Проверяются условия окончания работы алгоритма. Выход из цикла осуществляется при достижении заданного числа повторений шагов 3-5.

Модели модифицированного жадного алгоритма и генетического алгоритма реализованы в программе «Выбор механизмов». Для определения практических границ использования метода полного перебора и оценки точности рассмотренных алгоритмов в программу включен модуль полного перебора механизмов. По результатам моделирования получены следующие основные результаты.

Практические границы применимости метода полного перебора ограничиваются количеством механизмов <30-35. Выявлены предельные возможности использования генетического алгоритма в зависимости от степени несовместимости механизмов при фиксированных значениях количества механизмов в популяции и циклов алгоритма. Алгоритм эффективен в диапазоне 10-80 механизмов при количестве несовместимых механизмов <10%. При малых значениях несовместимости механизмов (<1%) во всем рабочем диапазоне генетический алгоритм превосходит жадный алгоритм по точности, при удовлетворительных значениях времени моделирования.

Жадный алгоритм существенно превосходит все остальные алгоритмы по времени моделирования (<1 мин. при количестве механизмов равном 100). Средняя относительная погрешность не превышает 5% на всем рабочем диапазоне исходных данных. Наихудшие реализации по точности с учетом адекватного подбора глубины просмотра *gl* не превышают 15%. Полные результаты сравнительного анализа представлены в диссертации в графическом виде.

Наряду с задачей выбора механизмов СУИР могут решаться задачи построения (выбора) подсистем информационной системы, обеспечивающих минимальную сумму расходов на создание (приобретение) подсистемы и величи-

ны общего ущерба от информационных рисков, которые могут иметь место при эксплуатации этой подсистемы.

Примером может служить задача *выбора подсистемы хранения данных* информационной системы. Задача формулируется следующим образом. При существующем уровне надежности аппаратных и программных средств, известных характеристиках информационных рисков, а также заданных ограничениях на быстродействие и емкость системы необходимо выбрать (создать) систему хранения данных, которая обеспечивала бы минимальные суммарные расходы, связанные с ее приобретением (созданием) и эксплуатацией, а также ущербом от наступления рисковых событий, нарушающих целостность и доступность информации. Для решения этой задачи создана модель, основанная на использовании аппарата цепей Маркова.

Для определенности в качестве подсистем хранения данных рассматриваются подсистемы, построенные с использованием RAID технологии.

Расходы на хранение и обеспечение доступа к данным исчисляются как сумма расходов на создание и модернизацию подсистемы хранения данных в пересчете этих расходов на год предполагаемой эксплуатации, а также затрат на эксплуатацию подсистемы хранения. Общий ущерб, связанный с рисками в сфере хранения данных предприятия, может быть определен следующим образом:

$$U_x = U_\partial + U_в + U_y ,$$

где U_∂ – ущерб от превышения времени доступа к данным; $U_в$ – ущерб, связанный с ремонтом (заменой) и восстановлением данных с использованием контрольной или резервной информации; U_y – ущерб от полной утраты информации. Величины соответствующих ущербов подсчитываются следующим образом:

$$U_\partial = \sum_{i=1}^{M} u_d^i\ (t_в^i);\ U_в = \sum_{i=1}^{M} u_в^i\ ;U_y = \sum_{i=1}^{M} u_y^i \nu , \quad (2)$$

где M – количество рисковых событий, имевших место за год; $u_d^i(t_в^i)$ – функция ущерба от i- го риска, зависящая от времени пребывания подсистемы хранения в недоступном состоянии $t_в^i$; $u_в^i$ – затраты на восстановление работоспособности блока и утраченных в результате i- го риска данных с использованием резервной (контрольной) информации; u_y^i – ущерб от утраты единицы объема данных, при которой информация утрачивается безвозвратно или требуется повторить весь процесс ее получения; ν – емкость блока в единицах объема данных.

Оценка общего ущерба U_x, связанного с использованием системы хранения, может быть получена с помощью математических ожиданий величин в выражениях (2). Тогда

$$U_x = u_d m_o + u_в m_o + u_y k_y m_o \nu ,$$

где $u_d, u_в, u_y$ – математические ожидания величин соответствующих ущербов, m_o – математическое ожидание количества рисковых событий за год, k_y<1

– коэффициент, определяющий, какую часть рисков от M составляют риски полной утраты информации.

Для определения вероятностно-временных характеристик подсистемы хранения данных использован аппарат марковских цепей.

Поскольку для анализа RAID-системы, состоящей из n независимых блоков с интенсивностями наступления рисковых событий λ_o и восстановления работоспособности блоков λ_v, достаточно различать только работоспособное и неработоспособное состояния, то граф состояний подсистемы может быть укрупнен (рис. 3).

Работоспособное состояние S_p соответствует состоянию, в котором работоспособны все блоки или неработоспособен только один блок. Все остальные состояния подсистемы соответствуют неработоспособному состоянию $S_н$. Интенсивности переходов соответствуют интенсивностям переходов состояний из полного графа для граничных состояний переходов между работоспособными и неработоспособными состояниями.

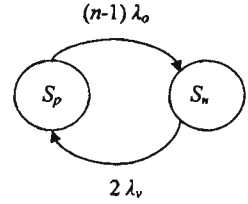

Рис. 3. Укрупненный граф состояний подсистемы хранения данных

В теории эксплуатации ЭВМ доказано, что случайные величины времени наступления отказов и времени восстановления электронных устройств подчиняются экспоненциальному закону распределения. Поток случайных событий разной природы, приводящих в неработоспособное состояние подсистему хранения данных, можно рассматривать как суперпозицию потоков независимых событий, интенсивность которых мала по сравнению с интенсивностью суммарного потока. Известно, что характеристики такого потока близки к характеристикам простейшего потока.

Тогда математическое ожидание m_o количества отказов независимых блоков за время t составит $m_o = (n-1)\lambda_o t$. А среднее время восстановления отказа $t_в$ определяется следующим образом: $t_в = \frac{1}{\lambda_v}$.

Финальная веротность нахождения системы в работоспособном состоянии P_p определяется из системы уравнений Колмогорова:

$$\begin{cases} -P_p(n-1)\lambda_o + P_н 2\lambda_v = 0 \\ P_p + P_н = 1. \end{cases} \qquad P_p = \frac{2\lambda_v}{(n-1)\lambda_o + 2\lambda_v}.$$

Интенсивности отказов определяются из статистических данных и документации на систему. Оценка характеристик ущерба производится на

основе анализа ценности информации на конкретном предприятии одним из выбранных методов.

Предполагаемые приведенные затраты на создание и эксплуатацию подсистемы хранения данных определяются достаточно просто. Общие расходы подсчитываются для каждой анализируемой подсистемы с возможными для нее уровнями RAID. С учетом ограничений на быстродействие и емкость подсистем, количество сочетаний подсистема-уровень не велико и позволяет организовать полный перебор перспективных вариантов. Для сокращения вычислительной сложности алгоритма возможно проведенение предварительного отбора вариантов с помощью экспертов.

Пятая группа проблем связана с оценкой и оптимизацией расходов на управление информационными рисками, комплексным применением экономических методов управления информационными рисками предприятий.

Предложенный подход к пониманию содержания информационных рисков требует разработки методологии определения расходов на управление рисками и активного использования экономических методов управления этими рисками. Для снижения ущерба при наступлении рискового события используются нефинансовые и финансовые механизмы. К нефинансовым механизмам относятся создание резервных запасов материальных средств, включая резервное оборудование, дублирование информации, создание средств оперативного обнаружения рисковых событий и локализации их воздействия на ИСП, создание организационных структур (возможно, нештатных) для оценки и устранения последствий информационных рисков, разработка планов действий и инструкций в условиях наступления рисковых событий.

Финансовые механизмы сокращения ущерба, нанесенного информационными рисками, предполагают создание резервов денежных средств и страхование информационных рисков. Расходы на управление определенным информационным риском зависят от того, какая стратегия управления риском выбрана для этого риска: принятие риска; предотвращение информационного риска; минимизация ущерба от риска; предотвращение информационного риска и минимизация ущерба от него.

Выражение для вычисления расходов на управление i- м информационным риском при выборе в отношении него стратегии принятия риска имеет следующий вид: $c_i^1 = p_i u_i$, где p_i – вероятность i- го риска, u_i – ожидаемая величина ущерба в денежном исчислении при наступлении i- го риска.

Если в отношении информационного риска выбрана вторая стратегия, то расходы на управление таким риском могут быть подсчитаны следующим образом: $c_j^2 = \nu_j + p_j u_j$, где p_j и u_j имеют тот же смысл, что и для первой стратегии, а ν_j – затраты на предотвращение j- го информационного риска.

При выборе третьей стратегии выражение для определения расходов на управление информационным риском имеет вид: $c_k^3 = \eta_k + p_k u_k$. Кроме известных уже обозначений p и u, в выражении используется величина η_k , которая обозначает затраты на снижение ущерба от k- го информационного риска.

Если для управления информационным риском выбрана четвертая стратегия, то затраты на управление l- м риском следует определять следующим образом: $c_l^4 = \nu_l + \eta_l + p_l u_l$. Все обозначения в выражении совпадают с ранее использованными обозначениями с точностью до индекса.

Если для снижения величины ущерба от k- го информационного риска используются нефинансовые механизмы, а также страхование, то для подсчета затрат на эти механизмы может быть использовано выражение: $\eta_k = \omega_k + h_k$, где ω_k – затраты на нефинансовые механизмы, h_k – страховой взнос при страховании от k- го информационного риска.

При страховании информационных рисков расходы предприятий сокращаются на величину страховой суммы φ_k в случае наступления k- го рискового события. Иными словами, ущерб u_k уменьшается на величину φ_k.

Если денежные резервы используются не полностью за рассматриваемый период, то расходы на их создание и использование могут вычисляться следующим образом: $\Delta\varepsilon = k_\mu \varepsilon - \varepsilon_o$, где $\Delta\varepsilon$ – расходы на создание и использование собственных и заемных денежных резервов, $k_\mu > 1$ – коэффициент учета затрат на создание и обслуживание резерва, ε – сумма резерва, ε_o – остаток резервного фонда.

Учитывая все введенные обозначения и приведенные соотношения, затраты предприятия на управление всеми значимыми информационными рисками представим следующим образом:

$$C = \sum_{i=1}^{N} p_i u_i + \sum_{j=1}^{J} \nu_j + \sum_{k=1}^{K} \omega_k + \sum_{l=1}^{L} (h_l - p_l \varphi_l) + \Delta\varepsilon , \qquad (3)$$

где N – общее количество значимых рисков, J – количество информационных рисков, для которых используются механизмы предотвращения рисковых событий, K – количество информационных рисков, для минимизации ущерба от которых применяются нефинансовые механизмы, L – количество страхуемых информационных рисков.

В практике страхования общепринято использование коэффициентов для подсчета страхового взноса от страховой суммы. Поэтому в (3) выполним подстановку $h_l = k_l^h \varphi_l$, где k_l^h – коэффициент, учитывающий вероятность l- го риска:

$$C = \sum_{i=1}^{N} p_i u_i + \sum_{j=1}^{J} \nu_j + \sum_{k=1}^{K} \omega_k + \sum_{l=1}^{L} (k_l^h - p_l) \varphi_l + \Delta\varepsilon . \qquad (4)$$

Проведем анализ выражения полных расходов на управление информационными рисками предприятия. Для этого представим нефинансовые величины выражения (4) в виде функциональных зависимостей от затрат. Вероятность информационного риска $p_i(\nu_i)$ является функцией от затрат на предотвращение этого информационного риска. Величина ущерба зависит от затрат на нефинансовые механизмы снижения ущерба и затрат на создание и обслуживание резерва собственных денежных средств $u(\omega_i, \Delta\varepsilon_i)$, где $\Delta\varepsilon_i$ - часть собственных

денежных резервов, используемая для снижения ущерба от i- го информационного риска.

Страховая сумма есть функция от ожидаемого ущерба и зависит от тех же затрат, что и ущерб. Страховой взнос зависит от величины страховой суммы и вероятности наступления страхового события.

Снижение вероятности рискового события, величины ожидаемого ущерба, страхового взноса при использовании соответствующих механизмов предотвращения информационного риска и снижения ущерба от него могут учитываться с помощью коэффициентов. Предположим, что при использовании комплекса антивирусных программ коэффициент снижения вероятности недоступности информации в ИСП равен 1/3. Тогда при установке пакета антивирусных средств в ИСП получим значение вероятности недоступности информации:

$$p_i^{av} = k^{av} p_i = p_i / 3 ,$$

где p_i^{av} – вероятность перехода системы в состояние недоступности информации при наличии антивирусной защиты за определенный период времени (например – за год), k^{av} – коэффициент учета эффективности антивирусного средства и доли вирусов в данном информационном риске, p_i – вероятность информационного риска без учета антивирусной защиты.

Зависимость величины ущерба от затрат на механизмы его снижения может быть учтена также с помощью коэффициентов эффективности вводимых механизмов. С использованием системы коэффициентов соотношение (4) принимает вид:

$$C = \sum_{i=1}^{N} k_i^p(v_i) p_i k_i^u(\omega_i, \Delta\varepsilon_i) u_i + \sum_{j=1}^{J} v_j + \sum_{k=1}^{K} \omega_k + \sum_{l=1}^{L} (k_l^h(v_l) - k_l^p(v_l) p_l) k_l^\varphi(v_l, \omega_l, \Delta\varepsilon_l) \varphi_l + \Delta\varepsilon \quad (5)$$

В этом выражении коэффициенты имеют следующие значения. Коэффициент $k_i^p(v_i)$ определяет, как изменится вероятность наступления i- го рискового события при использовании механизмов предотвращения риска, затраты на которые составили сумму v_i. Коэффициент $k_l^p(v_l)$ имеет тот же смысл, что и коэффициент $k_i^p(v_i)$, но для l-го риска. Коэффициент $k_i^u(\omega_i, \Delta\varepsilon_i)$ учитывает зависимость величины ущерба при наступлении i- го рискового события от суммы вложенных средств в механизмы сокращения величины ущерба. Коэффициент $k_l^\varphi(v_l, \omega_l, \Delta\varepsilon_l)$ определяет насколько изменится страховая сумма l- го информационного риска по сравнению с исходной (φ_l) после введение в СУИР механизмов предотвращения этого риска и снижения ущерба от него. Коэффициент вычисления страхового взноса $k_l^l(v_l)$ выбирается страховщиком в зависимости от эффективности механизмов предотвращения информационных рисков, которые применяет страхователь в своей ИСП. Считаем, что эффективность механизмов зависит от суммы вкладываемых в них средств.

Система управления информационными рисками является подсистемой системы управления предприятием. Полная оценка расходов на информационные риски должна учитывать взаимодействие данной подсистемы с другими подсистемами предприятия.

В выражении (5) не учитываются затраты на интеграцию всех механизмов защиты от информационных рисков в единую систему управления, затраты ресурсов ИСП и всего предприятия на нужды защиты от информационных рисков. Имеются в виду ресурсы, которые непосредственно не относятся к ресурсам СУИР, но используются для выполнения определенных функций управления информационными рисками.

Если системные затраты подсчитывать как сумму по каждому информационному риску, то выражение для подсчета полных расходов на управление информационными рисками примет следующий вид:

$$C_f = \sum_{i=1}^{N} c_s^i + \sum_{i=1}^{N} k_i^p(\nu_i) p_i k_i^q(\omega_i, \Delta\varepsilon_i) q_i + \sum_{j=1}^{J} \nu_j + \sum_{k=1}^{K} \omega_k + \sum_{l=1}^{L} (k_l^h(\nu_l) -$$

$$- k_l^p(\nu_l) p_l) k_l^\varphi(\nu_l, \omega_l, \Delta\varepsilon_l) \varphi_l + \Delta\varepsilon,$$

где C_f – полные расходы на управление информационными рисками, c_s^i – системные затраты на управление i-м информационным риском.

В зависимости от целей анализа расходов на управление информационными рисками могут подсчитываться расходы на создание системы управления информационными рисками, полные расходы на управление рисками за определенный период времени (обычно за один год) и общие расходы на управление информационными рисками на конец определенного года эксплуатации СУИР.

При подсчете полных расходов на управление информационными рисками могут быть использованы положения методики определения совокупной стоимости владения (Total Cost of Ownership, TCO). Применяя данную методику можно решить следующие задачи, связанные с расходованием средств на управление информационными рисками: определение полных расходов на создание и обеспечение функционирования СУИР; сравнение затрат предприятия на управление информационными рисками с такими же затратами на других предприятиях; повышение эффективности инвестирования в управление информационными рисками; определение направлений развития СУИР; обоснование части бюджета предприятия, направляемой на управление информационными рисками; определение эффективности нового проекта развития СУИР; определение стоимости услуг внешних организаций в области управления информационными рисками; определение эффективности СУИР в целом.

По сравнению с существующими методиками, предлагается учитывать все расходы с учетом нового представления об информационных рисках, а также системные расходы. Расходы на управление информационными рисками разделяются на группы в соответствии с целями исследования. Такой подход принят в бухгалтерском управленческом учете. Необходимо учитывать также особенности определения затрат на выполняемые операции, материальные средства, нематериальные активы. Следует учитывать необходимость выделения расходов на защиту от информационных рисков из общих расходов на информационные технологии, поскольку система управления информационными рисками является подсистемой информационной системы предприятия.

Целью управления информационными рисками предприятия является минимизация общих расходов на управление рисками, которые складываются из затрат на противодействие информационным рискам и ущерба, который несет предприятие в случае реализации рисковых событий. Известно, что искомый теоретический минимум общих расходов будет достигаться при равенстве затрат на противодействие информационным рискам и величины ущерба. Для сравнения эффективности СУИР, кроме абсолютных величин показателей, целесообразно использовать относительные величины показателей. Введем относительный показатель эффективности системы СУИР предприятия, который назовем приведенными полными расходами предприятия на управление информационными рисками C_{oc}. Тогда приведенные полные затраты на управление информационными рисками определяются следующим образом:

$$C_{oc} = \frac{C_f}{C_e},$$

где C_f – полные годовые расходы на управление информационными рисками, C_e – показатель эффективности функционирования предприятия. В качестве показателя эффективности функционирования предприятия могут использоваться: годовая прибыль предприятия, годовой объем производства продукции, годовой товарооборот, объем оказанных услуг и другие.

Приведенные полные расходы на управление информационными рисками позволяют сравнивать эффективность функционирования СУИР разных по масштабам предприятий, а также получать объективную оценку расходов на управление информационными рисками в условиях расширения и реконструкции предприятия.

Выбор того или иного показателя эффективности функционирования предприятия определяется целями исследования. Для сравнения показателей разных по масштабам предприятий или показателей предприятия в условиях реконструкции и развития в качестве показателя эффективности целесообразно выбирать показатели, характеризующие масштабы предприятия: объем произведенной продукции или услуг, стоимость основных средств и т. п.

При анализе эффективности вложения средств в различные сферы деятельности предприятия, при определении структуры расходов может использоваться показатель ROI (Return of Investments). Показатель ROI – это отношение экономического эффекта (прибыли или другого) от проекта к инвестициям, необходимым для реализации этого проекта. Реже ROI определяется как период, в течение которого полностью окупаются инвестиции. Применительно к анализу эффективности СУИР в качестве отношения могут использоваться следующие величины: в числителе – величина снижения ущерба от информационных рисков, а в знаменателе – вложение средств в СУИР (затраты на управление информационными рисками). Обе величины отношения подсчитываются за определенный интервал времени – обычно за один год.

Все приведенные показатели (полные расходы на управление информационными рисками, приведенные полные расходы на управление и ROI) имеют один общий недостаток – имеют статический характер. Они не учитывают воз-

можные изменения экономической ситуации во внешней и внутренней среде предприятия.

Для преодоления этого недостатка оценка эффективности вложения средств в управление информационными рисками может оцениваться с помощью динамических показателей, основанных на методе дисконтированных потоков денежных средств (Discounted Cash Flows – DCF). Оценка может осуществляться с помощью показателя чистой текущей стоимости (Net Present Value – NPV) и внутреннего коэффициента отдачи (Internal Rate of Return – *IRR*). Коэффициент *IRR* равен значению ставки дисконтирования, при которой показатель *NPV* равен 0. Тогда в качестве критерия принятия проекта может быть использовано условие: коэффициент *IRR* не меньше ставки дисконтирования. В работе приводится пример расчета показателя *NPV* для оценки инвестиций в проект усовершенствования подсистемы расчетов по банковским картам.

Актуальной является проблема использования *страхования информационных рисков* в качестве одного из наиболее эффективных механизмов защиты от информационных рисков. Специфику страхованию информационных рисков придают следующие особенности информационных рисков: сложность оценки ущерба от информационных рисков; необходимость обязательной экспертизы (сюрвея) при заключении договора; сложность сбора необходимых статистических данных об информационных рисках; сложность определения и правового подтверждения факта наступления страхового случая. На страхование информационных рисков оказывают влияние и особенности страховой системы и страхового рынка Российской Федерации: отсутствие развитой системы правового регулирования страхования информационных рисков; отсутствие необходимых методик страхования информационных рисков; отсутствие независимых лицензированных организаций аудита информационных систем, имеющих опыт работы в страховом бизнесе; страхование экономических рисков вообще и страхование информационных рисков в частности находятся в стадии становления.

Формальная постановка задачи оптимизации расходов на управление информационными рисками с применением механизмов страхования без ограничения на привлекаемые средства формулируется следующим образом. Требуется распределить средства на создание (приобретение) механизмов управления информационными рисками, включая страхование, таким образом, чтобы обеспечить минимальное значение общих расходов на управление информационными рисками:

$$C = \sum_K P_k U_k + \varepsilon + \sum_I (V_i + P_i \Delta U_i) + \sum_J (a_j + b_j + P_j(a_j) U_j(b_j)) + \\ + \sum_Z (a_z + b_z + V_z(a_z, b_z) + P_z(a_z) \Delta U_z(a_z, b_z)),$$

где K – подмножество принимаемых информационных рисков; ε – потери от создания собственных резервов для оперативного снижения ущерба; I – подмножество рисков, которые управляются только с помощью страхования; J – подмножество рисков, в отношении которых применяются только нефинансовые механизмы регулирования; Z – подмножество рисков, которые регулиру-

ются с помощью нефинансовых механизмов и страхования; a_i – затраты на предотвращение i- го информационного риска, b_i – затраты на снижение ущерба от i- го информационного риска; V_i – страховой взнос, P_i – вероятность наступления i- го рискового события, U_i – ожидаемый ущерб от i- го рискового события; ΔU_i величина франшизы. При установленной величине прибыли от страхования и величине франшизы расходы предприятия на управление i- м информационным риском зависят только от затрат на его предотвращение и снижение ущерба от этого риска. Ожидаемые значения вероятности наступления i- го рискового события и ущерба от этого риска зависят от затрат на нефинансовые механизмы противодействия риску.

Поставленная задача может быть решена одним из рассмотренных переборных алгоритмов. В работе представлена также модель с ограничениями на средства, которые могут быть направлены на управление информационными рисками.

К шестой группе относятся проблемы разработки практических рекомендаций по созданию организационных и организационно-технических подсистем информационной системы предприятия.

В этой группе представлены результаты обоснования рекомендаций по созданию организационной подсистемы СУИР и рекомендации по созданию компьютера защищенной структуры. Обоснование получено в результате использования нового подхода к пониманию информационных рисков, анализа современных технологий и тенденций создания организационно-технических систем, требований нормативно-правовых документов и обобщения практического опыта создания таких систем. В концентрированном виде основные рекомендации *по созданию компьютера защищенной структуры* могут быть сформулированы следующим образом:

- для выполнения функций обеспечения и контроля качества, а также безопасности обрабатываемой информации целесообразно выделить один из процессоров (ядер) компьютера;
- в архитектуре компьютера следует предусмотреть механизмы, которые обеспечивали бы доступ сотрудников служб безопасности и информационных отделов только к служебной информации, а к рабочей информации были допущены только пользователи ИСП;
- компьютер защищенной структуры должен обеспечивать возможность участия в управлении информационными рисками менеджерам и руководству предприятия, причем процесс должен быть максимально автоматизирован;
- в вычислительных системах, созданных на основе компьютеров защищенной структуры, необходимо реализовать режим функциональной замкнутости, который исключал бы возможность выполнения программ, не имеющих специального паспорта безопасности.

Анализ целей, решаемых задач и принципов построения СУИР показывает, что такая система не может создаваться как отдельная организационная единица предприятия. Задачи управления информационными рисками решаются на

всех уровнях и во всех звеньях управления и производственной деятельности. Каждый сотрудник предприятия в соответствии со своими функциональными обязанностями принимает участие в управлении информационными рисками.

Система управления информационными рисками должна объединять в единую систему все элементы предприятия, участвующие в управлении информационными рисками. Система управления предприятием адаптируется для выполнения, наряду с другими задачами, задач управления информационными рисками. При этом не требуется кардинально изменять организационно-штатную структуру предприятия. Необходимо лишь реорганизовать ее, в максимальной степени приспособить к решению задач управления информационными рисками.

Автором предлагаются следующие пути формирования структуры СУИР: объединение отделов (служб, специалистов) в единую организационную структуру, решающую важные задачи в одной области информационной сферы предприятия; создание нештатных управляющих органов; структурирование функциональных обязанностей сотрудников в области управления информационными рисками; полное комплексное обеспечение эффективного функционирования организационной структуры СУИР.

Структурный анализ исрархии информационных потоков и процессов информационной сферы предприятия позволяет выделить функции, которые необходимо решать в процессе управления информационными рисками. Для выполнения выделенных функций создается организационная система, один из возможных вариантов которой представлен в работе.

По теме диссертации опубликованы следующие основные работы.

I. Монографии

1. Завгородний В.И. Информационные риски: сущность, концепция управления [Текст] /Завгородний В.И. – М.: ЗАО «Издательство «Экономика», 2007. – 11,0 п.л.
2. Завгородний В.И. Информационные риски и экономическая безопасность предприятия [Текст] /Завгородний В.И. – М.: Финакадемия, 2008. – 9,3 п.л.
3. Завгородний В.И. Управление информационными рисками предприятия [Текст] /Завгородний В.И. – М.: ИНИОН РАН, 2009. – 11,0 п.л.

II. Статьи в периодических научных изданиях, рекомендованных ВАК Министерства образования и науки РФ для опубликования основных результатов диссертации на соискание ученой степени доктора наук

4. Завгородний В.И. Концепция создания ЭВМ защищенной архитектуры [Текст] /Завгородний В.И. //Безопасность информационных технологий. №1, 2006. – 0,75 п.л.
5. Завгородний В.И. Оценка расходов на управление информационными рисками [Текст] /Завгородний В.И. //Проблемы теории и практики управления. №4, 2006. – 0,45 п.л.
6. Завгородний В.И. Методика выбора механизмов управления информационными рисками [Текст] /Завгородний В.И. //Вестник Финансовой академии. №3, 2006. – 0,9 п.л.

7. Завгородний В.И. Функции персонала предприятия в современной системе управления информационными рисками [Текст] /Завгородний В.И. // Управление персоналом №18, 2007. – 0,3 п.л.
8. Завгородний В.И. Комментарий к новой дисциплине «Управление информационными рисками» [Текст] /Завгородний В.И. //Вестник Финансовой академии. №3. 2007.– 0,6 п.л.
9. Завгородний В.И. Выбор методов и средств управления информационными рисками [Текст] /Завгородний В.И. //Аудит и финансовый анализ. №5, 2007. – 1,2 п.л.
10. Завгородний В.И. Информационные риски: сущность и механизмы управления [Текст] /Завгородний В.И. //Сегодня и завтра российской экономики. №20, 2008. – 0,45 п.л.
11. Завгородний В.И. Системный анализ информационных рисков [Текст] /Завгородний В.И. //Вестник Финансовой академии. №4, 2008. – 0,65 п.л.
12. Завгородний В.И. Информационный риск-менеджмент [Текст] /Завгородний В.И. //РИСК: Ресурсы. Информация. Снабжение. Конкуренция. №4, 2008. – 0,7 п.л.
13. Завгородний В.И. Системное управление информационными рисками. Выбор механизмов защиты от информационных рисков [Текст] /Завгородний В.И. //Проблемы управления. №1, 2009. – 0,96 п.л.

III. Статьи в других периодических изданиях

14. Завгородний В.И. Анализ расходов на управление информационными рисками [Текст] /Завгородний В.И. //Бюллетень финансовой информации. №9-10 (124-125), 2005. – 0,7 п.л.
15. Завгородний В.И. Информация и экономическая безопасность предприятия [Текст] /Завгородний В.И. //Прикладная информатика. №2, 2006. – 0,5 п.л.
16. Завгородний В.И. Информационные и банковские риски [Текст] /Завгородний В.И. // Банковские услуги .- 2006. – 0,5 п.л.
17. Завгородний В.И. Подготовка студентов к работе в условиях информационных рисков [Текст] /Завгородний В.И. //Вестник Московского городского педагогического университета. №2, 2006. – 0,23 п.л.
18. Завгородний В.И. Управление на информационните рискове (на болгарском языке) [Текст] /Завгородний В.И. // //Бизнес управление. Год XVI Кн.4 Свищов: Полиграфична база на Академично издательство «Ценов» при Стопанска академия «Д.А.Ценов» – Свищов, 2006. – 1,25 п.л.
19. Завгородний В.И. Перспективы создания защищенной ЭВМ [Текст] /Завгородний В.И. //SORUCOM.2006:Развитие вычислительной техники в России и странах бывшего СССР: история и перспективы. Материалы I Международной конференции В 2 ч. Ч. 2 – Петрозаводск: Петрозаводский государственный университет, 2006. – 0,64 п.л.

20. Завгородний В.И. Управление внедрением новых информационных технологий на муниципальном уровне [Текст] /Завгородний В.И. // Российская модель местного самоуправления: технологии эффективной реализации: сборник статей Межрегиональной научно-практической конференции. Воронеж: Воронежский государственный университет, 2007. – 0,4 п.л.
21. Завгородний В.И. Информационные риски. Сущность, концепция управления и анализ [Текст] /Завгородний В.И. //Вопросы анализа риска. №2, 2007. – 1,3 п.л.
22. Завгородний В.И. От обеспечения безопасности информации к эффективности информационной сферы организации [Текст] /Завгородний В.И. Научное, экспертно-аналитическое и информационное обеспечение стратегического управления, разработки и реализации приоритетных национальных проектов и программ. Сб. науч. тр. ИНИОН РАН. Редкол.: Пивоваров Ю.С. (отв. Ред.) и др. - М.: ИНИОН РАН, 2007. – 1,5 п.л.
23. Завгородний В.И. Что имеем - бережем. Как обеспечить сохранность информации [Текст] /Завгородний В.И. //Risk management. №4, 2007. – 1 п.л.
24. Завгородний В.И. Особенности создания защищенной компьютерной системы как элемента системы управления информационными рисками [Текст] /Завгородний В.И. //Вестник компьютерных и информационных технологий. №4(46), 2008. – 0,5 п.л.
25. Завгородний В.И. Системный подход к управлению информационными рисками предприятия [Текст] /Завгородний В.И. Научное, экспертно-аналитическое и информационное обеспечение стратегического проектирования, приоритетных национальных проектов и программ. Сб. науч. тр. ИНИОН РАН. Редкол.: Пивоваров Ю.С. (отв. Ред.) и др. - М.: ИНИОН РАН, 2009. – 1,2 п.л.
26. Завгородний В.И. Управление информационными рисками в условиях неопределенности [Текст] /Завгородний В.И. Сборник трудов 3-й Международной научно-практической конференции «Информационные технологии в образовании, науке и производстве», 29.06-3.07.2009 г., ч.2.: – Серпухов, 2009, с. 265-267. – 0,3 п.л.
27. Завгородний В.И. Исследование информационных рисков в условиях неопределенности [Текст] /Завгородний В.И. //Информационно-аналитическое обеспечение управления: история и современность: материалы научно-практической конференции. Ч.1. – М.: Финакадемия; Тольятти: Изд-во ПВГУС, 2009. – С. 124-134. – 0,57 п.л.
28. Optimization of management by information risks of the enterprise [Текст] /Завгородний В.И. //Сборник доклади от международна научна конференция «Бизнес информатика» 11 октября 2007 г. София: Университет за национално и световно стопанство, 2007. – 0,4 п.л.

2