

**Б. В. Сазыкин, А. Г. Краев,  
В. П. Климов**

# **Управление операционным риском АЭС**

**Москва 2010**

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ  
УНИВЕРСИТЕТ «МИФИ»

Б.В. Сазыкин, А.Г. Краев, В.П. Климов

# Управление операционным риском АЭС

Учебное пособие

Москва 2010

УДК621.311.25:004.056.5(075)

ББК 31.47ня7

С14

*Сазыкин Б.В., Краев А.Г., Климов В.П.* **Управление операционным риском АЭС: Учебное пособие.** – М.: НИЯУ МИФИ, 2010. – 144 с.

В пособии изложены теоретические и практические подходы к управлению безопасностью и рисками АЭС. Рассмотрены качественные и количественные модели управления операционным риском. Основное внимание уделено процессному подходу к управлению операционным и технологическим рисками.

Пособие предназначено для студентов и аспирантов НИЯУ МИФИ, изучающих данные проблемы.

Рецензент: *С. Л. Буторин*, д-р техн. наук, первый зам. директора Международного центра по ядерной безопасности (АНО МЦЯБ)

Рекомендовано к изданию редсоветом НИЯУ МИФИ

ISBN 978-5-7262-1336-1

© *Национальный исследовательский ядерный университет «МИФИ»*, 2010

Редактор *Е.Н. Кочубей*

Макет подготовлен *Е.Н. Кочубей*

Подписано в печать 30.09.2010.      Формат 60×84 1/16.

Печ. л. 9,0.    Уч.-изд. 9,0.    Тираж 100 экз.

Изд. № 068-1.    Заказ № 317.

Национальный исследовательский ядерный университет «МИФИ»  
Типография НИЯУ МИФИ. 115409, Москва, Каширское ш., 31

# СОДЕРЖАНИЕ

Предисловие .....	4
<b>Раздел 1. Введение: проблемы управления безопасностью и рисками АЭС .....</b>	<b>6</b>
1.1. Безопасность АЭС .....	7
1.2. Управление безопасностью АЭС .....	14
1.3. Понятие риска и его место в обеспечении рентабельной безопасности АЭС .....	22
1.4. Управление рисками АЭС .....	29
1.5. Требования к процессу анализа риска .....	35
Вопросы и ответы .....	40
Тесты для самоконтроля .....	48
<b>Раздел 2. Управление операционным риском: процессный подход .....</b>	<b>50</b>
2.1. Основные понятия и определения .....	51
2.2. Декомпозиция задачи управления операционным риском .....	53
2.3. Стратегия управления операционным риском .....	55
2.4. Анализ и оценка операционного риска .....	57
2.5. Принятие решения и разработка мер реагирования на риск .....	62
2.6. Мониторинг и контроль операционного риска .....	65
Вопросы и ответы .....	67
Тесты для самоконтроля .....	72
<b>Раздел 3. Методы оценки операционного риска .....</b>	<b>73</b>
3.1. Методики измерения операционного риска, применяемые на практике .....	74
3.2. Усовершенствованные методы измерения операционного риска .....	75
3.3. Внутренняя рейтинговая модель для измерения операционного риска .....	77
3.4. Экспертная оценка операционного риска с применением структурных и логических моделей .....	82
3.5. Расчёт ожидаемых потерь бизнес-процесса методом ФСА .....	94
Вопросы и ответы .....	96
Тесты для самоконтроля .....	105
<b>Раздел 4. Модели оптимизации ТОиР для структурных компонент оборудования АЭС с учётом операционного риска .....</b>	<b>108</b>
4.1. Модели оптимизации ремонтного цикла с учётом показателей надёжности оборудования, инвестиционной и рисковости составляющими стоимости цикла .....	109
4.2. Применение моделей оптимизации для оценки длительности ремонтного цикла системы технического водоснабжения АЭС .....	119
Тесты для самоконтроля .....	132
<b>Заключение .....</b>	<b>134</b>
Библиография .....	138
Приложение 1. Классы направлений деятельности АЭС и классы событий .....	141
Приложение 2. Примеры структурных моделей бизнес-процессов .....	142

## Предисловие

В настоящее время во многих отраслях человеческой деятельности происходит смена концепций управления риском. В частности, концепция «безопасность – риск» заменяется концепцией «устойчивое развитие – риск». И это оправдано: ведь критики концепции безопасности (рассматриваемой как состояние защищённости объекта) полагают, что АЭС следует «закрыть» либо по причине «недостатка защиты», либо от её «избытка», поскольку АЭС будут не конкурентоспособны.

Сегодня нужны системы и механизмы управления, связанные со стоимостью риска и экономическими выгодами от снижения риска. В этом новом для атомной энергетики направлении начинают работать отечественные и зарубежные специалисты. Например, IBM открыла в г. Ла-Год (Франция) Глобальный центр перспективных технологий атомной энергетики (Global Center of Excellence for Nuclear Power) для сотрудничества в области безопасности, надежности и эффективности производства электроэнергии. Консультативный совет по атомной энергетике IBM Nuclear Power Advisory Council (NPAC) обнародовал приоритетные направления и стратегические задачи атомной отрасли. В частности, члены Совета особо подчеркнули, что производители и поставщики, работающие в атомной энергетике, «должны найти более прозрачные способы управления различными типами рисков в целях создания благоприятных условий для роста отрасли».

К сожалению, проблема управления рисками АЭС в России не нашла прямого отражения в стратегии развития атомной энергетики. Хотя «Стратегия развития атомной энергетики России до 2030 года и на период до 2050 года» учтена в «Энергетической стратегии России на период до 2020 года», утверждённой Правительством РФ в ноябре 2009 г.

Стратегия развития российской атомной энергетики в первой половине XXI века (далее Стратегия) основывается на таких принципах, как воспроизводство ядерного топлива, естественная безопасность, конкурентоспособность. А для обеспечения конкурентоспособности как раз и необходима система управления рисками и её интеграция в систему корпоративного управления. Более того, Стратегией предусмотрено продление срока службы существующих блоков АЭС. Сегодня установленный расчетный срок службы действующих энергоблоков АЭС 30 лет. Планируется продление срока службы: энергоблоков первого поколения до 40 лет; энергоблоков второго поколения до 50 лет. В этих условиях, если не будет создана эффективная система управления операционным и технологическим рисками, то не миновать беды...

В предлагаемом учебном пособии рассматриваются задачи управления операционным и технологическим рисками на основе, так называемого «процессного подхода» и приведён пример практической реализации этого подхода к оптимизации длительности ремонтного цикла оборудования системы технического водоснабжения блока атомной станции (СТВ АЭС).

Мы отказались от написания традиционно краткого введения, так как введение в систему перспективных подходов управления рисками АЭС, существующих стандартов и норм безопасности, повышающих управляемость и стимулирующих реализацию приоритетов развития АЭС, – объёмная и не до конца осмысленная многими проблема, требующая терминологической и методологической увязки. В настоящем пособии «Введение: проблемы управления безопасностью и рисками АЭС» – полноценный учебный раздел, дающий целостное представление о современных проблемах управления безопасностью и рисками.

Таким образом, структура пособия представлена четырьмя учебными разделами, в которых излагаются теоретические и практические вопросы управления операционным риском (включая технологический как разновидность операционного риска), ставятся конкретные задачи и предлагаются детализированные процедуры их решения. В начале каждого раздела сформулирована цель занятия и перечислены знания, приобретаемые читателем в результате осмысления учебного материала. Это позволит изучать предмет, не читая всё подряд «от корки до корки», а подходить к этому процессу избирательно, руководствуясь уровнем собственных начальных знаний. Основные разделы учебного пособия содержат обсуждение изучаемой проблемы в форме ответов на вопросы, проясняющих сложные теоретические и практические моменты, а также тесты для самоконтроля.

Авторы полагают, что данное учебное пособие будет полезно не только студентам и аспирантам НИЯУ МИФИ, но и сотрудникам организаций, входящих в недавно созданный Научно-образовательный центр «Системы управления рисками АЭС» (НОЦ СУР АЭС).

*Б.В. Сазыкин*, д.т.н., профессор НИЯУ МИФИ

*А.Г. Краев*, к.т.н., с.н.с. АНО МЦЯБ

*В.П. Климов*, старший преподаватель НИЯУ МИФИ

## Раздел 1

---

---

### ВВЕДЕНИЕ: ПРОБЛЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ И РИСКАМИ АЭС

---

---

#### **Цель занятия:**

- дать краткое, но целостное представление о современных проблемах управления безопасностью и рисками АЭС и обратить внимание читателя на ряд нерешённых задач.

#### **Вы узнаете:**

- что следует понимать под управлением безопасностью и рисками, какими нормативными документами это закреплено, что такое пирамида стандартов МАГАТЭ;
- какие виды финансовых и нефинансовых рисков могут возникать в процессе эксплуатации АЭС;
- какие нерешённые методологические проблемы стоят перед российскими специалистами в области управления безопасностью и рисками АЭС.

#### **В программе занятия:**

- лекция, которая должна заинтересовать читателя и мотивировать его на дальнейшее изучение учебного материала;
- вопросы и ответы;
- тесты для самооценки.

## 1.1. Безопасность АЭС

Общее понятие безопасности содержится в законе РФ «О безопасности» [1] и определено как состояние защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Такая общая трактовка безопасности применительно к АЭС нуждается в уточнении.

Поскольку АЭС – это сложная система, содержащая ядерный реактор (реакторы), комплекс систем, устройств, оборудования и сооружений с необходимым персоналом, то и её безопасность следует трактовать как безопасность сложной системы (СС).

**Определение [2]:** *Безопасность АЭС – свойство СС при нормальной эксплуатации и нарушениях нормальной эксплуатации, включая аварии, ограничивать радиационное воздействие на персонал, население и окружающую среду установленными пределами.*

Из приведённого определения следует, что свойство безопасности АЭС связано с её состояниями. На рис. 1.1 приведена схема состояний АЭС.

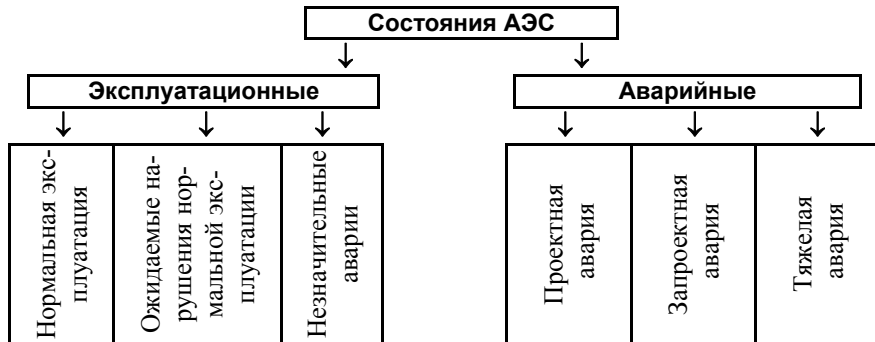


Рис. 1.1. Схема состояний АЭС

Ниже даны пояснения терминам, приведённым на рис. 1.1. Определения взяты из работ [2,3]. Приоритет отдаётся российским нормам [2], однако в тех случаях, когда эквивалентное определение в российских нормах отсутствует, даётся определение из международных норм и правил [3].



**Нормальная эксплуатация** [2] – эксплуатация АС в определенных проектом эксплуатационных пределах и условиях.

**Ожидаемые нарушения нормальной эксплуатации** (ожидаемое при эксплуатации событие) [3] – отклонение эксплуатационного процесса от нормальной эксплуатации, которое предположительно может произойти, как минимум, один раз в течение срока службы (жизненного цикла) установки, но которое благодаря соответствующим предусмотренным в проекте мерам не нанесёт значительного повреждения узлам, важным для безопасности, и не приведёт к аварийным условиям.

**Незначительные аварии** [3] – аварии, которые не квалифицируются определённо как проектные аварии, но охватываются последними.

**Проектная авария** [2] – авария, для которой проектом определены исходные события и конечные состояния и предусмотрены системы безопасности, обеспечивающие с учетом принципа единичного отказа систем безопасности или одной независимой от исходного события ошибки персонала ограничение ее последствий установленными для таких аварий пределами.

**Запроектная авария** [2] – авария, вызванная не учитываемыми для проектных аварий исходными событиями или сопровождающаяся дополнительными по сравнению с проектными авариями отказами систем безопасности сверх единичного отказа, реализацией ошибочных решений персонала.

**Тяжелая авария** [2] – запроектная авария с повреждением твэлов выше максимального проектного предела, при которой может быть достигнут предельно допустимый аварийный выброс радиоактивных веществ в окружающую среду.

### 1.1.1. Цели безопасности

*Общая цель ядерной безопасности* – защитить отдельных лиц, общество и окружающую среду от вредных последствий путём создания и поддержания на ядерных установках эффективных средств защиты от радиационной опасности.

*Цель защиты от радиационной опасности* – обеспечить, чтобы дозы облучения во всех эксплуатационных состояниях на установ-

ке или в результате любого запланированного выброса радиоактивных материалов с установки поддерживались ниже предписанных пределов и на разумно достижимом низком уровне, а также обеспечить смягчение радиологических последствий любых аварий.

*Принцип ALARA (As Low As Reasonably Achievable)* – предусматривает поддержание на возможно низком и достижимом уровне как индивидуальных (ниже пределов, установленных действующими нормами), так и коллективных доз облучения, с учетом социальных и экономических факторов. Принцип ALARA широко используется на АЭС и других радиационно-опасных объектах всего мира в качестве одного из важнейших принципов обеспечения радиационной безопасности при планировании, подготовке и выполнении радиационно-опасных работ.

*Техническая цель безопасности* – принять все практически осуществимые меры для предотвращения аварий на ядерных установках и смягчить их последствия, если они произойдут.

### **1.1.2. Классификация систем, элементов АЭС и классы безопасности**

Схема классификации систем и элементов АЭС приведена на рис. 1.2.

По влиянию элементов АС на безопасность устанавливаются четыре класса безопасности.

*К классу безопасности 1* относятся твэлы и элементы АЭС, отказы которых являются исходными событиями запроектных аварий, приводящими при проектном функционировании систем безопасности к повреждению твэлов с превышением установленных для проектных аварий пределов.

*К классу безопасности 2* относятся следующие элементы АЭС:

- элементы, отказы которых являются исходными событиями, приводящими к повреждению твэлов в пределах, установленных для проектных аварий, при проектном функционировании систем безопасности с учетом нормируемого для проектных аварий количества отказов в них;

- элементы систем безопасности, единичные отказы которых приводят к невыполнению соответствующими системами своих функций.

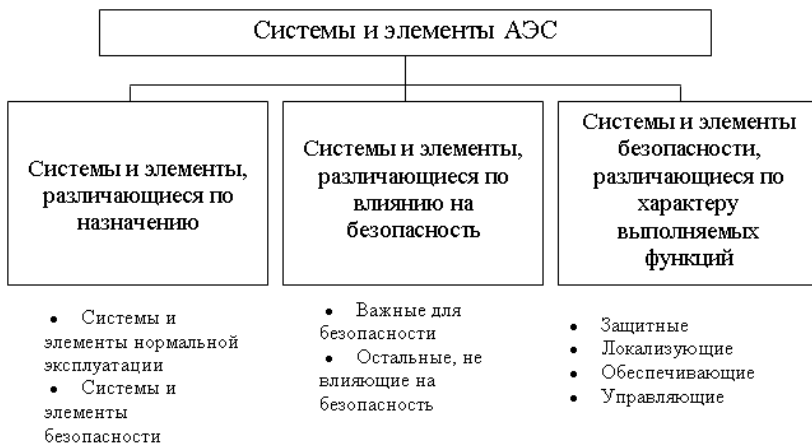


Рис. 1.2. Схема классификации систем и элементов АЭС

*К классу безопасности 3* относятся элементы АЭС:

- систем, важных для безопасности, не вошедшие в классы безопасности 1 и 2;

- содержащие радиоактивные вещества, выход которых в окружающую среду (включая производственные помещения АЭС) при отказах превышает значения, установленные в соответствии с нормами радиационной безопасности;

- выполняющие контрольные функции радиационной защиты персонала и населения.

*К классу безопасности 4* относятся элементы нормальной эксплуатации АС, не влияющие на безопасность и не вошедшие в классы безопасности 1, 2, 3.

### 1.1.3. Показатели состояний ядерной и радиационной безопасности АЭС

Проверки АЭС международными экспертами МАГАТЭ и Всемирной ассоциации организаций, эксплуатирующих АЭС (ВАО

АЭС) показали, что уровень безопасности российских АЭС соответствует международным требованиям [4].

Согласно [4] одним из основных показателей безопасности является «количество unplanned automatic reactor trips per 7000 hours of reactor operation». На рис. 1.3 показана динамика автоматических остановов реакторов из критического состояния для АЭС России и АЭС мира.

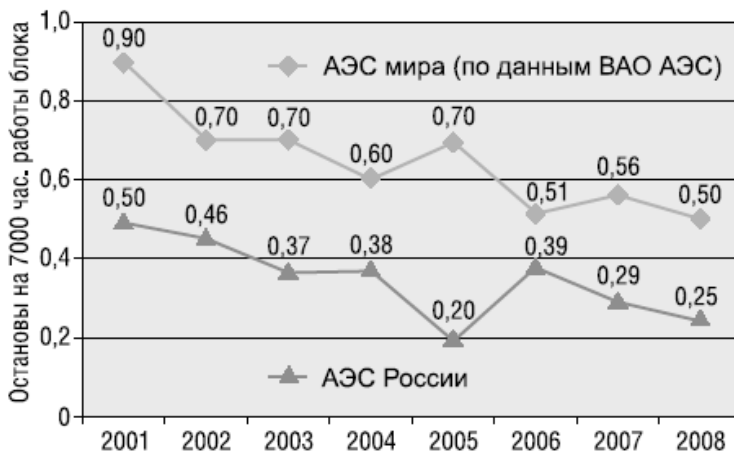


Рис. 1.3. Динамика автоматических остановов реакторов из критического состояния для АЭС России и АЭС мира [4]

Из приведённого рисунка видно, что в период 2001–2008 гг. уровень безопасности российских АЭС выше среднемирового. Например [4], в 2008 году на АЭС произошло 12 срабатываний различных систем безопасности, из них:

- автоматических срабатываний аварийной защиты (АЗ) из критического состояния – 8;
- срабатываний АЗ от ключа при работе энергоблока на мощности -3;
- срабатывание системы безопасности (СБ) вследствие внешнего воздействия – 1.

Другим важным показателем безопасности является вероятность облучения персонала («радиационный риск»). В соответствии с

международной практикой считается, что для персонала при техногенном облучении частота (вероятность) облучения должна находиться в диапазоне  $10^{-4} - 10^{-3}$  в год. На рис. 1.4 представлено распределение персонала Госкорпорации «Росатом» по «радиационному риску» и стажу [4].

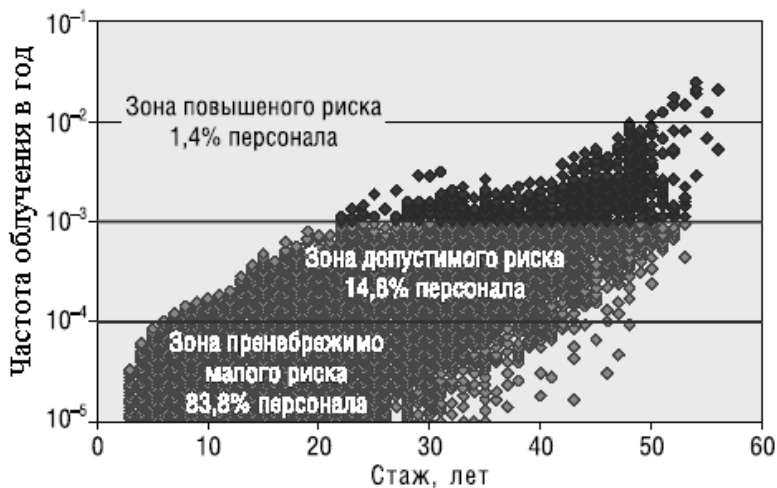


Рис. 1.4. Распределение персонала Госкорпорации «Росатом» по «радиационному риску» и стажу [4]

Из рис. 1.4 следует, что большинство работников (83 %) находятся в зоне пренебрежимо малого риска, 14,8 % персонала имеют приемлемый риск, у 755 человек (1,4 %) риск превышает приемлемый уровень (более  $10^{-3}$  в год).

Нормативно-технической документацией (НТД) по безопасности в атомной энергетике России определены и другие количественные критерии оценки степени безопасности АЭС. Например, это количественные значения тех технических показателей, которые нормируются, т.е. установлены определенные количественные требования (критерии). Эти значения не должны превышать (или быть меньше) некоторых установленных пределов. Выход же за нормируемые границы рассматривается как выход за пределы безопасности. Примерами таких ограничений могут быть: минимальное число дублирующих систем безопасности; максимальное

количество радиоактивных выбросов за сутки, месяц, год; вероятность крупных радиоактивных выбросов и вероятность разрушения активной зоны реактора в течение года, а также вероятность смерти человека вследствие аварии на АЭС. Расчет числовых значений указанных параметров проводится для каждого энергоблока отдельно на основе методов вероятностного анализа безопасности, рекомендованных МАГАТЭ.

Предельные значения таких интегральных критериев безопасности для одного реактора составляют:

- частота радиоактивных выбросов –  $1 \cdot 10^{-7}$ , 1/год;
- частота повреждения активной зоны –  $1 \cdot 10^{-5}$  1/год;
- индивидуальный риск для здоровья –  $1,65 \cdot 10^{-4}$  чел./бэр.

#### 1.1.4. Пирамида стандартов МАГАТЭ по безопасности

Пирамида стандартов МАГАТЭ представлена на рис. 1.5 [5].

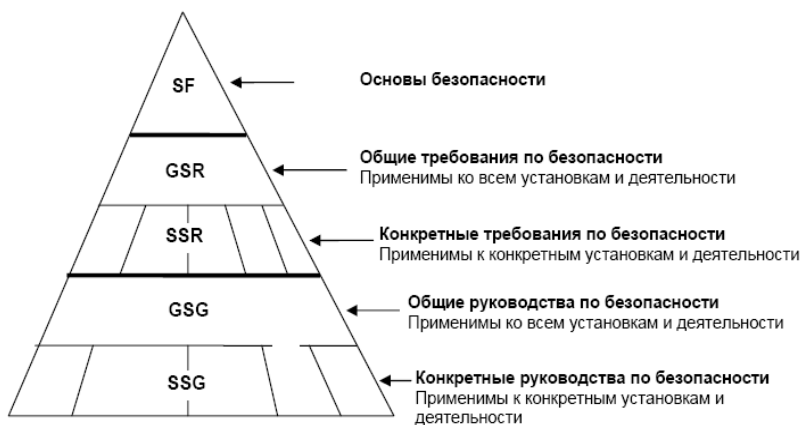


Рис. 1.5. Пирамида стандартов МАГАТЭ [4]

На вершине пирамиды находятся основы безопасности (SF – Safety Fundamentals) [5], устанавливающие цели и принципы безопасности. Далее следуют общие требования по безопасности (GSR – General Safety Requirements), которые применимы ко всем установкам и направлениям деятельности. На следующем этаже – кон-

кретные требования по безопасности (SSR – Specific Safety Requirements), применимые к конкретным установкам и деятельности. Следующий уровень пирамиды – общие руководства по безопасности (GSG – General Safety Guides), которые применимы ко всем установкам и деятельности. В основании пирамиды – конкретные руководства по безопасности (SSG – Specific Safety Guides).

## 1.2. Управление безопасностью АЭС

Управление безопасностью – это термин, используемый в отношении мер, необходимых для обеспечения того, чтобы приемлемый уровень безопасности поддерживался на протяжении всего жизненного цикла установки, включая снятие её с эксплуатации.

### 1.2.1. Общие принципы управления

Согласно [2] безопасность АЭС должна обеспечиваться за счет последовательной реализации концепции **глубоко эшелонированной защиты** (ГЭЗ). ГЭЗ основана на применении системы физических барьеров на пути распространения ионизирующего излучения и радиоактивных веществ в окружающую среду и системы технических и организационных мер по защите барьеров и сохранению их эффективности, а также по защите персонала, населения и окружающей среды.

**Система физических барьеров** блока АЭС включает топливную матрицу, оболочку твэла, границу контура теплоносителя реактора, герметичное ограждение реакторной установки и биологическую защиту.

**Система технических и организационных мер** должна образовывать пять уровней глубоко эшелонированной защиты, к которым относятся:

*Уровень 1. Условия размещения АЭС и предотвращение нарушений нормальной эксплуатации.*

*Уровень 2. Предотвращение проектных аварий системами нормальной эксплуатации.*

*Уровень 3. Предотвращение запроектных аварий системами безопасности.*

*Уровень 4. Управление запроектными авариями.*

*Уровень 5. Противоаварийное планирование.*

Концепция глубоко эшелонированной защиты применяется не только к барьерам и функциям безопасности, но и к человеческому фактору и организационным аспектам. Не существует какого-то одного способа группирования элементов (компонентов) ядерной безопасности. В европейской Организации экономического сотрудничества и развития (ОЭСР) они сгруппированы в три общие категории [6]:

1) технические (проект ядерной установки (ЯУ), техническое обслуживание; безопасность модернизаций; управление рисками и др.);

2) человеческие и организационные факторы (квалификация персонала; процедуры организационного и корпоративного управления; процедуры контроля работ, связанных с безопасностью);

3) программируемые факторы множественного влияния на элементы безопасности (условия для эксплуатации; защита от пожара; поверочные испытания; анализ опыта эксплуатации; обучение; управление старением оборудования; комплексные системы управления, включая обеспечение качества и самооценку; планы действий в случае чрезвычайных ситуаций).

### **1.2.2. Главный приоритет – обеспечение ядерной и радиационной безопасности**

Ядерная безопасность – это отсутствие физического ущерба, неоправданного риска и ущерба окружающей среде, вызванных эксплуатацией ядерных установок [6]. Термин «эксплуатация» подразумевает не только эксплуатацию установки, но и обращение с отработанным ядерным топливом и радиоактивными отходами, их захоронение, а также транспортировку радиоактивных материалов.

Компоненты ядерной безопасности подразделяются на те же три категории, принятые в ОЭСР, о которых говорилось выше.

Управление ядерной безопасностью обеспечивается мерами [6], предусмотренными для всех её компонент.



Для *технических компонент* должны быть предусмотрены:

- меры, обеспечивающие надежность проекта ядерной установки;
- организация высокопрофессиональной инженерной службы, проводящей техническое обслуживание установки;
- проведение оценки безопасности всех изменений и модернизаций;
- наличие программы радиологической защиты персонала;
- наличие программы использования информации о риске, полученной на основе системного анализа и опыта эксплуатации.

Для *человеческих и организационных факторов* должны быть предусмотрены:

- программа непрерывного обучения персонала;
- всеобъемлющий ряд процедур (инструкций и руководств) для эксплуатации установки, её технического обслуживания и управления аварией, включая руководство по управлению тяжелой аварией;
- организация корпоративного управления с таким руководством, которое устанавливает последовательность приоритетов с упором на приоритет ядерной безопасности;
- организация управления установкой, четко распределяющая полномочия и ответственность за безопасность;
- программа и процедуры, обеспечивающие контроль любых работ связанных с безопасностью.

Для *компонент с программируемыми факторами множественного влияния на элементы безопасности* должны быть предусмотрены:

- пределы и условия для эксплуатации, которые определяют и контролируют безопасный диапазон режимов эксплуатации ядерной установки;
- программы защиты от пожара и поверочные испытания;
- программа анализа опыта эксплуатации;
- программа управления старением оборудования;
- программа управления изменениями;
- создание комплексных систем управления (включая систему обеспечения качества, программы самооценки и корректирующих действий);

- планы действий в случае чрезвычайных ситуаций;
- программа по исследованиям ядерной безопасности, которая должна расширять базовые знания по основам безопасности;
- планы физической защиты установки, которые тестируются и обновляются с целью предотвращения угроз ядерной установке и предотвращения несанкционированного использования ядерных материалов.

Управление радиационной безопасностью достигается комплексным обеспечением мер безопасности, в первую очередь установленными нормами радиационной безопасности. Действующими и разрабатываемыми нормативно-техническими документами предусматривается следующее [7,8,9].

*Радиационная безопасность (РБ) на АЭС и вокруг неё обеспечивается за счет:*

- качества проекта АЭС;
- обоснованного выбора района и площадки для размещения АЭС;
- физической защиты источников излучения;
- зонирования территории вокруг АЭС и внутри них;
- условий эксплуатации технологических систем;
- санитарной оценки и лицензирования деятельности с источниками излучения;
- санитарной оценки изделий и технологий;
- наличия системы радиационного контроля;
- планирования и проведения мероприятий по обеспечению радиационной безопасности персонала и населения при нормальной работе АЭС, её реконструкции и выводе из эксплуатации;
- повышения качества вероятностного анализа безопасности (ВАБ) и оценки рисков.

*Радиационная безопасность персонала обеспечивается:*

- ограничениями допуска к работе по возрасту, полу, состоянию здоровья, уровню предыдущего облучения и другим показателям;
- знанием и соблюдением правил работы с источниками излучения;

- достаточностью защитных барьеров от источников излучения, а также ограничением времени работы с источниками излучения;
- созданием условий труда, отвечающих требованиям действующих норм и правил РБ;
  - применением индивидуальных средств защиты;
  - соблюдением установленных контрольных уровней;
  - организацией радиационного контроля;
  - организацией системы информации о радиационной обстановке;
  - проведением эффективных мероприятий по защите персонала при планировании повышенного облучения в случае угрозы и возникновения аварии.

*Радиационная безопасность населения обеспечивается:*

- созданием условий жизнедеятельности людей, отвечающих требованиям действующих норм и правил РБ;
- установлением квот на облучение от разных источников излучения;
  - организацией радиационного контроля;
  - эффективностью планирования и проведения мероприятий по радиационной защите в нормальных условиях и в случае радиационной аварии;
  - организацией системы информации о радиационной обстановке.

### **1.2.3. Схема управления безопасностью**

Общая схема управления безопасностью АЭС представлена на рис. 1.6. Определение целей, принципов, а также установление норм безопасности, контроль и обеспечение их выполнения лежит на *регулирующем органе*. Для атомного надзора России главным регулирующим органом является Ростехнадзор.

Непосредственные обязанности по управлению безопасностью АЭС осуществляет *эксплуатирующая организация*, которая имеет определённую структуру управления.



Рис. 1.6. Общая схема управления безопасностью АЭС

Эксплуатирующая организация должна:

- определять и осуществлять политику в области безопасности;
- иметь четкое разделение ответственности с установленными границами полномочий и линиями связи;
  - обеспечивать ресурсное управление (к ресурсам относятся: финансовые, материальные, информационные ресурсы; рабочие ресурсы, включающие операторов и автоматику);
  - обеспечивать достаточную укомплектованность персоналом с необходимым уровнем подготовки;
  - разрабатывать обоснованные регламенты и строго их придерживаться;
  - регулярно контролировать и проверять все относящиеся к безопасности вопросы жизненного цикла АЭС.

В России функции эксплуатирующей организации выполняет ОАО «Концерн Росэнергоатом», в состав которого входят АЭС.

Контроль и надзор являются важнейшими функциями управления безопасностью. Виды безопасности и структура регулирующих органов, способных выносить заключение о приемлемости уровня

безопасности на ядерных установках (ЯУ), приведены на рис. 1.7 [10].

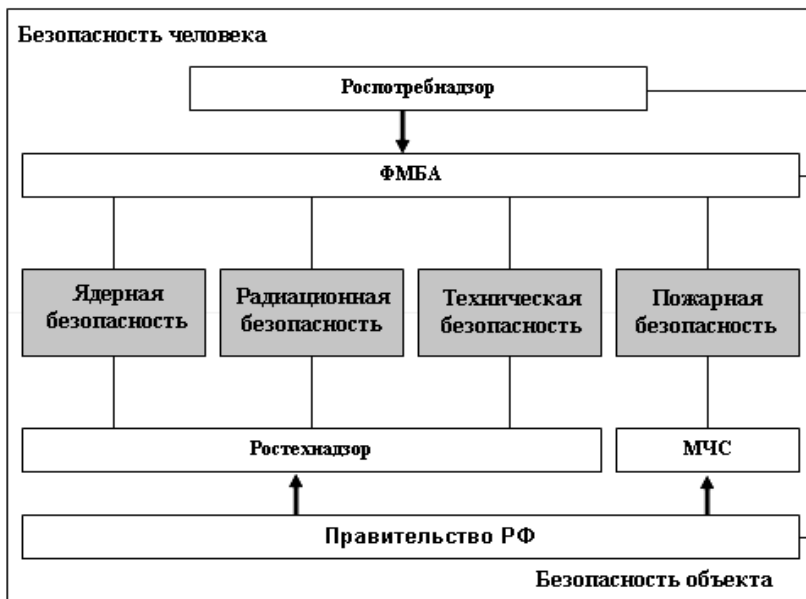


Рис. 1.7. Схема видов безопасности и структура регулирующих органов [10]: ФМБА – Федеральное медико-биологическое агентство; МЧС – Министерство РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, а также внесены поправки в связи с переподчинением Ростехнадзора Правительству РФ

#### 1.2.4. Проверка безопасности

Проверка безопасности ядерной установки на протяжении её жизненного цикла включает многие виды деятельности, в том числе:

- применение принципов обеспечения качества;
- независимую оценку безопасности;
- рассмотрение факторов, относящихся к площадке ядерной установки;
- рассмотрение результатов испытаний во время сооружения и ввода в эксплуатацию;

- непрерывный контроль и инспектирование установки в ходе эксплуатации, включая мониторинг окружающей среды;
- оценку потребности в модификациях и контроле в ходе их внедрения.

Таким образом, эксплуатирующая организация должна с помощью оценки, анализа, наблюдения, испытаний и инспектирования проверять, чтобы состояние установки и её эксплуатация соответствовали установленным нормам и требованиям безопасности.

### 1.2.5. Измерение безопасности

Одной из фундаментальных проблем, с которой сталкивается любой регулирующий орган (регулятор), является вопрос, как измерить элементы безопасности. Регуляторы, как правило, полагаются на комбинацию следующих факторов: свой предыдущий опыт, правильную инженерную оценку и понимание, основанное на информации о риске, для того, чтобы определить объективные свидетельства безопасности [6]. Эта информация затем сопоставляется и анализируется для измерения комплексного состояния безопасности установки. Связь между элементами, компонентами и объективными свидетельствами безопасности показана на рис. 1.8 [6].

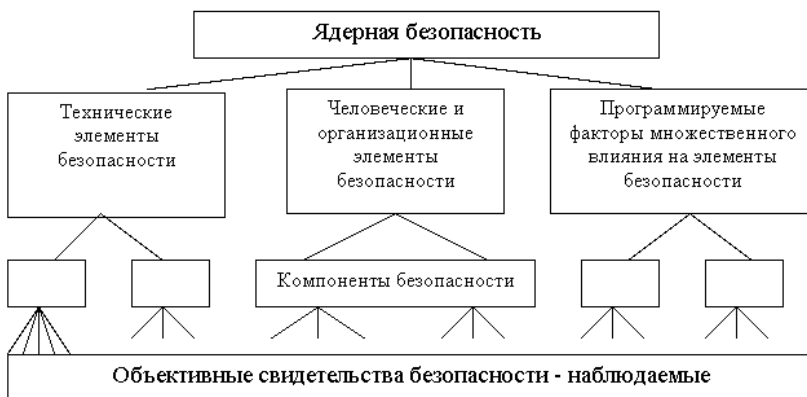


Рис. 1.8. Связь между элементами, компонентами и объективными свидетельствами безопасности

Некоторые регулирующие органы начали разрабатывать системные методы измерения, регистрации и анализа элементов безо-

пасности для того, чтобы обеспечить комплексную оценку достигнутого уровня безопасности. Например:

1) Система Швейцарской федеральной инспекции по ядерной безопасности (*HSK – Swiss Federal Nuclear Safety Inspectorate*). Дополнительную информацию можно получить на сайте [www.hsk.ch](http://www.hsk.ch)

2) Система Комиссии по ядерному регулированию США (*процесс реакторного надзора*). Дополнительную информацию можно получить на сайте: [www.nrc.gov](http://www.nrc.gov)

3) Система шведской инспекции по ядерной энергии (*SKI – Swedish Nuclear Power Inspectorate*). Дополнительную информацию можно получить на сайте [www.ski.se](http://www.ski.se)

4) Система канадской комиссии по ядерной безопасности (*CNSC – Canadian Nuclear Safety Commission*). Дополнительную информацию можно получить на [info@cnsccsn.gc.ca](mailto:info@cnsccsn.gc.ca)

5) Система Финского органа регулирования радиационной и ядерной безопасности (*STUK – Finnish Radiation and Nuclear safety Authority*). Дополнительную информацию можно получить на сайте [www.stuk.fi](http://www.stuk.fi)

### **1.3. Понятие риска и его место в обеспечении рентабельной безопасности АЭС**

Деятельность в ядерной области полагается безопасной, если возникающие из-за этого риски считаются приемлемыми [6]. Существует множество определений риска, но однозначной формулировки понятия «риск» нет. Более того, нет устоявшейся классификации рисков АЭС. Известно, что эффективность управления риском во многом определяется его классификацией. Под классификацией риска следует понимать распределение риска на конкретные группы по определенным признакам для достижения поставленных целей. Если цель – обеспечение безопасности, то мы столкнёмся с проблемами [11], связанными с критикой принятого в 2002 г. Федерального закона «О техническом регулировании». Если же цель – рентабельность АЭС в области производства электроэнергии при ограничениях на комплексную оценку достигнутого уровня безопасности, то мы придём к проблеме комплексной оценки риска, включающей финансовый и операционный (технологический) риски.

### 1.3.1. Понятие риска

*Риск* в широком смысле – неопределённость результата какой-либо деятельности, возможности его отклонения от ожидаемого или планируемого значения. То есть под риском понимают возможность наступления некоторого негативного события (опасности), влекущего за собой возникновение различного рода потерь.

Ситуацию риска можно охарактеризовать как разновидность «неопределенной ситуации», когда наступление событий вероятно и может быть определено, т.е. в этом случае объективно существует возможность оценить вероятность событий.

В ГОСТ Р 51901.1-2002 дано следующее определение риска.

**Риск** – сочетание вероятности события и его последствий (ущерб, вред и т.п.).

В данном случае вред – это физический ущерб или урон здоровью, имуществу или окружающей среде. Формально риск определяется соотношением:

Риск = (Вероятность негативного события; Ущерб).

**Оценка величины риска** – процесс присвоения значений вероятности и последствий риска. Последствия могут измеряться в натуральных показателях (количество разрушенных зданий, характеристики радиоактивного заражения территории, количество травм персонала и т.п.). Ущерб выражает последствия в стоимостных показателях, например, в рублях.

Универсальным показателем качества реализации технологических процессов и технических систем может служить степень риска.

*Замечание.* Техническая система – составной объект любого уровня сложности, который может включать персонал, процедуры, материалы, инструменты, оборудование, средства обслуживания, программное обеспечение.

**Степень риска** – это вероятность наступления случая потерь, а также размер возможного ущерба от него.

Под **негативными событиями** будем понимать любые события на АЭС, происходящие в штатном режиме (при нормальной эксплуатации), при нарушении нормальной эксплуатации, проектной, запроектной и тяжёлой (катастрофической) авариях.

Заслуживает внимания определение риска как деятельности экономического субъекта [12].



*Риск – это деятельность, рассчитанная на успех, при наличии неопределённости требующая от экономического субъекта умения и знания, как преодолеть негативные события. Это определение применимо только к бизнес-процессам АЭС.*

### 1.3.2. Показатели риска

По определению величина риска (или «степень риска») не может быть выражена только одним компонентом. В работе [13] указывается, что риск есть многокомпонентный вектор. Основные показатели (компоненты) определяются исходя из постановки решаемых задач [13]:

а) ущерб  $Y$  (потери, последствия) от негативного события измеряется стоимостными показателями, например, в рублях;

б) вероятность (частота)  $P$  реализации негативного события – безразмерная величина (частота, выражается в [1/год]);

в) ожидаемый ущерб для дискретных событий  $\bar{V} = \sum_i P_i V_i$ ; для непрерывной функции плотности вероятности  $p(Y)$

$$\bar{V} = \int p(Y) Y dY ;$$

г) затраты  $Z_1$  на уменьшение вероятности возникновения негативного события;

д) затраты  $Z_2$  на уменьшение последствий негативного события;

е) затраты  $Z_3$  на компенсацию ущерба;

ж) полные затраты на управление риском  $Z = Z_1 + Z_2 + Z_3$ ;

*Замечание.* Для определения величин  $Z_1, Z_2, Z_3$  необходимо знать распределение величины ущерба  $Y$  от вероятности (частоты) реализации негативных событий, а также нормативно установленные ограничения по минимальным вероятностям негативных событий (величины «хвостов распределений»);

з) предел страховой ответственности ущерба  $U_{\text{стр}}$  (ответственности предприятия без дотации государства).

### 1.3.3. Виды риска

В процессе эксплуатации АЭС могут возникать финансовые и нефинансовые риски. К **финансовым рискам**, например, относят-

ся рыночный риск, кредитный риск контрагента, риск процентной ставки, риск потери платежеспособности, риск ликвидности.

Источниками финансовых рисков могут быть:

- экономическая нестабильность в стране;
- инфляция;
- сложившаяся ситуация неплатежей в отрасли;
- дефицит бюджетных средств;
- политические факторы;
- колебания валютных курсов;
- государственное регулирование учетной банковской ставки;
- рост стоимости ресурсов на рынке капитала;
- повышение издержек производства и др.

Финансовые риски рассматриваться в данной работе не будут.

К **нефинансовым рискам** относятся:

- операционный риск;
- правовой риск;
- репутационный риск;
- стратегический риск;
- экологический риск.

**Операционный риск** [14] определяется как риск возникновения убытков (ущерба) в результате неадекватных или ошибочных внутренних процессов, связанных с людьми и системами, а также вследствие внешних воздействий. К внешним воздействиям, например, относятся природные катастрофы, пожары, террористические акции и др.

В технической литературе часто используется понятие технологического риска как разновидности операционного риска. **Технологический риск** связан с потенциально негативными последствиями, которые могут возникнуть в результате отказа в работе технических систем, сбоев в технологических процессах или ошибок со стороны обслуживающего персонала.

Различие в понятиях операционного и технологического рисков демонстрирует рис. 1.9. Из рисунка следует, что негативные события, относящиеся к операционному риску, находятся в вероятностном диапазоне от 1 до  $10^{-3}$  и включают события, относящиеся к технологическим и бизнес-процессам.

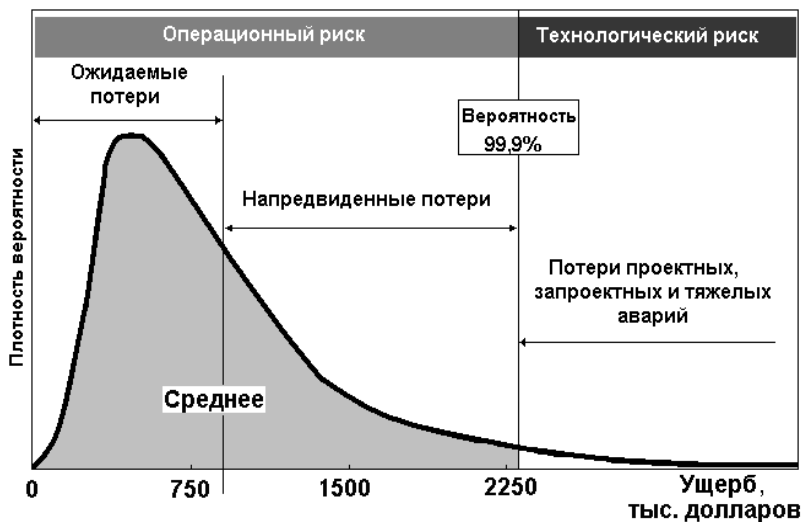


Рис. 1.9. Операционный и технологический риски

Граница операционного риска должна устанавливаться нормативно регулирующим органом. Технологический риск описывает ущерб от потенциальных или произошедших чрезвычайных событий (аварий). Такой подход позволяет поставить задачу управления рисками, как минимизацию операционного риска при жестких ограничениях технологического риска в рамках ядерной и радиационной безопасности.

Последствия операционного риска измеряются только стоимостными показателями и оцениваются ожидаемыми и непредвиденными потерями. Технологический риск может измеряться как в стоимостных показателях, так и в натуральных показателях (разрушенные здания, зараженные территории, смертность людей и т.п.). В технологический риск входят затраты на уменьшение чрезвычайного события (ЧС) и на компенсацию последствий ЧС.

Область оценки операционного и технологического рисков в матрице риска для АЭС показана на рис. 1.10.

Остальные виды рисков АЭС относятся к деятельности любой организации. Их реализация может оказать негативное влияние на её деятельность.

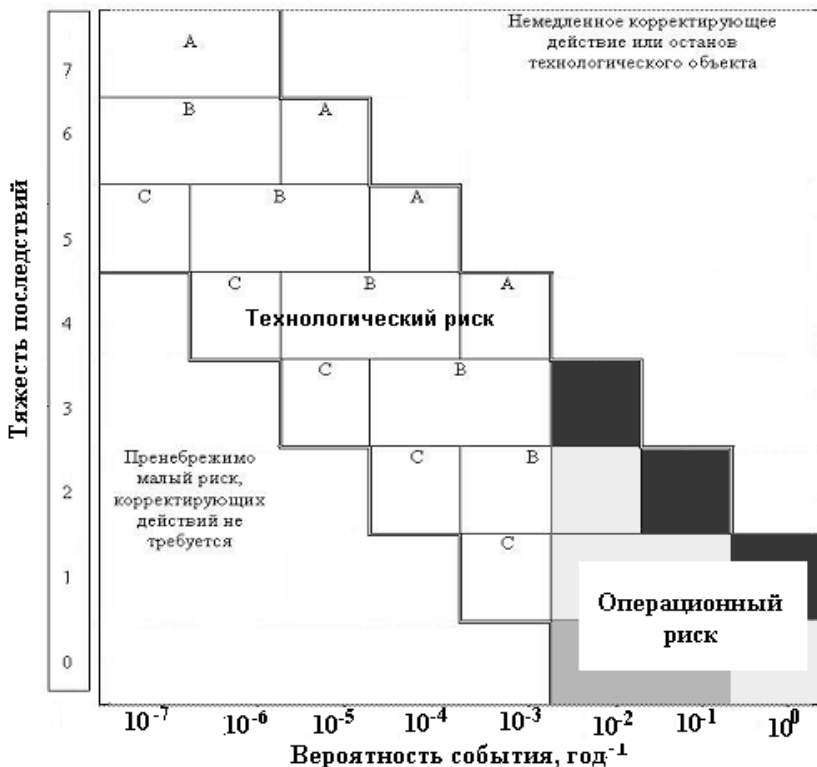


Рис. 1.10. Область оценки операционного и технологического рисков в матрице риска

**Правовой риск (ПР)** – риск возникновения у организации убытков обусловленных внутренними и внешними факторами. К внутренним факторам ПР относятся:

- несоблюдение организацией законодательства Российской Федерации;
- несоответствие внутренних документов организации законодательству Российской Федерации, а также неспособность организации своевременно приводить свою деятельность и внутренние документы в соответствие с изменениями законодательства;
- неэффективная организация правовой работы, приводящая к правовым ошибкам в деятельности организации вследствие действий служащих или органов управления организации;

- нарушение организацией условий договоров;
- недостаточная проработка организацией правовых вопросов при разработке и внедрении новых технологий и финансовых инноваций.

К внешним факторам ПР относятся:

- несовершенство правовой системы (отсутствие достаточного правового регулирования, противоречивость законодательства Российской Федерации, его подверженность изменениям, в том числе в части несовершенства методов государственного регулирования и (или) надзора, некорректное применение законодательства иностранного государства и(или) норм международного права), невозможность решения отдельных вопросов путем переговоров и как результат – обращение организации в судебные органы для их регулирования;

- нарушения контрагентами организации условий договоров.

**Риск потери деловой репутации организации (репутационный риск)** – риск возникновения у организации убытков вследствие формирования в обществе негативного представления об организации или характере её деятельности.

**Стратегический риск** – риск возникновения у организации убытков в результате ошибок (недостатков), допущенных при принятии решений, определяющих стратегию деятельности и развития организации (стратегическое управление), и выражающихся в неучете или недостаточном учете возможных опасностей, которые могут угрожать деятельности организации, неправильном или недостаточно обоснованном определении перспективных направлений деятельности, в которых организация может достичь преимущества перед конкурентами, отсутствии или обеспечении в неполном объеме необходимых ресурсов (финансовых, материально-технических, людских) и организационных мер (управленческих решений), которые должны обеспечить достижение стратегических целей деятельности организации.

**Экологические риски** возникают вследствие:

- изменения законодательства в части требований к окружающей среде;
- аварий;

- изменения отношения властей и общественности к результатам деятельности и самого процесса производства.

**Экологический риск** (по мнению специалистов компании экологического проектирования ШАНЕКО) «характеризуется как отклонение от общепризнанных принципов и норм отношений человека, хозяйствующих субъектов, общества и государства к окружающей природной среде, а также от норм социальных отношений возникающих между ними».

## 1.4. Управление рисками АЭС

Процесс управления риском охватывает различные аспекты работы с риском, от идентификации и анализа риска до оценки его допустимости и определения потенциальных возможностей снижения риска посредством выбора, реализации и контроля соответствующих управляющих действий [15].

### 1.4.1. Понятия управления риском

**Управление риском** [15] – действия, осуществляемые для выполнения решений в рамках менеджмента рисков.

**Менеджмент риска** [15] – скоординированные действия по руководству и управлению организацией в отношении рисков.

Управление риском включает: выявление (идентификацию) риска; мониторинг и оценивание риска; контроль риска и соответствие действий принятым решениям; минимизацию риска.

Соотношения между анализом риска и другими действиями по управлению риском показаны на рис. 1.11.

Управлять риском – значит предпринимать действия, направленные на поддержание такого его уровня, который соответствует целям управления в данный момент времени. Формально можно выделить две основных цели управления риском:

- поддержание риска на уровне не выше заданного;
- минимизация риска при некоторых заданных условиях, например, при заданном уровне прибыли и уровне безопасности (степени технологического риска).

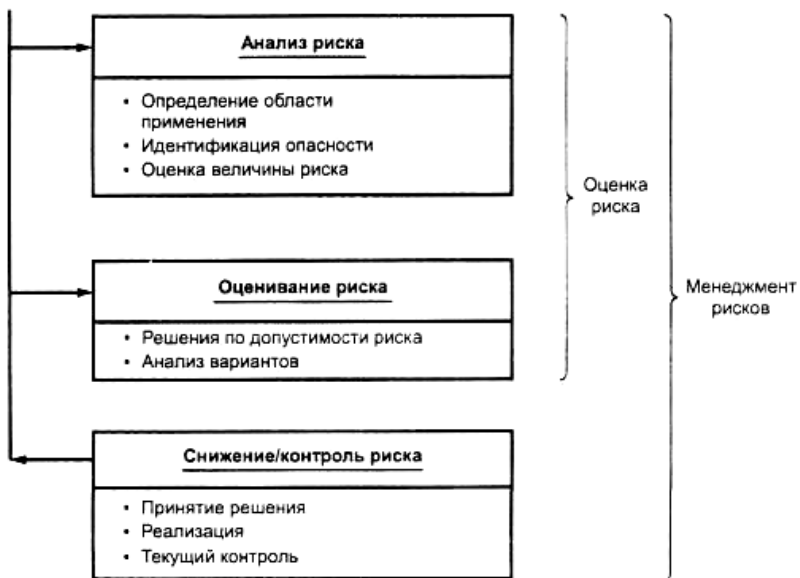


Рис. 1.11. Соотношения между анализом риска и другими действиями по управлению риском [15]

Эффективно управлять можно только тем, что можно измерить. Поэтому управление риском есть управление значениями его показателей.

Помимо управления отдельными рисками, существуют способы управления группами рисков и совокупным риском. Примером управления совокупным риском является управление величиной собственного капитала. Для эффективности управления совокупным риском необходимо его измерять в стоимостном выражении. Это достаточно просто делается для финансовых рисков, а, например, для операционного риска его стоимостное выражение может быть получено после стандартизованного описания процесса (технологических и бизнес-процессов) с последующим применением методов оценки риска и функционально-стоимостного анализа.

Важным моментом в постановке задачи управления рисками АЭС является:

- разработка общих технических регламентов (ОТР) управления операционным риском;

- разработка специальных технических регламентов (СТР) для управления технологическим риском.

#### **1.4.2. Концепция анализа риска для целей управления**

Концепция анализа риска для повышения эффективности управления риском подразумевает проведение предварительного анализа, включающего:

- идентификацию риска;
- сбор объективной информации для принятия решений;
- удовлетворение регламентированных требований к риску.

Затем результаты анализа риска могут использоваться лицом, принимающим решение (ЛПР) при оценке допустимости риска, а также при выборе между потенциальными мерами по снижению или устранению риска. С точки зрения ЛПР, к **задачам анализа риска** относятся:

- а) систематическая идентификация потенциальных опасностей;
- б) систематическая идентификация возможных видов отказов;
- в) количественные оценки или рейтингование рисков;
- г) оценка надежности возможных модификаций системы для снижения риска и достижения предпочтительных уровней ее надежности;
- д) выявление факторов, обуславливающих риск, и слабых звеньев в системе;
- е) более глубокое понимание устройства и функционирования системы;
- ж) сопоставление риска исследуемой системы с рисками альтернативных систем или технологий;
- и) идентификация и сопоставление рисков и неопределенностей;
- к) помощь в установлении приоритетов при совершенствовании санитарных требований и норм;
- л) формирование базы данных для рациональной организации профилактического обслуживания, ремонта и контроля;
- м) обеспечение возможности после аварийного расследования и мер по предупреждению аварий;
- н) возможность выбора мер и способов по обеспечению снижения риска.



Принятие решения ЛПР осуществляется посредством сопоставления результатов анализа риска с критериями допустимого риска. Во многих ситуациях возникает необходимость дополнительной оценки эффективности того или иного решения.

Одним из недостатков данного подхода является значительная неопределённость параметров управления. Это приводит к высокому росту темпа издержек АЭС[16], и, в конечном счете, может привести к неконкурентоспособности АЭС.

### 1.4.3. Концепция управления консолидированным риском

Управление консолидированным риском рассматривается как задача принятия решений с учётом рисков, возникающих во всех направлениях деятельности предприятия, и включающая как финансовые, так и нефинансовые риски.

Общая структурная схема управления предприятием (АЭС) представлена на рис. 1.12.

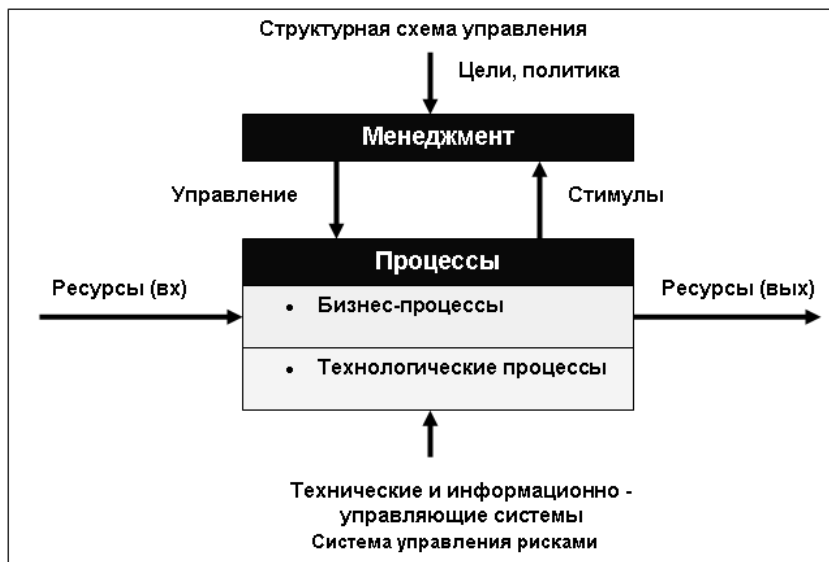


Рис. 1.12. Структурная схема управления предприятием

Менеджмент предприятия согласует ресурсы и цели. Для согласования ресурсов и целей и выработки управляющего воздействия необходимы стимулы. В консолидированном риск-ориентированном подходе в качестве стимулов для управления АЭС рассматриваются:

- ключевые показатели эффективности KPI (Key Performance Indicators);
- консолидированный риск и ключевые индикаторы риска KRI (Key Risk Indicators);
- ключевые показатели безопасности PI (Performance indicators);
- размер вознаграждения менеджмента, зависящий от показателя экономической добавленной стоимости с учётом риска [17].

Следует подчеркнуть, что, исходя из принципов культуры безопасности АЭС, проблемам безопасности уделяется главное внимание и для ключевых показателей безопасности PI устанавливается «высший приоритет». Согласно ОПБ-88/97 установлены целевые ориентиры в виде вероятности тяжелых запроектных аварий  $10^{-5}$  и вероятности предельного аварийного выброса радиоактивных веществ в окружающую среду, требующего эвакуации населения за пределы зоны планирования защитных мероприятий, равной  $10^{-7}$ . Таким образом, задачу управления АЭС можно рассматривать как оптимизационную задачу KPI и KRI при соблюдении жёстких ограничений по PI.

В условиях ограничений по PI целью управления рисками является поддержание принимаемого менеджментом совокупного (консолидированного) риска на уровне, определенном в соответствии с поставленными задачами. Такими задачами являются:

- выявление и анализ всех рисков, которые возникают на АЭС в процессе деятельности;
- количественная и качественная оценка (измерение) отдельных видов рисков;
- проведение полного анализа уровня рисков по всем технологическим и бизнес-процессам с целью определения суммарного размера рисков;
- оценка допустимости и обоснованности суммарного размера финансовых и нефинансовых рисков;

- создание подсистемы мониторинга и аудита рисков, а также подсистемы быстрого и адекватного реагирования, направленной на предотвращение или минимизацию риска.

Наглядной формой представления консолидированных оценок эффективности и риска является траектория развития организации/предприятия [18]. Пример такой траектории развития показан на рис. 1.13. На этом рисунке точками отмечены значения ежемесячных консолидированных оценок  $Z1(t) = F(KPI_t, KRI_t)$  и  $Z2(t) = G[(KPI_t - KPI_{t-1})/KPI_{t-1}, (KRI_t - KRI_{t-1})/KRI_{t-1}]$ , где функции  $F$  – некоторая непрерывная функция свёртки показателей эффективности и риска;  $G$  – некоторая непрерывная функция свёртки относительных изменений показателей эффективности и риска.

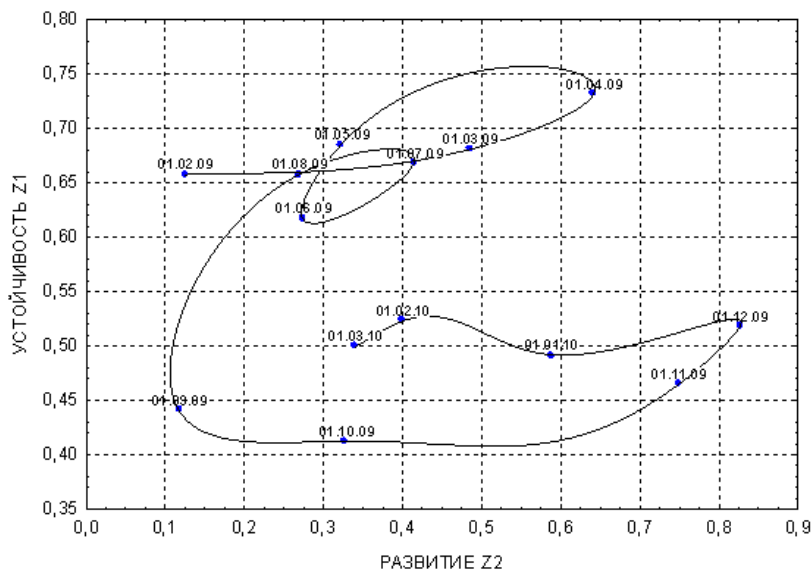


Рис. 1.13. Пример траектории развития

Исследования показали, что по характеру траекторий можно судить об успешности управления предприятием и об эффективности применяемых им стратегий управления. Применяя консолидированные оценки, например, можно добиться уменьшения вероятности потери предприятием экономической устойчивости. Эффект

достигается за счет ограничений величин рисков по координате «устойчивость»  $Z1$  и уменьшения амплитуды колебаний по координате «развитие»  $Z2$ . Но самое важное – это то, что *траектория развития показывает, насколько эффективными были мероприятия, направленные на совершенствование системы управления рисками*. По тому, как далеко траектория отодвинулась от точки с координатами (0,0) в направлении «идеальной» точки (1,1) можно судить об успешности проведенных технологических и бизнес-операций, качестве применённых технологических решений, эффективности управления операционным и технологическим рисками.

## **1.5. Требования к процессу анализа риска**

### **1.5.1. Этапы анализа**

Процесс анализа риска должен осуществляться в соответствии со следующими этапами:

- 1) определение области применения;
- 2) идентификация опасности и предварительная оценка последствий;
- 3) оценка величины риска;
- 4) проверка результатов анализа;
- 5) документальное обоснование;
- 6) корректировка результатов анализа с учетом последних данных.

Этапы процесса анализа показаны на рис. 1.14 [15].

### **1.5.2. Определение области применения анализа**

Определение области применения анализа риска должно включать в себя

- а) формулировку задач анализа риска;
- б) определение критериев отказа системы/процесса;
- в) описание исследуемой системы/процесса, включая обеспеченные ресурсами (энергетическими, материальными, финансовыми, людскими, информационными и др.);

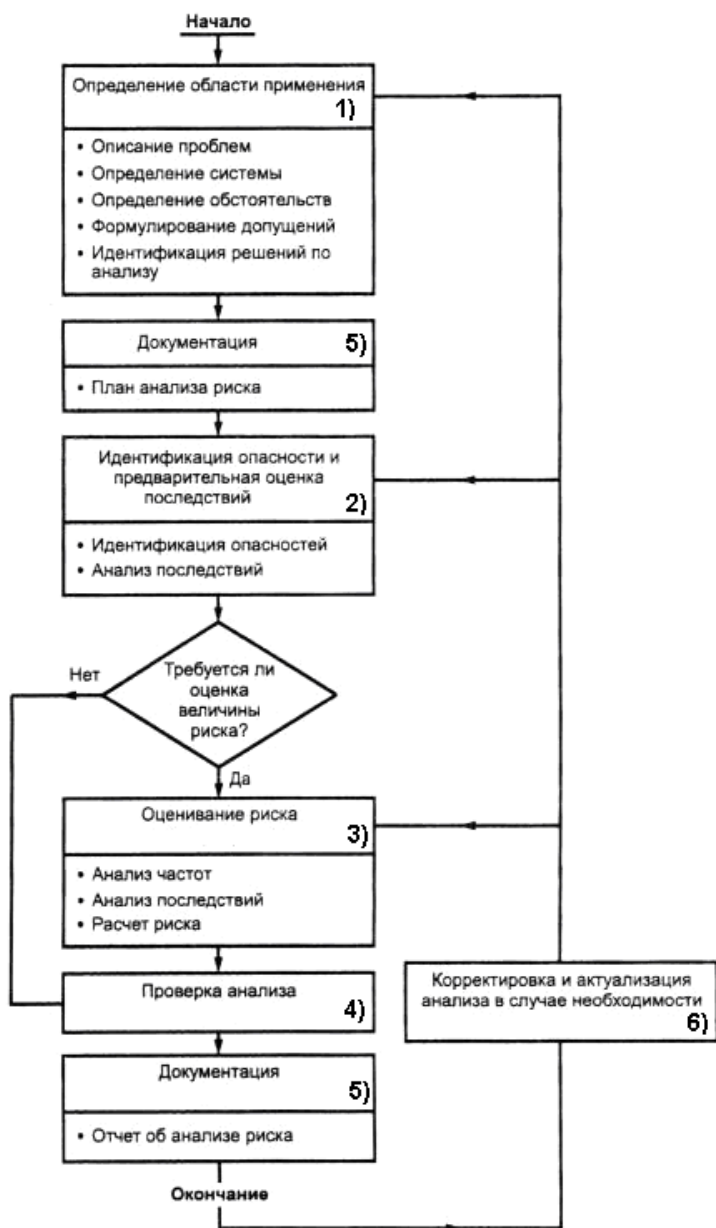


Рис. 1.14. Этапы процесса анализа риска [15]

г) установление источников риска, в частности, должны быть описаны любые обстоятельства, касающиеся ядерной и радиационной безопасности;

д) разработка формулировок решений, которые могут быть приняты.

### **1.5.3. Идентификация опасности и предварительная оценка последствий**

Для решения поставленной задачи должны быть идентифицированы опасности, являющиеся причиной риска, а также пути, по которым эти опасности могут реализовываться. Это – самый трудоёмкий этап с практически неустраняемыми элементами субъективизма.

Идентификация опасности предполагает систематическую проверку исследуемой системы/процесса с целью выявления типа присутствующих неустраняемых опасностей и способов их проявления. Полезными могут быть статистические записи аварий и опыт предшествующих анализов риска. Методы идентификации опасности включают следующие категории:

а) сопоставительные методы, примерами которых являются ведомости проверок, индексы опасностей и обзор данных эксплуатации;

б) методы идентификации опасностей путем постановки ряда вопросов типа «а что, если ... ?». Примерами такого типа методологии являются исследования опасности и связанных с ней проблем (HAZOP), а также анализ видов и последствий отказов (FMEA) [15];

в) методы индуктивного подхода, такие как логические диаграммы возможных последствий данного события (логические диаграммы «дерева событий», построение диаграмм функциональной целостности и логических критериев функционирования систем).

### **1.5.4. Оценка величины риска**

В процессе оценки величины риска для выбора критического уровня анализируемых рисков исследуются начальные события

или обстоятельства, последовательность потенциально опасных событий, любые смягчающие факторы и характеристики процессов деятельности, а также природа и частота возможных последствий идентифицированных опасностей. Показатели и меры риска (см. п. 1.3.2.) должны распространяться на риски для людей, имущества и окружающей среды и должны включать значения неопределенностей оценок.

**Анализ частот.** Анализ частот используется для оценки вероятности каждого негативного события, идентифицированного на стадии идентификации опасности. Для оценки частот происходящих событий обычно применяются следующие три подхода:

- использование имеющихся статистических данных (предыстория);
- получение частот происходящих событий на основе аналитических или имитационных методов;
- использование экспертных методов.

**Анализ последствий.** Анализ последствий используется для оценки вероятного воздействия, которое вызывается негативным событием (см. рис. 1.9). Анализ последствий должен:

- а) основываться на идентифицированных негативных событиях;
- б) описывать ущерб (последствия), являющиеся результатом негативных событий;
- в) учитывать существующие меры, направленные на смягчение последствий, наряду со всеми условиями безопасности, оказывающими влияние на последствия;
- г) устанавливать критерии, используемые для полной идентификации последствий;
- д) рассматривать и учитывать как немедленные последствия, так и те, которые могут проявиться по прошествии определенного периода времени, если это не противоречит поставленной задаче;
- е) рассматривать и учитывать вторичные последствия, распространяющиеся на смежное оборудование, системы и процессы.

**Анализ неопределенностей.** Анализ предусматривает определение изменений и неточностей в результатах моделирования, которые являются следствием отклонения параметров и предположений, применяемых при построении модели оценки риска. Обла-

стью, тесно связанной с анализом неопределенностей, является анализ чувствительности. Анализ чувствительности подразумевает определение изменений в реакции модели оценки риска на отклонения отдельных параметров модели.

Оценка неопределенности состоит из преобразования неопределенности критических параметров модели в неопределенность результатов в соответствии с моделью риска. Требования к полноте и точности оценки риска должны быть сформулированы настолько полно, насколько это возможно. Там, где это возможно, должны быть выявлены источники неопределенности. Это относится как к неопределенностям данных, так и к неопределенностям модели. Должны быть определены те параметры, к которым чувствителен анализ [15].

### **1.5.5. Проверка анализа**

Проверка анализа должна осуществляться людьми, не привлеченными к участию в анализе [15]. Проверка включает в себя следующие этапы:

- а) проверка соответствия области применения поставленным задачам;
- б) проверка всех важных допущений для обеспечения уверенности в том, что они являются правдоподобными в условиях имеющейся информации;
- в) подтверждение аналитиком правильности использованных методов, моделей и данных;
- г) проверка результатов анализа на устойчивость по отношению к различным форматам данных.

### **1.5.6. Документация и корректировка результатов анализа**

Отчет об анализе риска документально обосновывает процесс анализа риска. В отчете, должна быть отражена следующая информация:

- а) краткое изложение анализа;
- б) выводы;



- в) цели и область применения анализа;
- г) ограничения, допущения и обоснование предложений;
- д) описание соответствующих частей системы;
- е) методология анализа;
- ж) результаты идентификации опасностей;
- и) используемые модели, в том числе допущения и их обоснования;
- к) использованные данные и их источники;
- л) результаты оценки величины риска;
- м) анализ чувствительности и неопределенности;
- н) рассмотрение и обсуждение результатов (включая рассмотрение и обсуждение трудностей исследования);
- о) ссылки и рекомендации.

Если анализ риска используется для обеспечения непрерывного процесса управления риском, его необходимо выполнять и документировать таким образом, чтобы он мог корректироваться на протяжении всего жизненного цикла системы, оборудования или процессов деятельности. Анализ должен обновляться по мере поступления новой информации и в соответствии с потребностями процесса управления [15].

## Вопросы и ответы

**Вопрос.** Из приведённого определения безопасности следует, что безопасность это свойство системы. С другой стороны говорится о связи «свойства» и «состояния». Так всё же, безопасность это «свойство» или «состояние»?

**Ответ.** Следует различать безопасность человека (персонала, населения) и технического объекта (АЭС) [10]. Безопасность как *состояние* защищённости человека определено законами «О радиационной безопасности населения» №3-ФЗ от 9.01.1996 и «О санитарно – эпидемиологическом благополучии» №52 от 12.03.1999. Вместе с этим, безопасность промышленного объекта (как «*свойство*») нормируется законами «О пожарной безопасности» №63-ФЗ от 21.12.1994 и «О промышленной безопасности опасных производственных объектов» №116-ФЗ от 21.07.1997. Из этого следует

важный вывод: регулирование безопасности человека и объекта должно осуществляться разными органами по разным нормам и процедурам [10].

**Вопрос.** Понятно, что «безопасность» как-то связана с «риском». Но как? Как целевые показатели безопасности АЭС связаны с риском?

**Ответ.** Первая часть вопроса поставлена некорректно. Правильнее было бы говорить о количественных показателях, характеризующим безопасность и их соотношении с количественными показателями риска. А вот на вторую часть вопроса можно ответить. Но сначала я напомним тезис: «деятельность в ядерной области полагается безопасной, если возникающие из-за этого риски считаются приемлемыми».

Давайте рассмотрим следующий «простой» пример.

Пусть задан целевой показатель безопасности, например, частота «приемлемого» тяжёлого повреждения активной зоны (АЗ) реактора  $\lambda = 10^{-5}$  (1/реактор · год).

Риск  $R$  тяжёлого повреждения АЗ определён соотношением:

$$R = (P(Y); Y),$$

где  $Y$  – ущерб;  $P(Y)$  – вероятность ущерба  $Y$ .

Предположим, что известно распределение ущерба (например, убытки в млн. руб.) предписывающее каждому значению убытка  $Y$  соответствующую вероятность. Тогда  $P(Y) \leq \alpha(\lambda)$ , где  $\alpha$  – заданная вероятность, зависящая от  $\lambda$ , позволяющая считать убыток «приемлемым». Для грубой оценки можно положить  $\alpha(\lambda) = \lambda = 10^{-5}$ .

Из «кривой» распределения  $P(Y)$  с учётом  $P(Y) = 10^{-5}$  можно найти соответствующий убыток  $Y$ . Но сложность здесь в том, что трудно построить «кривую», описывающую комбинации вероятности и величины убытка. События ведь редкие ( $P = \sim 10^{-5}$ )! Поэтому в данном примере «обоснованный результат» может быть получен только методом математического моделирования (например, методом сценарного анализа) с использованием программных средств вероятностного анализа безопасности (ВАБ), позволяющих рассчитать «виртуальную» априорную вероятность ущерба. А это сделать не просто. Именно поэтому в слове «простой» поставлены кавычки.

**Вопрос.** Риск определяется как сочетание вероятности события и его ущерба. Что является мерой риска? Разве нельзя просто сказать, что риск – это произведение вероятности и ущерба?

**Ответ.** Ну, почему же нельзя? Сказать можно. Раньше так и делали. Условно говоря, есть два общих подхода к измерению риска: традиционный и современный. Традиционный подход заключается в том, что он описывает ущерб (убытки), как – будто они имеют один возможный исход, равный произведению вероятности события на его ущерб. На самом же деле убытки могут иметь распределение, предписывающее каждому значению исхода соответствующую вероятность (рис. 1.15).

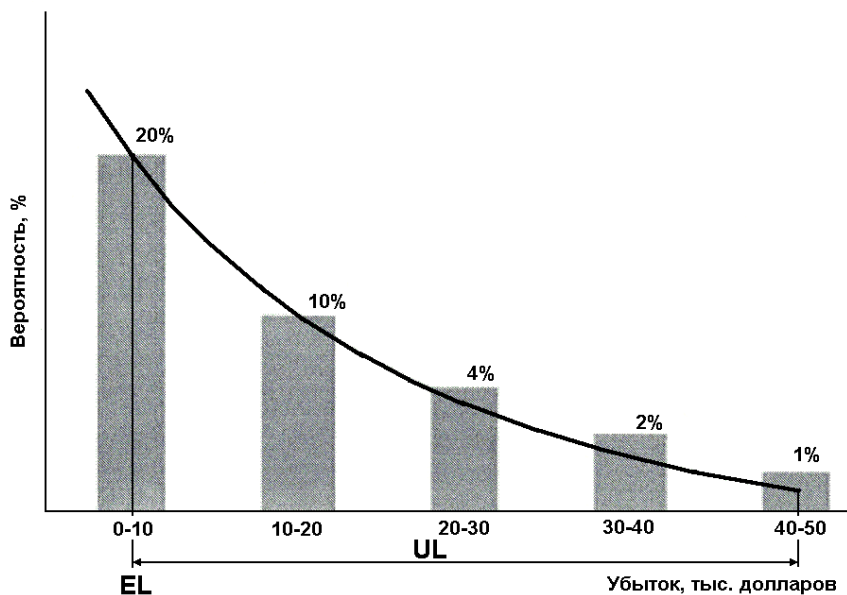


Рис. 1.15. Кривая, описывающая комбинации вероятности и величины убытка, построенная на исходных данных [19]

Традиционный подход фактически использует единственную среднюю точку этой кривой (ожидаемые потери EL см. рис. 1.15):

$$\begin{aligned}
 EL &= 5 \cdot 0,2 + 15 \cdot 0,1 + 25 \cdot 0,04 + 35 \cdot 0,02 + 45 \cdot 0,01 = \\
 &= 4,65 \text{ тыс. долларов.}
 \end{aligned}$$

При современном подходе исторические данные по ущербу используются для нахождения не только ожидаемых потерь EL, но и непредвиденных потерь UL:

$$UL = 45 - 4, 65 = 40, 35 \text{ тыс. долларов.}$$

Таким образом, в данном примере величины EL и UL являются мерой риска. По ежегодным изменениям величин EL и UL можно судить о том, насколько эффективными были процедуры управления риском.

Кроме «контрольных» функций, следует отметить следующую «практичность» современного подхода. На практике для определённого класса технологических процессов (на протяжении периода времени, например одного года) формируют резервы на внеплановые ремонты, равные EL, и резервы капитала, равные UL, под непредвиденные потери. То есть формируется база для планирования технического обслуживания и ремонта оборудования АЭС. В этом – суть практической значимости современного подхода оценки риска.

**Вопрос.** Я думаю, что на практике сложно использовать многокомпонентные оценки риска. Нужна какая-то более простая оценка. Существует ли такая единая, общепринятая мера возможных потерь?

**Ответ.** Да, существует. Эта общепринятая мера называется «показателем рискованности» (**value at risk -VaR**) [17], которая равна квантилю распределения убытка для необходимого уровня доверия.

Другими словами, величина VaR – это размер убытка  $x$ , который не будет превышен с вероятностью  $(100 - \alpha) \%$  в течение временного периода  $T$ . На практике для бизнес-процессов вероятность потерь  $\alpha$  устанавливается на уровне 1, 2,5 и 5 %. Тогда соответствующие доверительные интервалы  $(100 - \alpha) \%$  составляют 99, 97,5 и 95 %. Для оценки операционных потерь период  $T$  устанавливают равным 1 году. Тогда

$$Pr (VaR \leq x) = 1 - \alpha,$$

где  $Pr$  – обозначение вероятности.

Таким образом, показатель VaR – это выраженная в денежных единицах оценка величины, которую не превысят потери  $x$  в течение периода  $T$  с заданной вероятностью  $(1 - \alpha)$ .

**Вопрос.** Вы говорили об управлении АЭС по ключевым показателям эффективности KPI и риска KRI. Какие KPI и KRI следует выбирать? И вообще, как это делается? Приведите пример KPI и KRI.

**Ответ.** Выбор ключевых показателей KPI и KRI определяется целями управления АЭС, и эти показатели могут изменяться в течение жизненного цикла станции. Консультанты по риск-менеджменту рекомендуют осуществлять процедуру выбора в три этапа: формирование первоначального, «широкого» списка показателей; выбор критерия статистической проверки неоднородности данных (такого, например, как критерий Колмогорова – Смирнова); выбор *значимых* и технологически реализуемых показателей из первоначального списка.

Пример возможных ключевых показателей эффективности KPI:

$x_1 = K/(A - A_{p0})$  – показатель достаточности собственных средств (капитала);  $K$  – собственные средства (капитал);  $A$  – активы;  $A_{p0}$  – безрисковые активы;

$x_2 = \Pi/A_{cp}$  – показатель рентабельности активов;  $\Pi$  – прибыль до налогообложения;  $A_{cp}$  – средняя величина активов за период  $T$  (1 год);

$x_3 = \Pi/K_{cp}$  – показатель рентабельности капитала;  $K_{cp}$  – средняя величина капитала за период  $T$  (1 год);

$x_4 = P_y/(\Pi + P_y)$  – показатель структуры расходов;  $P_y$  – административно-управленческие расходы;

$x_5 = \text{КИУМ} = \sum_i^n P_i T_i / (PT)$  – коэффициент использования установленной мощности (КИУМ) энергоблока;  $T_i$  – время работы на  $i$ -м уровне стационарной мощности  $P_i$ ;  $T$  – полное время работы энергоблока (1 год);  $P$  – номинальная проектная мощность энергоблока;

$x_6 = Z_k / \Pi$  – коэффициент затрат на качество;  $Z_k$  – затраты на качество по всем видам деятельности АЭС.

Пример возможных ключевых показателей риска KRI:

$x_7 = \sum_j^m Y_j / P$  – индикатор уровня убытков;  $Y_j$  – фактические убытки от реализации  $j$ -го риска за период  $T$ ;  $P$  – суммарные расходы за период;

$x_8 = \sum_j^m EL_j / P$  – индикатор уровня ожидаемых потерь;  $EL_j$  – величина ожидаемых убытков (потерь) от реализации  $j$ -го риска за период  $T$ ;

$x_9 = \sum_j^m UL_j / K_{\text{ср}}$  – индикатор уровня непредвиденных потерь;  $UL_j$  – величина непредвиденных убытков (потерь) от реализации  $j$ -го риска за период  $T$ ;  $K_{\text{ср}}$  – средняя величина капитала за период  $T$ ;

$x_{10} = k_{\text{нг}}$  – коэффициент неготовности энергоблока, равный доле электроэнергии (которая не была выработана вследствие unplanned остановов) от максимального количества энергии, которое могло быть выработано за период  $T$ ;

$x_{11} = N_{\text{ср}} / 7000$  – показатель unplanned автоматических аварийных остановов реактора в критическом состоянии;  $N_{\text{ср}}$  – среднее количество срабатываний аварийной защиты отнесённое к 7000 часам (приблизительно 1 год) работы энергоблока в критическом состоянии;

$x_{12} = T_{\text{рв}} / 200000$  – показатель потерь рабочего времени в результате несчастных случаев, произошедших на АЭС, отнесённых к 200000 человеко-часам.

**Вопрос.** Перед предприятием поставлена задача обеспечения определённого уровня устойчивости, который необходимо поддерживать. Можно ли без применения уникальных методик, «на коленке» решить такую задачу? И вообще, как в этом случае оценить риск потери устойчивости?

**Ответ.** «На коленке», т.е. простыми «инженерными» методами можно решить сложную задачу, если перед этим была проведена серьёзная аналитическая работа. Теперь, что касается риска. В широком смысле риск – это возможность не достичь поставленной цели. В данном случае целью является обеспечение уровня устойчивости, ниже которого нельзя «провалиться» предприятию. Для решения такой задачи можно воспользоваться траекторией развития (см. рис. 1.13), задав значения уровней устойчивости  $Z1$  и развития  $Z2$  на предшествующем историческом периоде.

Для простоты восприятия упростим задачу и ограничимся лишь одной координатой  $Z1$  и «укороченным» рядом исторических данных. Пусть  $Z1$  определяется средневзвешенными значениями КРІ и КRІ (отнормированными и приведенными к месячному интервалу):

$$Z1 = \sum_k^K w_k X_k,$$

где  $X_k = (x_{k\max} - x_k)/(x_{k\max} - x_{k\min})$ ;  $\sum_k^{12} w_k = 1$ ;  $x_{k\max}$  – максимальное значение  $x_k$ ;  $x_{k\min}$  – минимальное значение  $x_k$ ;  $k = 1, \dots, K$  – количество показателей.

Значения показателя устойчивости  $Z1$  представлены в табл. 1.1.

Таблица 1.1

Дата	1 янв.	1 фев.	1 марта	1 апр.	1 мая	1 июня	1 июля	1 авг.	1 сен.	1 окт.	1 ноя.	1 дек.
<b>Z1, отн. ед.</b>	0,86	0,82	0,90	0,91	0,85	0,87	0,85	0,84	0,85	0,86	0,87	0,82

Воспользуемся методологией VaR [17] для оценки риска и методом исторического моделирования. Сначала ранжируем значения  $Z1$  в порядке убывания (табл. 1.2).

Таблица 1.2

№	1	2	3	4	5	6	7	8	9	10	11	12
<b>Z1, отн. ед.</b>	0,91	0,90	0,87	0,87	0,86	<b>0,86</b>	0,85	0,85	0,85	0,84	<b>0,82</b>	0,82

Затем установим уровень доверительной вероятности  $(1-\alpha) = 90\%$ ,  $(\alpha = 10\%)$  и рассчитаем VaR по следующей формуле:

$$\text{Var} = Z1_{P/2} - Z1_{P(1-\alpha/2)}.$$

В нашем случае  $P = 12$ ;  $P/2 = 6$ ;  $P(1 - \alpha/2) = 11$  и  $\text{VaR} = 0,86 - 0,82 = 0,04$  – есть мера риска.

Вывод: с доверительной вероятностью 90 % предельный уровень устойчивости предприятия не упадет ниже значения 0,82 в 6 случаях из 12 возможных (т.е. 6 месяцев в год предприятие не «провалится» ниже уровня 0,82).

**Вопрос.** Вы упомянули, что одним из стимулов управления является вознаграждение менеджеров, зависящее от экономической добавленной стоимости с учётом риска. Как это понимать? Как конкретно вознаграждение руководителя связано с риском?

**Ответ.** Начну с формального определения экономической добавленной стоимости. Это понятие нам в дальнейшем понадобится. В методологии корпоративного управления, разработанной американской компанией Stern Stewart & Co, предлагается строить систему стимулирования руководящего персонала на основе показателя **экономической добавленной стоимости** EVA (Economic Value Added) с учётом риска:

$$EVA = E - COE \cdot C,$$

где  $E$  – чистая прибыль после уплаты налогов и процентов;  $COE$  – доходность на акционерный капитал;  $C$  – капитал, который связан с основными рисками через соотношение уровня достаточности капитала.

Одним из возможных вариантов оценки  $C$  является линейная комбинация показателей регулятивного рискового капитала:

$$C = RC = CRC + MRC + ORC,$$

где  $RC$  (risk capital) – капитал, резервируемый под консолидированный (совокупный) риск;  $CRC$  (credit risk capital) – кредитный рисковый капитал равный непредвиденным потерям вследствие реализации кредитного риска;  $MRC$  (market risk capital) – непредвиденные потери вследствие рыночного риска;  $ORC$  (operational risk capital) – непредвиденные потери вследствие операционного (технологического) риска.

В указанной системе стимулирования размер вознаграждения руководителя  $S$  складывается из определённого процента EVA и некоторой функции нефинансовых показателей:

$$S = k \cdot EVA + f(x_1, \dots, x_n),$$

где  $k$  – фиксированный процент (например, 1 %);  $x_1, \dots, x_n$  – нефинансовые показатели, соответствующие критериям «лидерство», «отношения с субъектами управления» и т.п.

Таким образом, размер вознаграждения зависит от экономической эффективности деятельности  $E$  и оценки консолидированного риска  $RC$ . Обратите внимание, что величина  $RC$  зависит от непред-



виденных потерь вследствие операционного риска (ORC). Эти потери на АЭС обусловлены уровнем технологического развития, связаны с культурой безопасности АЭС и квалификацией персонала, в значительной степени определяются величиной инвестиций в техническое обслуживание и ремонты оборудования АЭС (ТОиР). Следовательно, руководители АЭС (в случае применения риск-ориентированного подхода к управлению) напрямую заинтересованы в технологическом развитии и поддержании высокого уровня показателей безопасности.

### Тесты для самоконтроля

1. Какие состояния АЭС, согласно нормам МАГАТЭ, относятся к эксплуатационным состояниям?

- Нормальная эксплуатация.
- Ожидаемые нарушения нормальной эксплуатации.
- Незначительная авария.
- Проектная авария.

2. Какие состояния АЭС, согласно нормам МАГАТЭ, относятся к аварийным состояниям?

- Незначительная авария.
- Проектная авария.
- Запроектная авария.
- Тяжелая авария.

3. Какова *общая цель* ядерной безопасности (согласно международным нормам)?

- Принятие мер для предотвращения аварий на ядерных установках.
- Защитить отдельных лиц от радиационной опасности.
- Защитить общество и окружающую среду от радиационной опасности.

4. Какова *техническая цель* безопасности АЭС?

- Обеспечить смягчение радиологических последствий аварий.
- Принять все возможные меры для предотвращения аварий на ядерных установках.

- Смягчить последствия аварий на ядерных установках, если аварии произойдут.

5. Какая организация (орган) в России непосредственно отвечает за управление безопасностью АЭС?

- Регулирующий орган (Ростехнадзор).
- Эксплуатирующая организация (Росэнергоатом).

6. Что такое риск?

- Неопределённость результата какой-либо деятельности.
- Сочетание вероятности события и его последствий.
- Произведение вероятности негативного события на ущерб от него.

7. Какие риски относятся к финансовым рискам?

- Рыночный риск.
- Кредитный риск.
- Риск процентной ставки.
- Стратегический риск.
- Риск потери платёжеспособности.

8. Какие риски относятся к нефинансовым рискам?

- Правовой риск.
- Операционный риск.
- Экологический риск.
- Риск ликвидности.

9. Технологический риск – это разновидность операционного риска?

- Да.
- Нет.

10. Какие действия относятся к управлению рисками АЭС?

- Анализ, оценивание, снижение/контроль риска.
- Разработка общих и специальных технических регламентов.
- Аутсорсинг и страхование.

## Раздел 2

---

---

### УПРАВЛЕНИЕ ОПЕРАЦИОННЫМ РИСКОМ: ПРОЦЕССНЫЙ ПОДХОД

---

---

#### **Цель занятия:**

- дать целостное представление о процессном подходе к управлению операционным риском, его структуре, основных задачах, которые должны решаться, как в краткосрочном, так и долгосрочном периоде жизнедеятельности не только АЭС, но любого предприятия атомной отрасли.

#### **Вы научитесь:**

- на основе полученных сведений формировать цели и задачи процессного управления;
- в соответствии со схемой декомпозиции задачи управления операционным риском находить её эффективное решение;
- применять процессный подход к выявлению, оценке, мониторингу и контролю операционного риска.

#### **В программе занятия:**

- лекция, в которой даются основные понятия и определения, разбирается этапы процессного управления операционным риском;
- вопросы и ответы;
- тесты для самоконтроля.

## 2.1. Основные понятия и определения

Процессный подход (Process Approach) к управлению деятельностью предприятий и организаций используется по всему миру и доказал свою эффективность, несмотря на то, что является относительно новым. В основе подхода лежат международные стандарты ИСО 9001 (2000 г.) ИСО/МЭК 15504 (1998 г.), ИСО/МЭК 12207 (1995 г.) и др.

Основной принцип процессного подхода: желаемый результат достигается более эффективно, когда связанные ресурсы и деятельность предприятия управляются как процесс. То есть процессный подход к управлению исходит из того, что любая деятельность трактуется как технологический процесс. Следуя устоявшейся терминологии, будем называть любой технологический процесс термином «бизнес-процесс», таким образом, в данном разделе не будем разделять технологические и бизнес-процессы.

**Бизнес-процесс** (БП) – совокупность взаимосвязанных операций (функций), направленных на получение определённого результата, с указанием начала и конца, точным определением входов, выходов, механизмов исполнения и управления.

**Процессное управление** – технология управления процессами (бизнес-процессами), направленная на достижение целей (бизнес-целей), включая обеспечение качества результатов деятельности. Таким образом, объектом управления являются бизнес-процессы, а уровень операционного риска характеризует качество бизнес-процессов.

### **Бизнес-цели:**

- получение дохода в результате основной деятельности предприятия;
- обеспечение условиями и ресурсами основной деятельности предприятия;
- управление деятельностью предприятия, его развитием.

Указанным целям соответствуют три **класса бизнес-процессов**:

- **основные** бизнес-процессы (бизнес-линии) – это процессы, в результате которых предприятие получает доход, то есть процессы его коммерческой и инвестиционной деятельности;

- **обеспечивающие** процессы – обеспечение деятельности предприятия всеми необходимыми ресурсами и условиями функционирования;

- процессы **управления** (организационные процессы) – процессы, направленные на повышение эффективности первых двух типов процессов.

**Задачи**, решаемые предприятием путём внедрения процессного управления:

- **унификация технологических процедур** (описание процессов);

- **управление изменениями** через усовершенствование процессов и снижение в них уровня операционного риска;

- оценка стоимости производимых предприятием продуктов через **стоимость процессов** (например, путём применения ABC – функционально-стоимостного анализа) и снижение стоимости процессов;

- автоматизация технологических процессов и бизнес-процессов (например, с использованием технологий **workflow** – потока работ и применением интегрированных систем SOA – архитектуры);

- структуризация и автоматическое обновление **регламентной документации** (например, на основе структуры моделей с использованием генераторов отчетов).

Процесс управления операционным риском (ОР) может быть эффективным, если созданная инфраструктура управления основана на надёжной рейтинговой системе.

**Рейтинговая система** включает в себя все методы, процедуры, системы контроля и сбора данных, а также информационные системы, которые содействуют оценке риска, присвоению внутренних рейтингов и количественным оценкам вероятности потерь и ущерба.

Важным элементом системы является **рейтинговая модель** управления операционным риском, которая включает показатели (атрибуты модели): подверженности операционному риску (EI), вероятности его проявления (PE), уровня потерь в случае реализации риска (LGE), ожидаемых потерь (EL), непредвиденных потерь (UL) и другие параметры (индикаторы) бизнес-процессов. Набор атрибутов рейтинговой модели называют **профилем риска**.

Процесс управления ОР – это информационный процесс, состоящий из двух этапов: 1) стратегии управления ОР и 2) процессного управления ОР (рис. 2.1).

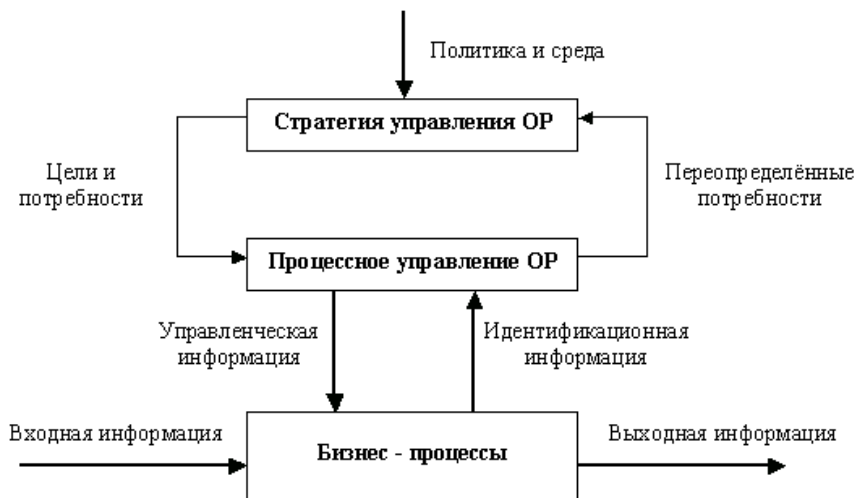


Рис. 2.1. Схема процесса управления операционным риском

На этапе 1 решается задача определения целей управления на основе а) состояний внешней и внутренней среды предприятия, политики управления ОР; б) принципов, правил управления ОР, показателей рейтинговой системы (потребностей).

На этапе 2 решается задача синтеза управляющих воздействий на основе рейтинговой модели управления ОР. Процессное управление состоит из идентификации, оценки, мониторинга, контроля и (или) минимизации ОР (включая выбор параметров рейтинговой модели).

## 2.2. Декомпозиция задачи управления операционным риском

Декомпозиция заключается в разделении задачи управления ОР на подзадачи, таким образом, чтобы поставленные бизнес-цели выполнялись, но при этом не создавались конфликтные ситуации.

На рис. 2.2 представлена схема вертикальной декомпозиции задачи управления ОР. Термин «вертикальная» означает разбиение задачи на этапы и типы работ, в отличие от «горизонтальной» декомпозиции по потребителям бизнес-процессов. Данная схема соответствует стандарту управления рисками ISO/IEC Guide 73 Risk Management. Все элементы схемы охвачены прямыми и обратными информационными связями, которые формируются в соответствии с утверждённой политикой (программой) управления ОР на уровне организационного управления ОР.

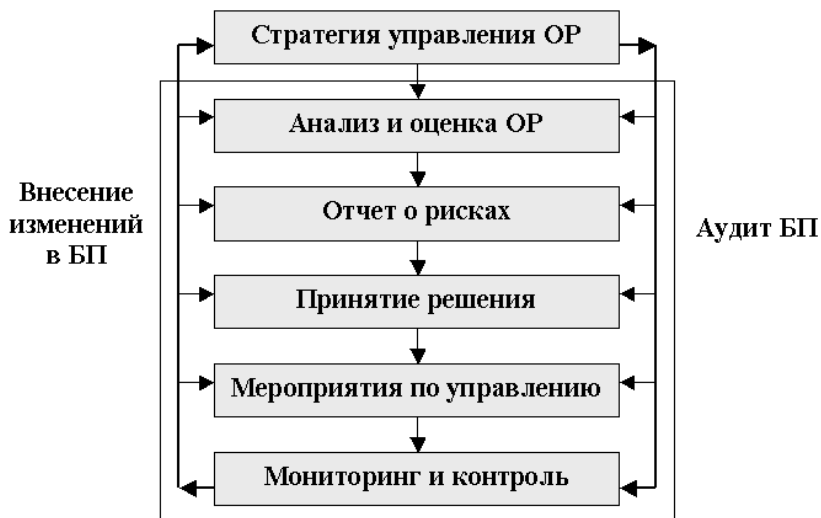


Рис. 2.2. Схема декомпозиции задачи управления операционным риском

Эффективное решение задач управления операционным риском достигается посредством:

- применения системного подхода (путём формирования замкнутой согласованной цепочки элементов: цели и планы – ресурсы – исполнители – процессы – угрозы – мониторинг и контроль – управление – эффект);
- улучшения процесса принятия решений (путём формирования понимания структуры бизнес-процессов, изменений в окружающей среде, потенциальных угроз);

- эффективного использования ресурсов и капитала предприятия;
- снижения степени неопределённости при осуществлении основной деятельности предприятия;
- оптимизации бизнес-процессов, включая минимизацию операционного риска;
- защиты имущественных интересов предприятия, повышения квалификации сотрудников и улучшения общественной репутации предприятия.

Управление ОР как сложной системой осуществляется путём итеративного применения алгоритма «агрегирования – дезагрегирования». Первая часть алгоритма «агрегирование» сосредоточена в подсистеме, обозначенной на рис. 2.2 как «Стратегия управления ОР». Детализация решения «дезагрегируется» на ряд задач, выделенных на рис. 2.2 прямоугольником. Такая модель управления ОР называется моделью принятия решений в условиях неопределённости (риска) [20].

Ниже даётся характеристика элементов приведённой схемы управления.

### **2.3. Стратегия управления операционным риском**

**Стратегия управления ОР** – цели, принципы, правила и методы управления ОР, основанные на моделях принятия решений в условиях неопределённости. Стратегия управления ОР является частью корпоративной стратегии развития, для реализации которой предусмотрено наличие ресурсов и их соответствующее распределение в организационной структуре предприятия. Таким образом, стратегия представляет собой спланированную систему действий, направленную на достижение установленных целей путём координации и сбалансированного распределения ресурсов (финансовых, материальных, информационных, людских и т.д.). По уровню иерархии выделяют корпоративные стратегии, стратегии бизнес-направлений, функциональные и операционные стратегии. Стратегия управления ОР относится к последнему из перечисленных уровней.



Формирование стратегии управления ОР включает разработку стратегии организации бизнес-процессов и риск-стратегию.

Формирование стратегии бизнес-процессов:

- цели организации БП и выбор приоритетных БП;
- ключевые показатели эффективности деятельности KPI (Key

Performance Indicators)

- методика и инструменты организации процессов;
- техническая поддержка БП;
- внутренние нормативные документы;
- модели процессов;
- порядок реализации, стимулирования и контроля.

Формирование риск-стратегии:

- планирование «работы с рисками» (предотвращение, уменьшение, принятие, передача рисков);
- формирование рейтинговой модели;
- показатели и критерии оценки риска KRI (Key Risk Indicators), рейтинговая модель;
- методика оценки операционного риска.

В качестве KPI могут быть выбраны показатели, формирующие траекторию развития предприятия, которые интерпретируются как составляющие консолидированного риска [18]. В состав KRI должны входить показатели и индикаторы рейтинговой модели (см. раздел 4).

Функциональное описание стратегии управления ОР приведено в табл. 2.1.

Таблица 2.1

<b>Входы</b>	<b>Функции</b>	<b>Выходы</b>
1. Политика 2. Данные внешней среды 3. Данные внутренней среды 4. Планы предприятия	1. Формирование стратегии организации БП 2. Формирование риск-стратегии	1. Цели, приоритеты, план управления ОР 2. Рейтинговая модель 3. Модели БП 4. Пороговые уровни и лимиты 5. Документы, методики и отчётные формы 6. Стимулы

Таким образом, стратегия управления ОР, как минимум, должна включать: оценку масштаба усилий по управлению риском (оценку трудоёмкости и стоимости); показатели KPI и KRI, параметры управления (параметры рейтинговой модели, лимиты и ограничения, при превышении которых вводятся в действие определённые процедуры и проводятся соответствующие мероприятия); периодичность проведения самооценок ОР, аудита бизнес-процессов, периодичность переопределения потребностей.

## 2.4. Анализ и оценка операционного риска

Анализ ОР включает идентификацию рисков и описание рисков.

**Идентификация рисков** – процесс выявления рисков, характерных для определённого вида деятельности (бизнес – процесса), и определения их характеристик.

Функциональное описание процесса идентификации ОР приведено в табл. 2.2.

Таблица 2.2

Входы	Функции	Выходы
1. План управления ОР 2. Список источников риска 3. Классификатор направлений деятельности 4. Классификатор событий 5. Структурные модели БП 6. Данные (потери, индикаторы, ресурсы)	1. Сбор данных 2. Выявление источников риска 3. Классификация риска 4. Определение эффекта воздействия риска	1. Заполненные экспертные идентификационные формы 2. Причины, факторы, характеристики риска 3. Информация в БД рисков 4. Связи с другими БП

Пример указанного в табл. 2.2. классификатора направлений деятельности АЭС и классификатор событий (источников риска) приведены в приложении 1.

Одной из типичных методологических ошибок идентификации операционных рисков является попытка собрать и «задокументи-

ровать навсегда» все возможные риски предприятия. Такой подход к решению задачи идентификации ОР невыполним на практике. Просто потому, что обязательно появляются новые возможные и «ранее не учтённые» источники риска. Конструктивным представляется подход последовательного анализа БП, в котором вначале строится структурная модель конкретного анализируемого БП, а затем только применительно к нему выявляются и классифицируются возможные ОР с использованием экспертных методов (интервью, техника номинальной группы, техника Дельфи, нечёткая логика и др.).

Последовательность этапов идентификации ОР представлена ниже.

1. Предварительный сбор данных об операционных потерях по всем бизнес-процессам.

2. Выбор бизнес – процесса или совокупности бизнес-функций (БФ) для анализа.

3. Подготовка экспертных форм по каждой из БФ процесса с учётом факторов, действующих на входе, выходе, управлении и механизмах реализации БФ (рис. 2.3).

4. Экспертная оценка факторов риска на БФ (ЕСТЬ/НЕТ воздействию) и их классификация.

5. Структурирование полученной информации на основе заполненных экспертных форм.



Рис. 2.3. Последовательность операций по идентификации операционного риска

**Описание рисков** – представление выявленных рисков в определённом формате для последующего анализа. Пример формы описания ОР представлен в табл. 2.3.

**Оценка ОР включает** качественное измерение рисков и количественное измерение рисков.

Таблица 2.3

<b>1. Наименование риска</b>	Операционный
<b>2. Вид деятельности</b>	Вид бизнес – процесса, описание рисков-ных событий
<b>3. Тип риска</b>	Категории и уровни классификации
<b>4. Заинтересованные лица</b>	Заинтересованные лица и их ожидания
<b>5. Количественное выражение риска</b>	Значение ожидаемых потерь и вероятность
<b>6. Приемлемость риска</b>	Финансовое значение возможных убытков, ограничения параметров рейтинговой модели, желаемый уровень качества бизнес – процесса
<b>7. Управление риском и механизмы контроля</b>	Действующие методы / практика управления риском, уровень качества контроля, существующие протоколы учета, анализа и контроля рисков
<b>8. Возможности для улучшения</b>	Рекомендации по снижению риска
<b>9. Стратегические и управленческие улучшения</b>	Функции, ответственность за разработку и внедрение стратегии и процессного управления рисками

**Качественное измерение ОР** предполагает оценку вероятности события и оценку возможных последствий реализации риска. Пример качественной оценки вероятности события приведён в табл. 2.4.

Таблица 2.4

<b>Оценка вероятности</b>	<b>Описание</b>	<b>Пояснения</b>
<b>Высокая</b>	Вероятность наступления события каждый год, вероятность больше 25%	Потенциальная вероятность того, что событие наступит несколько раз в течение года. Событие произошло недавно.
<b>Средняя</b>	Существует вероятность наступления события в течение года, вероятность менее 25 %	Возможно, что событие наступит несколько раз в течение года. Существует история наступления события
<b>Низкая</b>	Практически отсутствует вероятность наступления события в течение года, вероятность менее 2 %	Событие не наступало. Вероятность наступления события мала

Пример качественной оценки возможных последствий реализации риска приведён в табл. 2.5.

Таблица 2.5

<b>Высокий</b>	<p>Финансовые последствия не превысят <math>UL = A</math> тыс. руб.          Существенное влияние на стратегическое развитие и деятельность предприятия.          Существенная обеспокоенность заинтересованных лиц</p>
<b>Средний</b>	<p>Финансовые последствия находятся в пределах <math>X = B</math> тыс. руб. и <math>Y = C</math> тыс. руб.          Умеренное влияние на стратегическое развитие и деятельность предприятия.          Умеренная обеспокоенность заинтересованных лиц</p>
<b>Низкий</b>	<p>Финансовые последствия ниже <math>UL = D</math> тыс. руб.          Слабое влияние на стратегическое развитие и деятельность предприятия.          Слабая обеспокоенность заинтересованных лиц</p>

Количество градаций качественной оценки может быть увеличено, например: высокий, значительный, средний, ниже среднего, низкий.

На практике **количественное измерение** ОР бизнес-процесса основано на оценке величины ожидаемых потерь  $EL$ :

$$EL = q \cdot C,$$

где  $q$  – мера возможности наступления негативного события, приводящего к убыткам. Мерой возможности наступления события может служить либо вероятность его наступления, либо её нечёткий аналог, задаваемый с помощью характеристических функций.  $C$  – стоимость «под риском», характеризующая величину последствия негативного события (сумма потерь в результате реализации негативного события).

На практике применяют следующие подходы вычисления  $EL$ .

**«Индикаторный» подход.** Оценка  $EL$  производится по формуле

$$EL = k \cdot Ind,$$

где  $k$  – некоторый коэффициент, вычисляемый на основе статистических данных по негативным событиям с учётом их последствий; Ind – индикатор бизнес-процесса или направления деятельности. Примером индикаторов могут служить: зарплата сотрудников, обслуживающих бизнес-процесс; валовой доход бизнес-процесса; величина материальных активов и др.

**«Вероятностный» подход.** Оценка EL производится по формуле

$$EL = P \cdot C,$$

где мерой возможности наступления негативного события является  $P$  – вероятность его наступления.

**«Нечёткий» подход (Fuzzy Logic).** Оценка EL производится по формуле

$$EL = P(\text{ПОР}) \cdot C,$$

где вероятность  $P$ , зависящая от показателя операционного риска ПОР, определяется экспертами с применением аппарата нечёткой логики **Fuzzy Logic** [21].

**«Комбинированный» подход** на основе рейтинговой модели, объединяющий два последних подхода. Функциональное описание «комбинированного» подхода представлено в табл. 2.6, а его формализованное описание будет дано в пп. 3.3 и 3.4.

Таблица 2.6

Входы	Функции	Выходы
1. Экспертные идентификационные формы 2. Качественные оценки 3. Данные статистики (внешние, внутренние)	1. Обработка экспертной информации (Fuzzy Logic) 2. Обработка статистической информации	1. Экспертные оценки показателя операционного риска (ПОР) 2. Показатели рейтинговой модели 3. Оценка необходимых резервов

**Отчёт о рисках.** Основные положения отчёта об операционных рисках должны быть чётко определены, а информация об ОР должна быть доступна для всех заинтересованных лиц. К заинтересованным лицам относятся:

- члены Наблюдательного Совета (Совета директоров);
- исполнительное руководство предприятия;
- руководители структурных подразделений;
- сотрудники;
- контрагенты.

Формы отчетов для заинтересованных лиц закрепляются во внутренних документах предприятия. Формальный отчёт должен в себя включать:

- методы системы внутреннего контроля в части ответственности менеджмента в вопросах управления ОР;
- способы идентификации ОР и их практическое применение в действующей системе управления;
- основные инструменты системы внутреннего контроля в отношении наиболее значимых ОР;
- действующие механизмы мониторинга и контроля ОР;
- основные «узкие моменты» и предлагаемые способы управления ОР.

Возможная структура отчёта приведена в табл. 2.7.

Таблица 2.7

№	Структура отчёта
1	Основания для составления отчёта (план, реализация рискового события с тяжёлыми последствиями, аудиторская проверка и т.д.).
2	Объект анализа (бизнес-линия, бизнес-процесс, бизнес-функции)
3	Данные мониторинга (статистика, индикаторы, «опасные» признаки)
4	Описание рисков (качественные, количественные характеристики ОР, сводная форма описания)
5	Оценка необходимых резервов под ОР и резервы капитала под ОР
6	Заключение (оценка качества объекта, перечень приоритетных рисков, изменения, дополнения, предложения)

## 2.5. Принятие решения и разработка мер реагирования на риск

**Принятие решения.** Под принятием решения в данном случае будем понимать выбор из конечного множества альтернатив такого варианта, который обеспечит минимальный уровень операционно-

го риска. В качестве альтернатив рассматриваются следующие способы работы с риском, направленные на то, чтобы:

- избежать риск (устранение, где это возможно, причин возникновения риска);
- снизить величину риска (за счёт снижения возможности возникновения негативного события или стоимости «под риском»);
- принять риск (принятие последствий риска и разработка мер по устранению последствий);
- передать риск (страхование или передача управления риском третьей стороне, если это возможно).

При подготовке альтернатив необходимо проанализировать плотность распределения потерь для различных типов операционного риска и оценить величину принимаемых и передаваемых рисков. На рис. 2.4 представлен пример кривой распределения потерь для случаев причинения ущерба материальным активам.

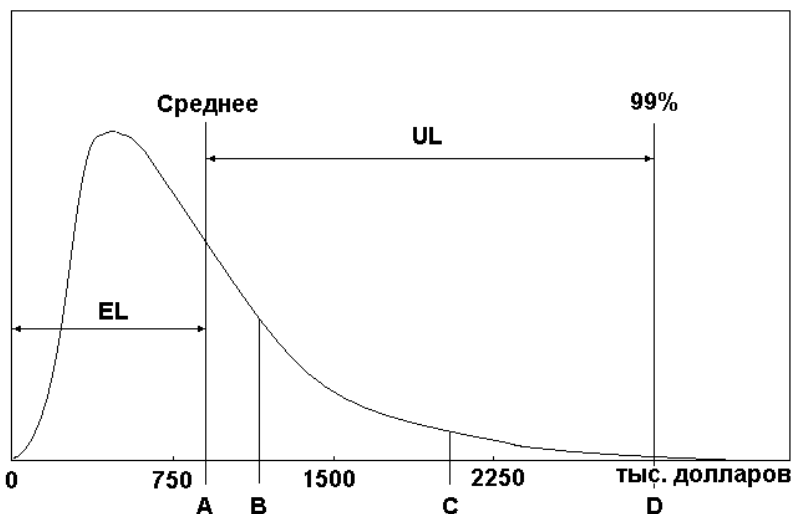


Рис. 2.4. Пример распределения потерь для случаев причинения ущерба материальным активам

Проиллюстрирована ситуация с передачей ОР путём страхования. Точка *A* соответствует величине ожидаемых потерь  $EL = 1000$  тыс. долларов. Эти потери могут быть приняты и покрыты за счёт



сформированных под них резервов. Величина непредвиденных потерь  $UL$  может быть покрыта следующим образом. Риск, соответствующий величине потерь  $AB$ , может быть принят и отнесён на величину лимита/франшизы страхового полиса. Риск  $BC$  может быть передан и покрыт за счёт страхования. А величина  $CD$  покрыта капиталом предприятия, зарезервированным под операционный риск.

**Разработка мероприятий.** После того, как выбрана оптимальная реакция на выявленные риски, необходимо разработать ряд превентивных мероприятий. Целью этих работ является ослабление проявления ОР. Они включают разработку планов по предотвращению операционного риска и ослаблению его влияния, а также меры по реагированию на реализовавшиеся риски.

Прежде всего, должны быть установлены граничные условия, при которых риск становится неприемлемым. Обычно эти условия оговариваются на этапе формирования стратегии управления ОР. Затем планируются изменения в требованиях и действующих практиках реализации бизнес-процессов. Все эти изменения должны устранить источники неприемлемых рисков или заместить их решениями с меньшим уровнем риска.

Согласно стандартам управления рисками [22] система мероприятий должна быть направлена на обеспечение следующего минимума:

- надёжность и эффективность работы предприятия;
- эффективность системы внутреннего контроля;
- соответствие законодательству.

Не смотря на сжатость и кажущуюся простоту формулировки приведённых выше требований, реализовать их достаточно сложно в условиях несовершенных корпоративных отношений. В качестве примера действий по уменьшению последствий ОР можно рекомендовать следующее:

- укомплектование команды служащих предприятия талантливymi и компетентными людьми;
- проведение функционально-стоимостного анализа бизнес-процессов;

- разработка организационной структуры, внутренних правил и процедур (регламентов) совершения операций таким образом, чтобы исключить (или минимизировать) возможность возникновения факторов операционного риска;
- развитие систем автоматизации технологий и защиты информации;
- передача риска или его части третьим лицам (например, аутсорсинг);
- использование традиционных видов имущественного и личного страхования;
- создание комплексной системы мер по обеспечению непрерывности финансово-хозяйственной деятельности при совершении банковских операций и других сделок, включая планы действий на случай непредвиденных (чрезвычайных) обстоятельств;
- проведение регулярных аудитов бизнес-процессов;
- проведение на постоянной основе обучения и переподготовки служащих.

После того как принято решение, выработаны меры и определены механизмы реализации решения, необходимо организовать процесс наблюдения и контроля параметров принятого решения.

## **2.6. Мониторинг и контроль операционного риска**

**Мониторинг ОР** – систематическое наблюдение за состоянием предприятия в целях оценки, контроля и прогнозирования операционного риска, т.е. мониторинг обеспечивает систематический контроль бизнес-процессов и оценку эффективности действий по управлению ОР на основе принятой системы индикаторов.

Цель проводимых работ – установить факт того, что:

- система реагирования на риски действует в соответствии с планом;
- «реагирование» эффективно или необходимы изменения;
- риски изменились или не изменились по сравнению с предыдущим периодом;
- влияние на финансовый результат «положительное» или «отрицательное»;

- необходимые меры приняты или они остались лишь «на бумаге»;
- воздействие оказалось запланированным или незапланированным.

Для каждого индикатора необходимо установить лимиты (пороговые значения), что позволит обеспечить выявление значимых для предприятия операционных рисков и своевременное адекватное воздействие на них.

Мониторинг операционного риска может проводиться как на уровне подразделений, так и в целом по предприятию. Полученную в процессе мониторинга операционного риска информацию о потенциальном изменении уровня риска следует своевременно доводить до соответствующих органов управления, подразделений, служащих для принятия необходимых мер.

**Контроль** соблюдения установленных правил и процедур осуществляется в рамках системы внутреннего контроля предприятия. В отношении контроля операционного риска наиболее важным является:

- контроль соблюдения установленных лимитов на показатели риска;
- соблюдение установленного порядка доступа к информации и материальным активам;
- надлежащая подготовка персонала.

Функциональное описание процесса мониторинга и контроля ОР приведено в табл. 2.8.

Таблица 2.8

Входы	Функции	Выходы
1. План управления ОР 2. Информация базы данных ОР 3. Данные внутреннего аудита	1. Слежение за идентификацией ОР 2. Структурный анализ БП и операционного риска 3. Контроль выполнения плана управления ОР 4. Контроль эффективности («план-факт» на основе индикаторов риска) 5. Подготовка информации для ЛПР	1. Переработанный план управления ОР 2. Корректирующие действия 3. Требования на реструктуризацию или реинжиниринг (если необходимо) 4. Отчёты

Таким образом, главными задачами мониторинга и контроля ОР являются: приведение плана мероприятий противодействия рискам в соответствие с текущим состоянием направлений деятельности предприятия и отдельных бизнес-процессов, количественные и качественные анализы ОР, дополнительная идентификация ОР в ходе технологического процесса.

Следует подчеркнуть перспективность применения процессного подхода к управлению операционным риском предприятия. Это обусловлено тем, что любую систему преобразования входов в выходы можно представить как систему принятия решений. С другой стороны, – любую деятельность можно рассматривать как систему принятия решений, опираясь на целесообразность поведения системы и составляющих её элементов. Если, конечно, целенаправленное поведение возможно и оно формализовано. Только в этом случае можно считать, что формализованная цель, определённая задачей принятия решений может быть достигнута, а сама задача решена.

## Вопросы и ответы

**Вопрос.** Что даёт предприятию, кроме дополнительных затрат, внедрение процессного подхода к управлению операционным риском?

**Ответ.** Следует отметить, что внедрение процессного подхода не обязательно приводит к повышению стоимости обслуживания технологических и бизнес-процессов предприятия. Ведь суть подхода заключается именно в разработке процессов, минимизирующих указанную стоимость, например, с помощью проведения функционально-стоимостного анализа. Используя процессный подход, предприятие удовлетворяет свои потребности в качественной технологии. Реализация данного подхода позволяет предприятию не только сохранить свою устойчивость, но и развиваться. Каким образом? Путём вытеснения старой, теряющей свою конкурентоспособность технологии, и замены её на новую, менее рискованную и более качественную.

**Вопрос.** Как практически осуществить идентификацию операционного риска? Какова должна быть последовательность шагов?

**Ответ.** Давайте разберём последовательность проведения идентификации ОР на простом примере, моделирующем ситуацию идентификации риска. Предположим, что предприятию необходимо закупить программное обеспечение и оборудование (Продукт) для совершенствования своей ИТ – технологии. Для этого требуется реализовать бизнес-процесс «Определение требований к Продукту». Необходимо идентифицировать операционный риск этого бизнес-процесса.

Сначала необходимо выявить источники риска. Для этого строится структурная модель операций. Простая структурная модель в стандарте IDEF0, описанная как бизнес-функция (БФ), показана на рис. 2.5.



Рис. 2.5. Пример модели бизнес-функции «Определение требований к продукту»

Входами модели являются: методика оценки бизнес-процессов (БП); заявка на Продукт, поступившая от заказчика; внутренние требования ИТ – технологии. В качестве управляющих воздействий на БФ рассматриваются международные стандарты и внутренние инструкции управления. На выходе БФ должен быть сформирован документ «Требование на Продукт». В качестве механизма реализации БФ рассматривается ИТ – подразделение предприятия.

Затем осуществляется подготовка экспертных форм с учётом факторов, действующих на входе, выходе, в управлении и механизмах реализации БФ. Для упрощения задачи предположим, что ОР идентифицируется путём разделения негативных событий на две группы: первая группа связана с технологическими особенностями обслуживания БФ; вторая – со случайными событиями источников риска. Пример экспертных форм приведен в табл. 2.9.

На следующем шаге разработанные формы предъявляются экспертам. После обработки их ответов вычисляются средние значения факторов риска FT и FC. Затем классифицируется ОР с помощью классификатора событий (см. Прилож.1). В данном примере операционный риск относится к категории 5: "Качество процесса и процедур управления".

**Вопрос.** Чем должен заниматься риск-менеджер структурного подразделения предприятия в части управления операционным риском? Каковы его функции?

**Ответ.** Следует заметить, что на предприятиях атомной отрасли ещё не создан "институт" риск-менеджеров. Но международный опыт показывает, что на каждом предприятии должен быть разработан и утверждён *свой* собственный внутренний документ, устанавливающий порядок проведения операций по управлению операционным риском. Например, в этом документе может быть прописан порядок выполнения следующих основных функций риск-менеджерами:

- организация сбора информации о фактах убытков, понесенных структурным подразделением предприятия (СПП) от реализации операционных рисков и индикаторах указанных рисков;
- проведение первичного анализа полученной информации;
- построение структурных моделей процессов "как есть" и "как надо" для анализа ОР;
- ввод информации о фактах убытков, понесенных СПП от реализации операционных рисков и индикаторах указанных рисков в аналитическую базу данных предприятия;
- информирование руководителя СПП о наличии признаков возможности существенных потерь в случае реализации рисков.

Процесс выполнения указанных функций собственно и составляет основу мониторинга ОР.

Таблица 2.9

**Определение требований к Продукту**  
Оценка индикаторов технологического риска FT

<b>Вопрос для оценки фактора</b>		<b>Да=0 Нет=1</b>
	Определяются ли различные точки зрения (финансовая, юридическая, управленческая, техническая) на требования к Продукту, отвечающему нуждам Заказчика?	1
	Требования регулярно пересматриваются в соответствии с нуждами Заказчика?	1
	Анализируются ли требования безопасности, надежности, сопровождаемости и эффективности Продукта?	1
	Соответствуют ли требования на Продукт стандарту ИСО 8402	1
	Утверждается ли документ требований (спецификация) на Продукт?	2
<b>FT</b>		
<b>Оценка индикаторов событийного риска FC</b>		<b>Да=1 Нет=0</b>
	<b>Вопрос для оценки фактора</b>	
	Возможны ли неквалифицированные действия или злоупотребления персоналом при реализации БФ?	
	Чувствительна ли БФ к последствиям утраты в результате аварий или внешних воздействий? (т.е. трудно ли восстановить БФ?)	
	Существует ли зависимость от "незаменимых" исполнителей?	
	Зависит ли БФ от юридически некорректных документов?	
	Имели ли место случаи невыполнения должностных обязанностей исполнителями?	
<b>FC</b>		<b>0</b>

**Вопрос.** Как и каким индикатором можно оценить уровень операционного риска в случае отказа какого-нибудь элемента технической системы предприятия?

**Ответ.** Давайте рассмотрим следующую «модельную» ситуацию. Предположим, в результате короткого замыкания был на сутки остановлен насос НА-3 (насос аппаратный системы технического водоснабжения АЭС) со стоимостью текущего обслуживания  $C = 30$  тыс. руб.

Оценку проведём в два этапа: 1) классифицируем ОР и дадим ему качественную оценку; 2) затем дадим количественную оценку ОР на основе индикатора возможных потерь.

Из контекста «модельной» ситуации следует, что ОР соответствует направлению деятельности «Эксплуатация гидротехнических сооружений и водное хозяйство» (см. приложение 1) и бизнес-процессу «Техническое обслуживание и ремонт». Источник риска – «Работа оборудования (надёжность/готовность)». Такая классификация позволяет определить статистические параметры ОР (например, из базы данных рисков). При качественной оценке операционного риска риск-менеджер должен оценить ОР по некоторой шкале. Пусть внутренняя методика оценки ориентирована на пятибалльную шкалу: 1 – риск отсутствует; 2 – низкий; 3 – умеренный; 4 – значительный; 5 – высокий.

Пусть риск-менеджер оценил риск как «умеренный». После проведения классификации риска и качественной оценки ОР осуществляется расчёт вероятности потерь  $P$  для параметров классификации и связанных с ними статистических параметров. Предположим, что в соответствии с внутренней методикой плотность вероятности потерь распределена по закону Пуассона. Для бизнес-процесса «Техническое обслуживание и ремонт»

$$P(t = 1 \text{ сутки}; n = 1, \text{ «умеренный»}) = 0,016.$$

Тогда количественная оценка операционного риска находится путем расчета индикатора возможных потерь (ИВП) в соответствии с формулой:

$$\begin{aligned} \text{ИВП} &= P(t = 1 \text{ сутки}; n = 1, \text{ «умеренный»}) \cdot C = \\ &= 0,016 \cdot 30 \text{ тыс. руб.} = 0,48 \text{ тыс. руб.} \end{aligned}$$



## Тесты для самоконтроля

1. Что это такое, по сути, процессное управление?
  - Технология управления бизнес-процессами.
  - Процесс управления операционным риском.
2. К какому классу бизнес-процессов относится контроль операционного риска?
  - Основной процесс.
  - Обеспечивающий процесс.
  - Организационный процесс.
3. Рейтинговая модель и рейтинговая система это одно и то же?
  - Да.
  - Нет.
4. Какие функции входят в структуру процесса идентификации операционного риска?
  - Выявление источников риска.
  - Классификация риска.
  - Определение эффекта воздействия риска.
5. Различаются ли по смысловому содержанию «оценка вероятности события операционного риска» и «оценка возможных последствий реализации операционного риска»?
  - Да.
  - Нет.
6. Какие процедуры входят в состав процесса мониторинга операционного риска?
  - Наблюдение за показателями операционного риска.
  - Анализ показателей операционного риска.
  - Контроль показателей операционного риска.
  - Представление показателей операционного риска в форме, необходимой для принятия решений.
7. Выберите верный ответ: *Франшиза страхового полиса – это...*
  - Условие договора страхования, согласно которому страховщик освобождается от возмещения убытков, не превышающих определённой денежной суммы.
  - Не знаю. Поскольку в п. 2.5 упоминается этот термин без определения и разъяснения.

## Раздел 3

---

### МЕТОДЫ ОЦЕНКИ ОПЕРАЦИОННОГО РИСКА

---

#### **Цель занятия:**

- в простой и доступной форме изложить методы оценки операционного риска, предложенные международным Базельским комитетом, дать описание модели оценки операционного риска, основанной на внутреннем рейтинге бизнес-процессов, изложить методику экспертной оценки операционного риска с применением структурных и логических моделей.

#### **Вы научитесь:**

- на основе методов оценки операционного риска рассчитывать величину ожидаемых и непредвиденных убытков;
- оценивать вероятностные характеристики операционного риска;
- строить правила логических операций для оценки показателя операционного риска бизнес-процесса;
- проводить расчёт ожидаемых потерь с применением синтетического подхода, объединяющего функционально-стоимостной анализ и нечёткую оценку показателей операционного риска.

#### **В программе занятия:**

- лекция, в которой излагаются методы оценки операционного риска и вычислительные процедуры, связанные с этими оценками;
- вопросы и ответы;
- тесты для самоконтроля.

### 3.1. Методики измерения операционного риска, применяемые на практике

В развиваемом Базельским комитетом подходе операционный риск предлагается оценивать величиной ущерба/убытков (ожидаемых и непредвиденных потерь), которые должны быть «покрыты» соответствующим размером отчисляемого на операционный риск капитала ORC. Из соглашения по капиталу, принятого Базельским комитетом [23,24], следует что

$$OP = 1/k \cdot \text{размер капитала, отчисляемого на ОР,}$$

где ОР – операционный риск; коэффициент  $k = 0,08$  устанавливается органом надзора. То есть с точностью до константы операционный риск измеряется размером капитала, отчисляемого на операционный риск. Такой подход хорошо согласуется с процессным методом управления риском и экономически увязан с методами корпоративного управления.

Следует отметить, что кроме указанного подхода существуют и другие методы измерения риска. Например, в работе [25] количественное описание риска, связанного с технологическими процессами и безопасностью, опирается на теоретико-вероятностный подход. В этом случае риск  $R(\theta, \delta(x))$ , зависящий от параметра  $\theta$ , представляется функцией:

$$R(\theta, \delta(x)) = \int L(\theta, \delta(x)) f(x|\theta) dx,$$

где  $\delta(x)$  – оценка параметра  $\theta$ , вычисленная по наблюдениям  $x$ ;  $L(\theta, \delta(x))$  – функция потерь;  $f(x|\theta)$  – функция плотности распределения случайной величины  $x$ , зависящая от параметра  $\theta$ .

Относительно пределов интегрирования следует отметить, что нижний предел соответствует установленному порогу фиксации потерь (порог, начиная с которого ущерб оценивается как «значимый» для предприятия), а верхний предел ограничен величиной квантиля 99,9 % уровня значимости. Теоретико-вероятностные методы пока не нашли широкого применения в системах управления рисками предприятий.

В документе [23] излагаются три подхода (методики) расчета размера капитала, отчисляемого на операционный риск: 1) базовый

метод показателей (**BIA** – Basic Indicator Approach); 2) стандартизированный метод (**TSA** – Standardised Approach); и 3) усовершенствованные методы измерения (группа методов **AMA** – Advanced Measurement Approaches).

Первые два подхода соответствуют «грубой» оценке ОР. Наиболее предпочтительными для построения риск-ориентированных систем управления являются усовершенствованные методы группы **AMA**.

### 3.2. Усовершенствованные методы измерения операционного риска

Основу группы «усовершенствованных» методов **AMA** составляют подходы, развиваемые в рамках моделей **IMA** (Internal Measurement Approaches), **LDA** (Loss Distribution Approaches) и экспертных моделей **SA** (Scorecard Approaches).

Подход, основанный на усовершенствованных методах измерения операционного риска, включает три основных этапа.

**Этап 1.** Выделение на предприятии  $i = 1, 2, \dots, I$  типовых направлений деятельности и их структурное описание.

**Этап 2.** Определение кластеризованных видов ущерба (разбиение по категориям источников риска)  $j = 1, 2, \dots, J$  для каждого направления  $i$ .

**Этап 3.** Расчёт размера резервируемого под риск капитала в соответствии с соотношением

$$\begin{aligned} \text{ORC} &= \sum_i \sum_j (\gamma(i, j) \cdot \text{EI}(i, j) \cdot \text{PE}(i, j) \cdot \text{LGE}(i, j)) = \\ &= \sum_i \sum_j (\gamma(i, j) \cdot \text{EL}(i, j)), \end{aligned}$$

где  $\text{EI}(i, j)$  – индикатор подверженности операционному риску («стоимость под риском»);  $\text{PE}(i, j)$  – вероятность проявления случаев операционных потерь;  $\text{LGE}(i, j)$  – уровень потерь (по терминологии **AMA** – «тяжесть потерь» на один негативный случай) в случае реализации риска;  $\text{EL}(i, j)$  – размер ожидаемого убытка (средние потери за 1 год);  $\gamma(i, j)$  – коэффициент непредвиденных убытков.

Индикатор **EI (Exposure Indicator)** представляет собой «замениТЕЛЬ» размера рисковой стоимости. Базельский комитет предлагает стандартизовать **EI** для направлений деятельности (бизнес-

линий) и видов ущерба. В качестве таких индикаторов рассматриваются: валовой доход, среднегодовые активы, фонды под управление материальными активами, зарплата сотрудников и др.

Параметр **PE (Probability of loss Event)** представляет собой вероятность наступления негативных событий, связанных с ущербом/убытками («частота событий» за период времени  $t$ ), а **LGE (Loss Given Event)** – представляет собой долю потерь (от «стоимости под риском»), которая соответствует установленному негативному событию.

Коэффициент  $\gamma$  не может быть определён на основе только внутренних статистических данных о потерях, собранных на предприятии. Нужны внешние статистические данные по всей отрасли. На рис. 3.1 приведена ситуация, в которой частота редких, но больших по размеру потерь (так называемый «хвост» распределения потерь) может быть оценена лишь с привлечением внешней информации. Возможно, эти коэффициенты следует вводить директивно.

Количество случаев



Рис. 3.1. Пример распределения величины убытков

Условия применения модели:

- временной интервал при расчете операционного риска  $t = 1$  год;

- уровень доверия в расчётах – **99,9 %**, т.е. сумма ожидаемых и непредвиденных потерь рассчитывается с вероятностью 99,9 %);
- минимальный размер резервируемого капитала определяется с учетом **ожидаемых и непредвиденных** убытков (ожидаемые и непредвиденные потери с вероятностью 99,9 % покрываются капиталом, если ожидаемые убытки не учтены сформированными на предприятии резервами «под потери»);
- величина периода  $T$  накопленных статистических данных должна составлять не менее **5 лет**.

### **3.3. Внутренняя рейтинговая модель для измерения операционного риска**

Термин «**рейтинговая модель**» тесно связан с ранее определённым термином «рейтинговая система» и включает в себя формализованное описание характеристик операционного риска и процедур его оценки.

Формальное описание рейтинговой модели для измерения операционного риска, основанное на подходе AMA, представим в следующей символической форме:

$$IRM = \{ПОР, PE, LGE, EL, EI, UL\}.$$

Символом **IRM** обозначена внутренняя рейтинговая модель, справедливая для любой из стандартизованных бизнес-линий. В скобках указаны элементы модели, которые определяются на основе экспертной и статистической информации.

**ПОР** (показатель операционного риска) – индикатор возможности потерь, область значений которого лежит в интервале от 0 до 1; определяется на основе экспертных методов по результатам аудита бизнес-процессов; характеризует уровень вероятности проявления негативных событий, связанных с бизнес-процессами (чем больше значение вероятности случаев потерь, тем выше уровень ПОР). То есть уровень ПОР – есть рейтинг анализируемого бизнес-процесса в модели IRM. Уровень ПОР определяется технологическими FT и случайными FC факторами, может быть оценен методами Fuzzy Logic (подробнее см. п. 3.4).

Вероятность случаев потерь  $PE$  характеризует «частоту» негативных событий в год. Величина  $PE$  рассчитывается на основе функции распределения  $F(n_x)$ :

$$F(n_x) = \sum_{n=0}^{n_x} h(n),$$

где в качестве  $h(n)$  рассматриваются [26] распределение Пуассона или биномиальное распределение числа негативных событий  $n$ .

Вероятность того, что число негативных событий  $n$  будет меньше  $n_x$ :

$$PE = F(n_x).$$

Распределение Пуассона имеет вид

$$h(n) = \lambda^n \exp(-\lambda)/n!,$$

где параметр распределения  $\lambda$  – среднее число негативных событий в год. Пример функции распределения  $F(n)$  для  $\lambda = 10$  приведён на рис. 3.2.

**Распределение числа негативных событий (PE в АМА)**

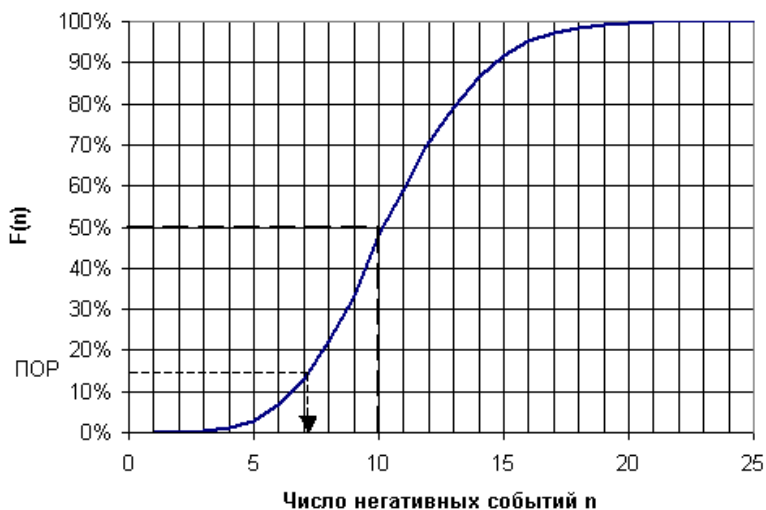


Рис. 3.2. Пример функции распределения  $F(n)$  негативных событий  $n$  (случаев потерь) для  $\lambda = 10$

**Уровень потерь LGE** в модели IRM определяется функцией распределения  $F_x$  случайной величины  $x$ . Для того чтобы понять, что есть  $x$ , необходимы следующие пояснения.

Пусть в течение года произошло  $n$  случаев потерь (негативных событий), и их величина в денежном выражении имела значения  $x_i$ ,  $i = 1, \dots, n$ . Тогда совокупные годовые потери определяются формулой  $z = x_1 + x_2 + \dots + x_n$ .

В модели IRM переменная  $z$ , зависящая от случайных величин  $n$  и  $x$ , является случайной величиной с функцией распределения  $F_z$ . Случайная величина потери на одно негативное событие  $x$  имеет функцию распределения

$$F_x = \int_{-\infty}^x g(\xi) d\xi,$$

где  $g(\xi)$  – плотность логнормального распределения случайной величины  $\xi$ . Если обозначить

$$u(x) = (\ln x - \mu)/\sigma,$$

где  $\mu$ ,  $\sigma$  – математическое ожидание и стандартное отклонение логарифма случайной величины  $\xi$ , то для уровня потерь LGE можно записать

$$\text{LGE} = F_x = \Phi(u(x)),$$

где  $\Phi(u)$  – табулированная функция Лапласа [27].

Таким образом, LGE – вероятность потери на одно негативное событие объёмом  $\xi < x$ . Вид функции распределения  $F_x$  показан на рис. 3.3.

**Пример.** Пусть необходимо найти LGE для бизнес-линии, у которой функции распределения  $F(n)$  и  $F_x$  имеют вид, показанный на рис. 3.2 и 3.3, средние потери на одно событие  $x_{\text{cp}} = \$10$  млн., а показатель операционного риска ПОР по результатам аудита имел величину 15 %.

Сначала найдём величину  $n_x$ :

$$n_x = F^{-1}(\text{ПОР}) = 7,$$

где  $F^{-1}$  – функция, обратная  $F(n)$ . Иными словами, откладывая на оси ординат (см. рис. 3.2) значение ПОР = 15 %, находим на оси абсцисс значение  $n_x = 7$ . Затем ищем значение  $x$ , соответствующее  $\text{PE} = \text{ПОР} = 15\%$ :

$$x = \lambda \cdot x_{\text{cp}} / n_x = 10 \cdot 10 \text{ млн. долларов} / 7 = 14,3 \text{ млн. долларов.}$$



### Распределение потерь на одно событие (LGE в АМА)

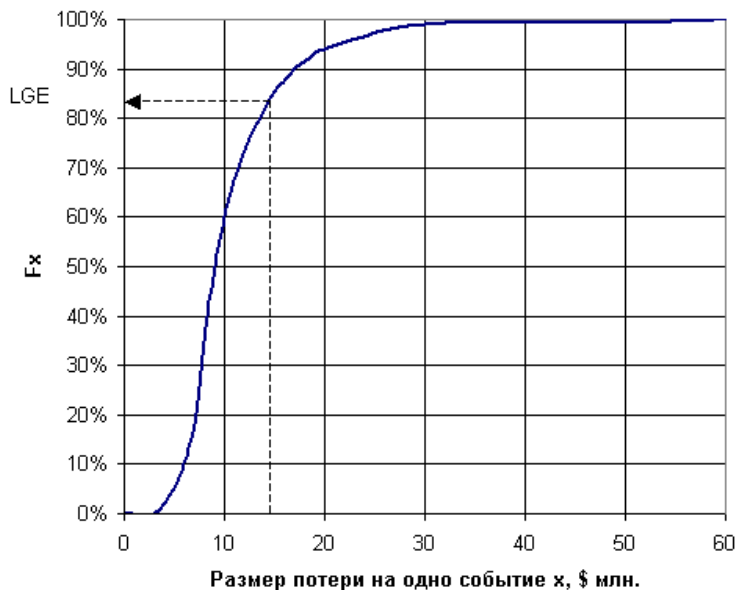


Рис. 3.3. Пример функции распределения потерь  $F_x$

Используя график  $F_x$  (см. рис. 3.3) для  $x = 14,3$  млн. долларов, находим  $LGE = 83\%$ . Следует обратить внимание на то, что для логнормального распределения среднее значение потерь всегда больше медианы:  $x_{\text{med}} = \$9$  млн.;  $x_{\text{cp}} = \$10$  млн.

В качестве оценок параметров логнормального распределения  $\mu$  и  $\sigma$  можно принять:

$$\underline{\mu} = \ln \underline{x};$$

$$\underline{x} = \left( \prod_{i=1}^k x_i \right)^{1/k};$$

$$\underline{\sigma}^2 = \left\{ \sum_{i=1}^k (\ln x_i - \ln \underline{x})^2 \right\} / k,$$

где  $x_i, i = 1, 2, \dots, k$  – выборка потерь размером  $k$ .

**Размер ожидаемого убытка EL** (ожидаемых потерь в год) определяется соотношением:

$$EL = E(n) \cdot E(x),$$

где  $E(n)$  – математическое ожидание числа негативных событий (числа случаев потерь);  $E(x)$  – математическое ожидание величины потерь на одно негативное событие. В качестве оценки  $E(n)$  для закона Пуассона принимается  $\lambda_{\text{ср}}$ , т.е. величина  $\lambda$ , усреднённая на интервале времени  $T = 5$  лет; а в качестве оценки  $E(x)$  – средняя величина потерь  $x_{\text{ср}}$  за тот же интервал времени.

Размер ожидаемого убытка EL связан с индикатором подверженности операционному риску EI соотношением:

$$EL = PE \cdot LGE \cdot EI.$$

**Индикатор подверженности операционному риску EI** выбирается, исходя из анализа бизнес-процессов предприятия. Общая формула для расчёта EI имеет вид:

$$EI = k \cdot \text{Ind},$$

где в качестве индикатора Ind рассматриваются [28] валовой доход, зарплата служащих, объём материальных активов и др.;  $k$  – коэффициент нормировки, вычисляемый из соотношения

$$PE \cdot LGE \cdot k \cdot \text{Ind} = \lambda_{\text{ср}} \cdot x_{\text{ср}}.$$

**Размер непредвиденного убытка UL** (непредвиденных потерь) рассчитывается на основе соотношения:

$$UL = F_z^{-1}(0,999) - EL,$$

где  $F_z$  – функция распределения совокупных годовых потерь;  $F_z^{-1}$  – функция обратная  $F_z$ . На рис. 3.4 приведён пример функции распределения совокупных годовых потерь; на этом же рисунке показаны ожидаемые потери, которые равны \$100 млн.

На практике [29, 30] размер непредвиденного убытка UL вычисляют по результатам моделирования (методом Монте-Карло). В этом случае делается предположение о логнормальном распределении потерь или двух параметрическом распределении Вейбулла [30]. По результатам моделирования определяют коэффициенты непредвиденных убытков  $\gamma$ , устанавливающие связь UL и EL для каждой бизнес-линии:

$$UL = \gamma EL.$$

### Распределение совокупных годовых потерь

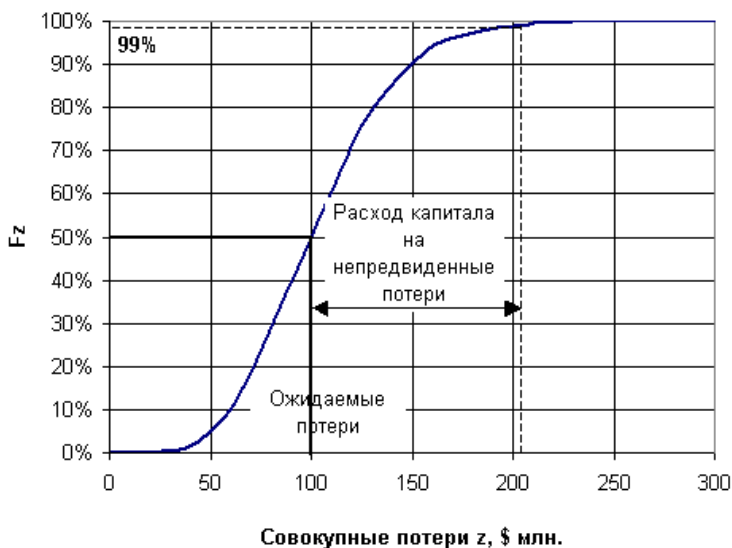


Рис. 3.4. Пример функции распределения совокупных годовых потерь

Для использования коэффициентов  $\gamma$  в повседневной практике в странах ЕС, например, необходимо получить разрешение надзорного органа. Возможно, на предприятиях «Росатома» значения этих коэффициентов будут установлены нормативно.

### 3.4. Экспертная оценка операционного риска с применением структурных и логических моделей

Под методикой экспертной оценки операционного риска с применением структурных и логических моделей следует понимать алгоритм принятия решений о степени рискованности направлений деятельности (бизнес-линий), составляющих их бизнес-процессов и отдельных бизнес-функций.

В системе оценок ОР, основанной на рейтинговой модели, должны присутствовать *определенные ключевые признаки*:

- применение внутренних и внешних *статистических данных* по случаям убытков и величинам потерь;

- использованы *субъективные суждения экспертов* о вероятности и масштабах убытков с учётом значимости факторов риска, воздействующих на бизнес-процесс.

Статистические данные по потерям должны накапливаться в базе данных по рискам предприятия и использоваться для верификации рейтинговой модели. Что же касается субъективных суждений экспертов о рискованности процесса, их отражает элемент рейтинговой модели, называемый *показателем операционного риска* (ПОР), то они должны использоваться для валидации процессов. Уровень ПОР может быть оценен экспертом с применением математического аппарата нечёткой логики (Fuzzy Logic) [31].

### 3.4.1. Понятия и определения Fuzzy Logic

**Нечеткая логика (Fuzzy Logic)** – раздел современной математической логики, в основе которой лежат операции сложного высказывания, определенные на нечетких множествах.

**Нечеткое множество  $A$**  – множество элементов  $x$  вместе с определенными на нем функциями принадлежности  $\mu(x)$ , т.е.

$$A = \{x, \mu(x)\},$$

$x$  принадлежит универсальному множеству  $E$ .

**Функция принадлежности** – характеристическая функция, областью определения которой является универсальное множество  $E$ , а областью значений – интервал  $[0,1]$ . Пример функций принадлежности фактора риска  $x$ , для нечетких множеств типа «низкий», «средний», «высокий» приведён на рис. 3.5.

**Логические правила** – формализованные высказывания, составленные на основе символов и логических операций.

**Импликация** – логическая операция, близкая по смыслу высказыванию «из  $A$  следует  $B$ ».

**Логическая модель** – нечеткая математическая модель, определяющая функции принадлежности входных и выходных величин, логические правила их обработки и алгоритм формирования выходных величин.

**Агрегирование результатов импликаций** – операция построения функции принадлежности выходной переменной в логической модели.



Рис. 3.5. Пример функций принадлежности

**Дефазификация** – метод выделения единственного значения выходной переменной логической модели из множества возможных значений по её функции принадлежности.

Математический аппарат нечёткой логики позволяет описывать нечёткие понятия и знания, оперировать этими знаниями, делать выводы. Нечёткая логика даёт эксперту средства отображения неопределённостей и неточностей описания реальных моделей бизнес-процессов, факторов операционного риска. Но самое главное даёт в руки риск-менеджеров адекватный аппарат повторных воспроизведений показателя операционного риска, даже если состав группы экспертов был полностью заменён по тем или иным причинам.

### 3.4.2. Двухгрупповая классификация операционного риска для проведения экспертных оценок

Для оценки ПОР с применением аппарата нечёткой логики целесообразно классифицировать операционный риск на два типа:

- технологический риск;
- риск случайных негативных событий.

Источники воздействия, характеризующие технологический риск:

- неотлаженность технологических процессов (управление проектом);

- неполная или задержанная управленческая информация (управление процессами);
- несовершенство методик и моделей анализа (управление процессами);
- изменения, связанные с внедрением, функционированием и модернизацией технических и информационных систем (управление проектом, управление процессами);
- несогласованность или отсутствие взаимодействия подразделений предприятия на уровне организации бизнес-процессов (управление процессами);
- несовершенство механизмов реализации отдельных бизнес-функций и всего бизнес-процесса, недостатки контроля (управление процессами).

Источники воздействия, характеризующие риск случайных негативных событий:

- непреднамеренные ошибки;
- внутренние злоупотребления;
- внешнее воздействие (вмешательство регулирующих органов, введение новых нормативных требований и др.);
- отказы технологического оборудования;
- конфликты трудовых отношений и безопасность труда;
- нанесение ущерба материальным активам;
- катастрофы (пожары, наводнения, террористические акты и т.п.).

Факторы риска, и индикаторы состояния внутренней операционной среды, выделяются экспертом при структурном анализе бизнес-процессов. Они включают группы факторов входящей, выходящей информации и воздействий на механизм реализации бизнес-процесса.

Значимость каждого фактора, входящего в соответствующую группу, оценивается экспертом в баллах (например, от 1 до 10) по характеристическим признакам в соответствии с источниками воздействия на технологический риск и риск случайных негативных событий.

Вычисление степени воздействия нескольких факторов на оценку показателя операционного риска и сама оценка производится в

соответствии с логическими правилами, которые формируются экспертом при анализе конкретного бизнес-процесса. В результате анализа логической модели вычисляется показатель операционного риска ПОР, значения которого лежат в интервале от 0 до 1.

### 3.4.3. Модели и алгоритмы нечёткого вывода

Методика экспертной оценки ОР предполагает последовательное решение пяти основных задач анализа:

1) выделение перечня учитываемых факторов, влияющих на рискованность каждой составляющей операции или бизнес-функции (БФ);

2) определение функций принадлежности для каждого учитываемого фактора;

3) построение правил логических операций, преобразующих характеристики выделенных факторов в нечеткие характеристики ОР.

4) построение алгоритма расчета ПОР для каждой БФ;

5) вычисление агрегированных показателей ПОР для бизнес-процессов и направлений деятельности (бизнес-линий) по значениям  $ПОР_i$  для отдельных  $БФ_i$  в соответствии с диаграммой дерева узлов;

Задачи 2–4 составляют основу логической модели оценки показателя операционного риска. Эта модель, по сути, устанавливает соответствие «балльной» и «вероятностной» шкал оценки ОР. Схема логической модели приведена на рис. 3.6.

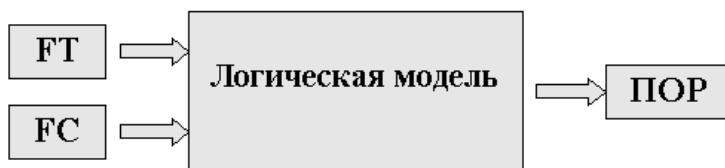


Рис. 3.6. Схема логической модели

**Выделение перечня учитываемых факторов.** Факторы оценки объектов функциональных блоков устанавливают связь между биз-

нес-функцией (БФ) и степенью подверженности БФ операционному риску. В модели структурного анализа объекты заданы стрелками (рис. 3.7). Перечень учитываемых факторов определяется эвристическим путем в соответствии с типом ОР и целиком зависит от профессионализма эксперта.

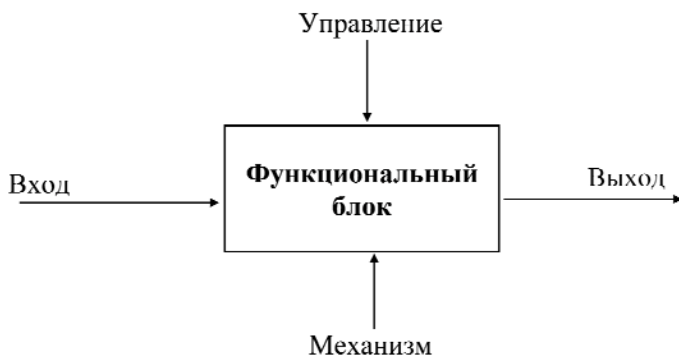


Рис. 3.7. Изображение функционального блока в стандарте IDEF0

При выделении перечня учитываемых факторов следует руководствоваться следующими положениями.

Все факторы, связанные с анализируемой БФ, следует разбить на четыре группы:

- факторы, воздействующие на входящую информацию;
- факторы, воздействующие на выходящую информацию;
- факторы, влияющие на управление БФ;
- факторы, воздействующие на механизм реализации БФ.

Внутри каждой группы формируются факторы технологической и событийной оценки.

**Определение функций принадлежности.** Все выделенные факторы технологической и событийной оценки являются входными величинами логической модели ОР. Выходной величиной является оценка ПОР.

За каждой входной величиной и результатом логических операций на входных величинах ПОР необходимо закрепить соответствующие функции принадлежности (ФП) нечетких множеств. Например, если область изменения выделенного фактора лежит в



диапазоне от 0 до 10 баллов, то область значений функции принадлежности этого фактора должна лежать между 0 и 1.

Все входные величины и ПОР предлагается оценивать в двух метриках: «грубой» и «точной». Грубую оценку следует применять для факторов с большой неопределенностью, о которых имеется крайне мало информации. Точная оценка принимается во всех остальных случаях.

Грубая оценка фактора и его влияние на ОР может быть описана следующими лингвистическими терминами: «низкий», «средний», «высокий». Терму «низкий» соответствует малый уровень риска.

Точная оценка фактора описывается терминами: «низкий», «ниже среднего», «средний», «выше среднего», «высокий».

Соответствующая оценка ПОР описывается терминами: «низкий», «умеренный», «значительный», «высокий».

Каждому из указанных лингвистических термов соответствует определённая ФП. Выбор типа ФП остается за экспертом.

Пример задания функций принадлежности для грубой оценки фактора приведен на рис. 3.5, а для точной – на рис. 3.8.



Рис. 3.8. Пример функций принадлежности в «точной метрике»

**Правила логических операций.** Построение логических операций производится в соответствии с методологией Fuzzy Logic [31, 32].

Конструкции на языке Fuzzy Logic строятся для всех выделенных факторов технологической и событийной оценки. Используются конструкции следующих типов:

IF FT IS «ниже среднего» OR FC «низкий» THEN ПОР = «низкий»,

IF FT IS «выше среднего» AND FC «низкий» THEN ПОР = «умеренный»,

где FT и FC – выделенные факторы технологической и событийной оценки риска; ПОР –показатель операционного риска; IF, IS, OR, AND, THEN – операторы языка Fuzzy Logic.

Система правил логических операций конструируется для всех комбинаций лингвистических термов, используемых в «грубой» и «точной» метрике.

**Алгоритм расчета ПОР.** В алгоритм расчета ПОР для оцениваемой БФ входят следующие операции.

1. Оценка экспертом выделенных факторов в выбранных им лингвистических терминах на основе *признаков*, сформированных для факторов технологической и событийной оценки.

2. Расчет индикаторов влияния технологических и событийных факторов на ПОР в 10 балльной шкале по формулам

$$FT = n; \quad FC = m,$$

где  $n$  и  $m$  – количество выявленных признаков для оценки технологических и событийных факторов риска соответственно (например,  $n = 3$ , если эксперт дал три ответа «Да» на вопросы анкеты). Примеры анкет для оценки индикаторов FT технологического и FC событийного риска приведены в табл. 3.1 и табл. 3.2.

3. Построение результатов импликаций в соответствии с матрицей соответствий для технологических и событийных факторов. Матрица соответствий для «точной» метрики имеет вид, приведённый в табл. 3.3. «Грубая» оценка производится на основе матрицы соответствий, представленной в табл. 3.4.

Примеры шкал «точной» и «грубой» оценки ПОР приведены в табл. 3.5 и табл. 3.6.

Таблица 3.1

### Оценка индикаторов технологического риска

№ п/п	Вопрос для оценки фактора	Да = 1 Нет = 0
1	Является ли НЕДОСТОВЕРНОЙ или НЕПОЛНОЙ входная и выходная информация БФ?	
2	Является ли БФ для исследуемого бизнес-процесса НОВОЙ или НЕ ДО КОНЦА ОТРАБОТАННОЙ?	
3	Часто ли входные и выходные объекты БФ подвергаются технологическим ИЗМЕНЕНИЯМ (модернизациям)?	
4	Являются ли входные или выходные объекты БФ СЛОЖНЫМИ, многокомпонентными, обладающими большим информационным объемом или трудно контролируемые?	
5	Являются ли НЕКАЧЕСТВЕННЫМИ применяемые модели и методики, лежащие в основе реализации БФ?	
6	Осуществляется ли КОНТРОЛЬ при выполнении БФ?	
7	Правда ли, что используемое оборудование НЕНАДЁЖНО или устарело?	
8	Осуществляется ли обработка данных преимущественно вручную (БФ НЕАВТОМАТИЗИРОВАНА)?	
9	Используется ли в механизме реализации БФ устаревшее или НЕКАЧЕСТВЕННОЕ программное обеспечение?	
10	Участвуют ли в реализации БФ сотрудники без должной КОМПЕТЕНЦИИ и ответственности?	

Таблица 3.2

### Оценка индикаторов событийного риска

№ п/п	Вопрос для оценки фактора	Да = 1 Нет=0
1	Возможны ли НЕКВАЛИФИЦИРОВАННЫЕ или ЗЛОУМЫШЛЕННЫЕ действия персонала при реализации БФ?	
2	Возможен ли НЕСАНКЦИОНИРОВАННЫЙ доступ к источникам информации или оборудованию?	
3	Существует ли зависимость от «НЕЗАМЕНИМЫХ» исполнителей?	
4	Часто ли происходят ОТКАЗЫ оборудования в механизмах реализации БФ?	

№ п/п	Вопрос для оценки фактора	Да = 1 Нет=0
5	Чувствительна ли БФ к последствиям УТРАТЫ в результате аварий и катастроф?	
6	Зависит ли реализация БФ от НЕКОРРЕКТНЫХ или устаревших внутренних документов?	
7	Были ли случаи несоблюдения НОРМ поведения при взаимодействии с коллегами по работе?	
8	Имело ли место ВНЕШНЕЕ ВОЗДЕЙСТВИЕ на механизм реализации БФ?	
9	Имели ли место случаи НЕВЫПОЛНЕНИЯ СЛУЖЕБНЫХ обязанностей?	
10	Случались ли у вас КРАЖИ в подразделении?	

Таблица 3.3

**Матрица соответствий оценки факторов FT и FC  
для «точной метрики»**

FT	FC		
	Низкий	Средний	Высокий
<b>Низкий</b>	ПОР=низкий	ПОР=низкий	ПОР=умеренный
<b>Ниже среднего</b>	ПОР=низкий	ПОР=низкий	ПОР=умеренный
<b>Средний</b>	ПОР=умеренный	ПОР=умеренный	ПОР=умеренный
<b>Выше среднего</b>	ПОР=умеренный	ПОР=значительный	ПОР=значительный
<b>Высокий</b>	ПОР=значительный	ПОР=высокий	ПОР=высокий

Таблица 3.4

**Матрица соответствий оценки факторов FT и FC  
для «грубой метрики»**

FT	FC		
	Низкий	Средний	Высокий
<b>Низкий</b>	ПОР=низкий	ПОР=низкий	ПОР=умеренный
<b>Средний</b>	ПОР=умеренный	ПОР=умеренный	ПОР=умеренный
<b>Высокий</b>	ПОР=умеренный	ПОР=высокий	ПОР=высокий

Таблица 3.5

**Шкала оценки операционного риска («точная метрика»)**

Диапазон риска	0–25 %	26–50 %	51–75 %	76–100 %
Терм ПОР	Низкий	Умеренный	Значительный	Высокий

Таблица 3.6

**Шкала оценки операционного риска («грубая метрика»)**

Диапазон риска	0–25 %	26–50 %	51–100 %
Терм ПОР	Низкий	Умеренный	Высокий

Пример результатов импликаций для 13 правил логического вывода показан на рис. 3.9. В первой колонке на рисунке приведены «усечённые функции принадлежности для индикатора  $FT = 4$ , во второй колонке – аналогичные ФП для индикатора  $FC = 2$ , а в третьей колонке – результаты импликаций. Уровни «отсечения» для каждого из правил осуществляются с использованием операции МИНИМУМ. Этот результат показан заштрихованными фигурами в третьей колонке (строки 1–13).

4. Агрегирование результатов импликаций в соответствии с правилами логических операций.

Агрегирование результатов импликаций в соответствии с алгоритмом Mamdani (с использованием операции МАКСИМУМ [31]) показан в последней строке третьего столбца на рис. 3.9.

5. Дефазификация результатов агрегирования результатов импликаций в выбранном формате оценки ПОР (числовом или процентном).

Фактически, дефазификация является операцией приведения к чёткости операции нечёткого вывода и получение чёткого значения ПОР. На рис. 3.9, например, согласно алгоритму Mamdani чёткое значение  $ПОР = 0,299$  получено центроидным методом [31].

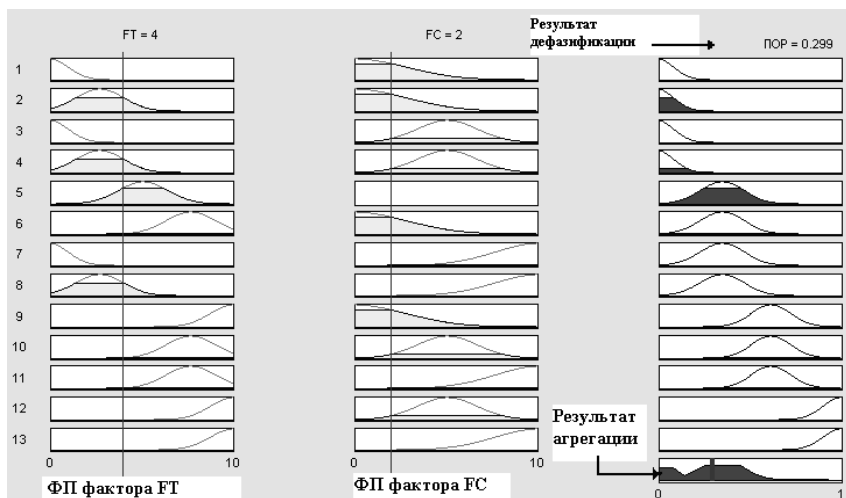


Рис. 3.9. Пример нечёткого логического вывода для двухфакторной модели

**Агрегирование показателей операционного риска.** Вычисление агрегированных показателей ПОР бизнес-процесса по значениям  $ПОР_i$  для совокупности  $i = 1, 2, \dots, k$  бизнес-функций производится в соответствии с формулой

$$ПОР = w_1 \times ПОР_1 + w_2 \times ПОР_2 + \dots + w_k \times ПОР_k,$$

где  $w_i$  – вес  $i$ -го операционного риска;  $ПОР_i$  – показатель операционного риска  $i$ -й БФ. Веса  $w_i$  назначаются экспертом в соответствии со значимостью  $ПОР_i$  для рассматриваемого бизнес-процесса и с учетом того, что  $w_1 + w_2 + \dots + w_k = 1$ .

Вычисление агрегированных показателей ПОР для бизнес-линий производится аналогично вычислению агрегированных показателей ПОР для бизнес-процессов.

**Экспертная оценка весов БФ.** Экспертная оценка весовых коэффициентов  $w_i$  производится в два этапа.

*Этап 1.* Выбор «соразмерного» числа экспертов  $N$ . Согласно [25] минимальное число экспертов определяется соотношением

$$N > q^2(a)(D^2/F^2),$$

где  $N$  – число экспертов;  $q(a)$  – квантиль нормального распределения; для ошибки  $a = 5\%$  –  $q(a) = 1,96$ ;  $D^2$  – дисперсия оценки;  $F^2$  –

допустимое отклонение полученных оценочных значений (от значений при  $N \rightarrow \infty$ ). При  $D^2/F^2 = 1$

$$N > 1 \cdot (1,96)^2 = 3,84 \sim 4 \text{ чел.}$$

*Этап 2.* «Балльная» оценка «значимости» БФ и вычисление весов. «Значимость» каждой БФ, с точки зрения операционного риска, оценивается каждым экспертом в баллах, например от 1 до 5, а затем вычисляются коэффициенты  $w_i$ . Пример экспертных оценок коэффициентов  $w_i$  для  $N = 4$  приведён в табл. 3.7.

Таблица 3.7

### Пример экспертных оценок

Участники экспертизы	Балл БФ <sub>1</sub>	Балл БФ <sub>2</sub>	Балл БФ <sub>3</sub>	Сумма
Эксперт 1	3	5	4	12
Эксперт 2	2	4	4	10
Эксперт 3	3	4	5	12
Эксперт 4	2	5	4	11
Балл БФ <sub>i</sub> /Сумма				
Эксперт 1	0,25	0,42	0,33	1,00
Эксперт 2	0,20	0,40	0,40	1,00
Эксперт 3	0,25	0,33	0,42	1,00
Эксперт 4	0,18	0,45	0,36	1,00
Сумма	0,88	1,60	1,51	4,00
$w_i = \text{Сумма}/N$	0,22	0,40	0,38	1,00

### 3.5. Расчёт ожидаемых потерь бизнес-процесса методом ФСА

Ожидаемые потери бизнес-процесса оцениваются на основе функционально стоимостного анализа (ФСА) структурной модели процесса и значений показателей операционного риска, рассчитанных для каждой из бизнес-функций структурной модели.

Для оценки ожидаемых потерь бизнес-процесса, входящего в состав определённой бизнес-линии, применим комбинацию «затратного подхода» [33] и подхода АМА оценки операционного

риска [23, 24]. В этом случае ожидаемые потери бизнес-линии от операционного риска можно вычислить по формуле

$$EL = \text{ПОР} \cdot \text{LGE} \cdot k \cdot Z$$

где  $k \cdot Z = EI$  – индикатор подверженности операционному риску;  $Z$  – совокупность затрат, связанных с поддержанием работоспособности и управлением бизнес-линии; ПОР – агрегированный по бизнес-функциям показатель операционного риска бизнес-линии; LGE – уровень потерь бизнес-линии. Коэффициент  $k$  – коэффициент нормировки, вычисляемый из соотношения

$$\text{ПОР} \cdot \text{LGE} \cdot k \cdot Z = \lambda_{\text{ср}} \cdot x_{\text{ср}}$$

где  $\lambda_{\text{ср}}$  – среднее число негативных событий (случаев потерь) в год;  $x_{\text{ср}}$  – средние потери на одно негативное событие для рассматриваемой бизнес-линии.

Совокупность затрат  $Z$  является характеристикой себестоимости технологических процессов бизнес-линии, которая, в соответствии с методологией ФСА определяется как сумма трёх составляющих [34]:

$$Z = \text{ПР} + \text{КР} + \text{ОБР},$$

где ПР – прямые расходы; КР – косвенные расходы; ОБР – общие расходы.

*Прямые расходы* – затраты, непосредственно связанные с поддержанием работоспособности бизнес-линии. К прямым расходам относится суммарный фонд материального вознаграждения сотрудников, непосредственно исполняющих технологические операции в процессах, и стоимость технического оснащения их рабочих мест с учетом амортизации оборудования.

*Косвенные расходы* – затраты участников технологических процессов, не связанные непосредственно с исполнением технологических операций основной деятельности, включая представительские, командировочные и расходы, услуги сторонних организаций, транспортные, почтовые и т.п.

*Общие расходы* – затраты (сметные расходы, включая суммарный фонд материального вознаграждения и амортизацию технического оснащения менеджеров), относящихся к функциональной зоне «управление» и «общехозяйственные расходы» предприятия.



Если ввести допущение, что значения коэффициентов  $k$  и LGE постоянны для всех бизнес-функций, входящих в состав модели бизнес-процесса, то величина ожидаемых потерь  $EL_{\text{БП}}$  бизнес-процесса (БП) рассчитывается по формуле:

$$EL_{\text{БП}} = k \cdot LGE \cdot \sum_j^n (w_j \cdot \text{ПОР}_j \cdot Z_j),$$

где  $w_j$  – веса бизнес-функций (БФ), входящих в БП, причем  $w_1 + w_2 + \dots + w_n = 1$ ,  $n$  – число БФ;  $\text{ПОР}_j$  – показатель операционного риска  $j$ -й БФ;  $Z_j$  – затраты на выполнение отдельной БФ, входящей в анализируемый бизнес-процесс. Величины  $w_j$  и  $\text{ПОР}_j$  вычисляются с применением экспертных методов, описанных ранее, а величины  $Z_j$  – методами ФСА.

Значения  $Z_j$  и  $Z$  (как и оценки  $EL_{\text{БП}}$  и  $EL$ , согласно рекомендациям Базельского комитета) вычисляются на отчётном периоде  $T = 1$  год. Величины  $Z_j$  для  $j$ -й БФ могут быть вычислены, например, по методике, изложенной в работе [35]. В соответствии с этой методикой разнесение затрат БП по бизнес-функциям может быть произведено пропорционально доле времени  $t_j/t_{\text{БП}}$ , где  $t_j$  – затраты времени на выполнение  $j$ -й БФ;  $t_{\text{БП}}$  – затраты времени на выполнение всех БФ, входящих в структурную модель бизнес-процесса. Это не единственный способ разнесения затрат. Например, в работе [34] предлагается затраты разносить пропорционально доле служащих, занятых обслуживанием отдельной бизнес-функции.

Рассмотренный синтетический подход к оценке операционного риска предполагает, что уровень риска можно оценить на основе анализа информации, собираемой на уровне бизнес-линий, бизнес-процессов и отдельных бизнес-функций. Модели обработки информации могут опираться на комбинации самых разнообразных методов – от статистических методов до экспертных оценок уровня зрелости процессов и систем.

## Вопросы и ответы

**Вопрос.** Какой вид статистического распределения для случаев потерь следует использовать в расчётах операционного риска?

**Ответ.** Трудно дать однозначный ответ, поскольку каждое предприятие имеет свои особенности и присущую только ему

внутреннюю статистику потерь. Только математический аппарат проверки статистических гипотез позволяет «грамотно» ответить на этот вопрос. Но определённые рекомендации дать можно. В рабочих материалах Базельского комитета чаще всего применяются распределение Пуассона и биномиальное распределение для случайной величины, которую называют терминами: «число случаев потерь» или «число негативных событий». Распределение Пуассона имеет вид:

$$h(n) = (\lambda t)^n / n! e^{-\lambda t}, \quad n = 0, 1, 2, \dots$$

где  $h(n)$  – вероятность того, что  $n$  негативных событий (случаев потерь) произойдёт на интервале времени  $t$ ;  $\lambda$  – средняя частота негативных событий (случаев потерь) на заданном интервале времени.

Базельским комитетом принято оценивать операционный риск на интервале в 1 год. Поэтому в выше приведённом выражении следует положить  $t = 1$  и  $\lambda$  оценивать средним числом негативных событий в год.

Часто применяется биномиальное распределение следующего вида [26,30]:

$$h(n) = \binom{a+n-1}{n} \left( \frac{1}{1+b} \right)^a \left( \frac{b}{1+b} \right)^b,$$

где  $a$  и  $b$  – параметры распределения;  $\binom{a+n-1}{n}$  – число комбинаций.

Биноминальное распределение даёт результат, который неплохо согласуется с имеющимися статистическими данными. Что же касается распределения Пуассона, то оно плохо «работает» при больших значениях  $\lambda$ .

**Вопрос.** А как рассчитать число комбинаций? Приведите пример расчета случаев потерь  $h(n)$ .

**Ответ.** Давайте рассмотрим случай  $n = 1$ ,  $a = 4$ ,  $b = 5$ . Число комбинаций определяется следующим образом:

$$\binom{a+n-1}{n} = \binom{4}{1} = \frac{4!}{1 \times (4-1)!} = \frac{1 \times 2 \times 3 \times 4}{1 \times (1 \times 2 \times 3)} = 4.$$

Сомножители:

$$\left(\frac{1}{1+b}\right) = \frac{1}{1+5} = 0,167; \quad \left(\frac{b}{1+b}\right) = \frac{5}{1+5} = 0,833.$$

Тогда  $h(n) = 4 \times (0,167)^4 \times 0,833 = 0,003$ .

**Вопрос.** Вероятность случаев потерь и вероятность потерь разве не одно и то же?

**Ответ.** Нет, не одно и то же. Когда мы говорим о вероятности **случаев** потерь, то имеем в виду статистическую оценку, связанную со случайным процессом «произошло или не произошло негативное событие», сколько произошло таких событий в год. А вероятность потерь связана с **величиной** потерь. То есть мы оцениваем вероятность убытка в денежном выражении меньше заданного значения. Например, **вероятность потерь** менее 0,5 миллионов Евро равна 0,3 для статистических данных, представленных на рис. 3.3, а **вероятность случаев потерь**  $n < 5$  в год равна 0,034 (см. рис. 3.2).

**Вопрос.** Можете на простом примере показать, как рассчитать вероятность потерь для бизнес – процесса?

**Ответ.** К сожалению, в решении сложной проблемы «простого примера» быть не может. Тем не менее, давайте рассмотрим пример расчёта вероятности потерь в диапазоне от 1 до 2 млн. долларов. При этом будем учитывать реальное обстоятельство, что статистика собиралась при условии превышения потерь величины в 1 млн. долларов. И, конечно же, постараемся максимально упростить вычисления. Для расчета воспользуемся следующей формулой для «усечённой» плотности распределения [36]:

$$f(x| x > u) = f(x) \cdot G(x) / \int f(x) \cdot G(x) dx,$$

где  $f(x) = \exp(-x/b)/b$ ,  $G(x) = 1 / [1 + \exp(-\beta(x - \tau))]$ ,  $x = \ln(X) - \ln(U)$ ,  $U$  – порог «усечения» равный 1 млн. долларов;  $X$  – величина потерь в миллионах долларов;  $u = \ln(U)$ ;  $\int f(x) \cdot G(x) dx = Nf$  – нормировка

распределения. Значения параметров  $b$ ,  $\beta$ ,  $\tau$  для бизнес-линии возьмем из приведенной выше работы:  $b = 0,72$ ;  $\beta = 0,76$ ;  $\tau = 3,98$ .

Сначала разобьем диапазон изменения  $X$  на интервалы:

$X$ , млн. долл.	1–2	2–5	5–10	10–20	20–30	30–40	40–50	>100
------------------	-----	-----	------	-------	-------	-------	-------	------

и найдём величины  $dX$

$dX$ , млн. долл.	1	3	5	10	10	10	10	50
-------------------	---	---	---	----	----	----	----	----

Затем в верхних границах интервалов рассчитаем значения  $f(x) \cdot G(x)$ :

$f \cdot G$	0,040	0,021	0,012	0,007	0,005	0,004	0,003	0,001
-------------	-------	-------	-------	-------	-------	-------	-------	-------

Умножая на  $dX$  полученные значения и складывая результаты умножения, найдём приближённую оценку нормировки  $Nf$ :

$$Nf \approx 0,040 \cdot 1 + 0,021 \cdot 3 + 0,012 \cdot 5 + 0,007 \cdot 10 + 0,005 \cdot 10 + 0,004 \cdot 10 + 0,003 \cdot 10 + 0,001 \cdot 50 = 0,421.$$

Тогда искомая величина вероятности потерь в диапазоне от 1 до 2 миллионов долларов будет равна

$$f \cdot G \cdot dX / Nf = 0,040 \cdot 1 : 0,421 = 0,095.$$

**Вопрос.** Можно ли рассчитать LGE, если отсутствует информация по функциям распределения потерь?

**Ответ.** Нет. Можно лишь дать ориентировочную оценку. Например, уровень потерь LGE для «среднестатистического» предприятия можно приблизительно оценить, воспользовавшись данными по коэффициентам восстановления  $R$  [28]. Для операционного риска принимается модель, аналогичная кредитному риску:

$$LGE = 1 - R.$$

Коэффициент восстановления  $R$  определяется, как полное количество возвратов, включая страхование и «другие» возвраты в случае реализации операционного риска.

**Вопрос.** Как оценить вероятность проявления негативного события, с точки зрения реализации операционного риска, не в течение года, а предположим, в течение рабочего дня? Ведь опубликованная статистика приводится на интервале в 1 год?

**Ответ.** Давайте рассмотрим пример расчета вероятности того, что произошло одно негативное событие для заданной бизнес-линии. Величину средней частоты негативных событий  $\lambda$  примем равной 57,7 событий в год [28];  $t = 8$  ч. Для расчета вероятности воспользуемся распределением Пуассона для случая  $n = 1$ . При малых значениях  $\lambda t$  искомая вероятность будет

$$h(1) \approx \lambda t = 57,7 \cdot 8 : 365 : 24 = 0,05.$$

**Вопрос.** Как на практике осуществляется экспертная оценка уровня операционного риска? Приведите пример использования методики экспертной оценки.

**Ответ.** Применение методики экспертной оценки уровня операционного риска рассмотрим на примере аттестации зрелости бизнес-процессов, относящихся к сфере информационных технологий (ИТ) [37]. Аттестация проводилась на основе моделей бизнес-процессов в соответствии со стандартом ГОСТ Р ИСО/МЭК 15504, а оценка зрелости БП оценивалась по величине показателя операционного риска (ПОР) в соответствии с принципом: чем выше уровень ПОР, тем ниже уровень зрелости БП.

Схема алгоритма анализа бизнес-процессов была разбита на три последовательных этапа:

*Этап 1.* Моделирование:

- построение эталонной модели (описание измерения «процесс», измерение «зрелости» процесса);
- подготовка анкет для экспертной оценки ПОР по каждой бизнес-функции процесса.

*Этап 2.* Аттестация:

- создание группы экспертов для аттестации БП и сбор ответов на вопросы анкет;
- обработка анкет и оценка ПОР БФ;
- определение средней оценки ПОР по каждой БФ и всему БП;
- определение уровня «зрелости» процесса по средним значениям ПОР.

*Этап 3.* Документирование: представление результатов аттестации в виде отчёта и выдача рекомендаций по совершенствованию БП.

Эталонная модель, согласно ГОСТ Р ИСО/МЭК 15504, группирует процессы ИТ в три класса:

- основные;
- поддерживающие;
- организационные.

В данном примере практического применения методики уровни операционного риска оценивались только для основных процессов, которые включали:

- категорию *Заказчик – Поставщик* (в эталонной модели она получила спецификацию А11 «Приобретение необходимого ПО и оборудования (далее Продукта)»);

- *инженерную* категорию (А12 «Разработка ПО и эксплуатация»).

Перечень бизнес-функций (БФ), составляющих указанные бизнес-процессы, приведён в табл. 3.8.

Таблица 3.8

**Перечень анализируемых бизнес-процессов  
и составляющих их бизнес-функций**

Обозначение	Наименование БП	Составляющие БП бизнес-функции
A11	Приобретение необходимого ПО и оборудования (Продукта)	<p>Определение потребностей. Определение требований к Продукту. Подготовка стратегии приобретения. Заключение и поддержка договора. Приёмка Продукта и управление потребностями Заказчика</p>
A12	Разработка ПО и эксплуатация	<p>Анализ системных требований. Разработка требований к ПО. Разработка ПО. Интеграция и тестирование системы. Эксплуатация системы и ПО</p>

На рис. П2.1 и П2.2 в приложении 2 представлены структурные модели анализируемых процессов с описанием входов, выходов и управлений, воздействующих на соответствующие БФ.

Измерение зрелости процесса. Зрелость процесса (его качество) определяется числовым значением ПОР, которому соответствует определённый уровень зрелости. Согласно ГОСТ Р ИСО/МЭК 15504 и ГОСТ Р ИСО/МЭК 12207 повышение уровня зрелости представляет собой рациональный путь прогрессивного улучшения любого процесса. Пусть внутренняя модель предприятия, опирающаяся на указанные стандарты, регламентирует 6 уровней зрелости:

*Уровень 0 (неполный):* в целом БП (или БФ) не соответствует своему назначению; значения ПОР лежат в диапазоне (1,00 – 0,80).

*Уровень 1 (выполняемый):* в целом БП (или БФ) соответствуют своему назначению, но его выполнение не может быть строго запланировано и отслежено; значения ПОР лежат в диапазоне (0,79 – 0,60).

*Уровень 2 (управляемый):* БП (или БФ) даёт рабочие продукты в соответствии с определёнными процедурами, а также планируется и отслеживается; значения ПОР лежат в диапазоне (0,59 – 0,40).

*Уровень 3 (устоявшийся):* реализации БФ процесса используют для получения заданного показателя результата (т.е. заданного уровня ПОР), приняты и адаптированы к конкретной ситуации стандартного и полностью документированного процесса; значения ПОР лежат в диапазоне (0,39 – 0,21).

*Уровень 4 (предсказуемый):* реализован постоянный мониторинг БП (и каждой отдельной БФ), процесс полностью регламентирован; значения ПОР лежат в диапазоне (0,20 – 0,10).

*Уровень 5 (оптимизируемый):* устанавливаются количественные ориентиры (цели) по эффективности БП и каждой БФ; осуществляется постоянный мониторинг продвижения процесса к этим целям, основывающийся на количественной обратной связи; значения ПОР < 0,10.

Согласно приведенной в п. 3.4 методике значения ПОР рассчитываются с учётом факторов FT технологической и FC событийной оценок риска по результатам анкетирования. Пример анкеты и ре-

зультаты ответов Эксперта для БФ «Определение требований к Продукту» приведены в табл. П2.1 и П2.2 приложения 2.

В рассматриваемом примере при расчёте ПОР применялась упрощенная модель. Суть «упрощения» состояла в том, что нечёткая логическая модель была заменена простой таблицей, привязанной к значениям индикаторов FT и FC, оцениваемым экспертом по 10-балльной шкале. Это удалось сделать в результате проведения многочисленных экспериментов с нечёткой логической моделью. Таблица для расчёта значений ПОР по индикаторам FT и FC (10-ти балльная шкала) представлена на рис. 3.10.

10	0,329	0,333	0,353	0,409	0,465	0,511	0,575	0,672	0,741		
9	0,315	0,319	0,341	0,395	0,453	0,508	0,573	0,672	0,731		
8	0,267	0,272	0,295	0,353	0,434	0,508	0,570	0,672	0,712		
7	0,210	0,215	0,263	0,335	0,434	0,505	0,565	0,672	0,710		
6	0,175	0,183	0,252	0,335	0,431	0,502	0,558	0,656	0,682		
5	0,142	0,171	0,248	0,335	0,423	0,498	0,546	0,620	0,641		
4	0,129	0,169	0,244	0,333	0,414	0,480	0,530	0,570	0,572		
3	0,094	0,151	0,242	0,325	0,374	0,414	0,460	0,506	0,540		
2	0,089	0,147	0,232	0,274	0,320	0,373	0,434	0,487	0,532		
1											
0											
	0	1	2	3	4	5	6	7	8	9	10

Рис. 3.10. Таблица для расчёта значений ПОР по индикаторам FT и FC (10-ти балльная шкала)

В примере, приведённом в табл. П2.1 приложения 2, значение  $FT = 4$ ,  $FC = 2$ . Тогда, используя рис. 3.10, находим значение  $ПОР = 0,325$ .

Результаты процесса аттестации бизнес-процессов. Аттестация проводилась группой экспертов (4 чел.) в соответствии с аудиторским заданием и документированными БП А11 и А12. Аудиторское задание содержало регламент для определения уровня зрелости



процессов по величине ПОР для всех бизнес-функций, составляющих А11 и А12. В качестве инструментального средства аттестации использовалась программа ВРwin и совмещённые с ней процедуры экспертной оценки операционного риска. Результаты аттестации представлены в табл. 3.9.

Таблица 3.9.

### Результаты аттестации бизнес-процессов А11 и А12

№	Наименование бизнес-процесса и составляющих его бизнес-функций	Эксперт 1 ПОР1, отн.ед.	Эксперт 2 ПОР2, отн.ед.	Эксперт 3 ПОР3 отн.ед.	Эксперт 4 ПОР4, отн.ед.	Среднее ПОР <sup>ср</sup> отн.ед.	Уровень зрелости
<b>А11</b>	<b>«Приобретение необходимого ПО и оборудования (Продукта)»</b>	<b>0,4</b>	<b>0,3</b>	<b>0,4</b>	<b>0,3</b>	<b>0,36</b>	<b>3</b>
1	Определение потребностей	0,3	0,4	0,6	0,4	0,43	-
2	Определение требований к Продукту	0,4	0,2	0,3	0,2	0,28	-
3	Подготовка стратегии приобретения	0,4	0,4	0,5	0,1	0,35	-
4	Заключение и поддержка договора	0,1	0,1	0,1	0,2	0,13	-
5	Приёмка Продукта и управление потребностями Заказчика	0,7	0,4	0,7	0,7	0,63	-
<b>А12</b>	<b>«Разработка ПО и эксплуатация»</b>	<b>0,5</b>	<b>0,2</b>	<b>0,6</b>	<b>0,4</b>	<b>0,43</b>	<b>2</b>
1	Анализ системных требований	0,4	0,2	0,5	0,4	0,38	-
2	Разработка требований к ПО	0,6	0,5	0,6	0,4	0,53	-
3	Разработка ПО	0,5	0,1	0,6	0,4	0,40	-
4	Интеграция и тестирование системы	0,2	0,1	0,5	0,5	0,33	-
5	Эксплуатация системы и ПО	0,6	0,1	0,6	0,5	0,45	-

Аттестация показала, что в целом:

1) процесс А11 «Приобретение необходимого ПО и оборудования (Продукта)» соответствует третьему уровню зрелости;

2) процесс А12 «Разработка ПО и эксплуатация» соответствует второму уровню зрелости.

Анализ выявил ряд бизнес-функций, которые имеют повышенный уровень ПОР:

- определение потребностей в программном обеспечении и оборудовании ИТ (ПОР<sub>ср</sub> = 0,43);
- приёмка программного обеспечения и оборудования ИТ (Продукта) и управление потребностями Заказчика (ПОР<sub>ср</sub> = 0,63);
- разработка требований к программному обеспечению (ПОР<sub>ср</sub> = 0,53);
- разработка программного обеспечения (ПОР<sub>ср</sub> = 0,40);
- эксплуатация системы и ПО (ПОР<sub>ср</sub> = 0,45).

Из приведённого примера следует, что менеджменту предприятия необходимо разработать комплекс мер, позволяющих понизить уровень операционного риска перечисленных бизнес-функций, и провести реструктуризацию соответствующих бизнес-процессов.

## Тесты для самоконтроля

1. Какая информация лежит в основе Усовершенствованных методов оценки операционного риска АМА?

- Внутренняя статистическая информация предприятия.
- Экспертные суждения.
- Внешние данные по отрасли.

2. Какие убытки должны учитываться при расчёте минимального размера капитала под операционный риск?

- Минимальный размер резервируемого капитала определяется с учётом непредвиденных убытков;
- Минимальный размер резервируемого капитала определяется суммой ожидаемых и непредвиденных убытков, если ожидаемые убытки не учтены сформированными резервами под потери.

3. Какова должна быть минимальная величина периода накопленных данных по случаям потерь для расчёта ORC в моделях АМА?

- Не менее 3 лет.
- Не менее 5 лет.
- Не менее 7 лет.

4. Правильным ли является следующее утверждение: размер ожидаемого убытка есть математическое ожидание годовых потерь равное произведению математического ожидания числа негативных событий (числа случаев потерь) на математическое ожидание величины потерь (на одно негативное событие)?

- Да.
- Нет.

5. Какое из следующих утверждений является справедливым?

- Среднее значение величины убытков больше медианы в случае принятия гипотезы о логнормальном распределении убытков.
- Среднее значение величины убытков равно медиане в случае принятия гипотезы о нормальном распределении убытков.
- Не знаю. Надо ещё проверить справедливость принятой гипотезы.

6. Зачем для оценки уровня показателей операционного риска (ПОР) применяют аппарат нечёткой логики?

- Чтобы запутать представителей надзорного органа при осуществлении проверок предприятия.
- Чтобы снизить отрицательное влияние «человеческого фактора» на результат оценки ПОР, получить согласованный по группе экспертов результат оценки и возможность передачи технологии экспертной оценки ПОР другим группам экспертов.
- Чтобы осуществить адекватное преобразование «балльной» шкалы оценки в «вероятностную» шкалу оценки ПОР.

7. Входами или выходами логической модели являются факторы технологической FT и событийной оценки FC?

- Входами.
- Выходами.

8. Как называется отношение, связывающее лингвистические оценки факторов FT и FC с лингвистическими оценками ПОР?

- Импликация.
- Дефазификация.
- Матрица соответствий.

9. Какое минимальное число экспертов может быть привлечено для аттестации бизнес-процессов?

- Три.
- Четыре.
- Пять.
- Семь.

10. Как называется индикатор EI (затратный подход + АМА), устанавливающий связь ожидаемых потерь бизнес-процесса с совокупностью затрат на этот процесс?

- Индикатор подверженности операционному риску.
- Индикатор общих расходов.
- Индикатор средних потерь на одно негативное событие.

## Раздел 4

---

### МОДЕЛИ ОПТИМИЗАЦИИ ТОиР ДЛЯ СТРУКТУРНЫХ КОМПОНЕНТ ОБОРУДОВАНИЯ АЭС С УЧЕТОМ ОПЕРАЦИОННОГО РИСКА

---

#### **Цель занятия:**

- демонстрация эффективности методики оптимизации ремонтного цикла компонент (элементов) оборудования АЭС на основе оценки рисков и инвестиционной составляющих стоимости цикла. Необходимость учёта операционного риска для минимизации затрат на проведение технического обслуживания и ремонтов (ТОиР).

#### **Вы научитесь:**

- применять методологию оптимизации обслуживания оборудования на основе оценки операционного риска и финансовом методе дисконтированного денежного потока;
- оценивать удельную восстановленную стоимость оборудования;
- строить модели вероятности отказа и модели уровня возможных потерь при отказе оборудования;
- применять рассмотренные модели на практике, например, для оценки длительности ремонтного цикла оборудования системы технического водоснабжения (СТВ АЭС).

#### **В программе занятия:**

- лекция, в которой представлено семейство моделей ремонтного цикла на основе оценки риска и показателей надёжности компонент оборудования и вычислительные процедуры, связанные с этими оценками.
- тесты для самоконтроля.

## **4.1. Модели оптимизации ремонтного цикла с учётом показателей надёжности оборудования, инвестиционной и рискованной составляющими стоимости цикла**

### **4.1.1. Применяемая методология, общесистемные предположения и замечания**

Теоретической базой моделей ремонтного цикла является методология оптимизации обслуживания на основе оценки риска. В качестве риска отказа компонент оборудования рассматривается операционный риск. Оценка качества операций обслуживания с учётом риска (выраженного в ожидаемых затратах) основана на стоимостном критерии и финансовом методе дисконтированного денежного потока.

Стоимостная модель ремонтного цикла обслуживания оборудования АЭС разработана применительно к определённому классу систем. Примерами классов таких систем являются система управления и защиты реактора, система аварийного охлаждения реактора, система аварийной подпитки барабан сепаратора, система технического водоснабжения и т.д.

Предполагается, что каждый класс систем имеет структурную модель, состоящую из конечного числа базисных конфигураций элементов. В качестве базисных конфигураций допускается использовать: последовательное соединение элементов; параллельное соединение; замкнутый контур; многоканальные соединения с другими элементами [38].

Базисными элементами структурной модели системы являются простые и сложные элементы (компоненты). Простой элемент не разлагается на элементы и имеет самостоятельную характеристику надёжности, используемую при расчетах и выполняющую определенную частную функцию в интересах системы. Сложный базисный элемент допускает разложение на простые элементы и сложные элементы и не имеет самостоятельной характеристики надёжности (собственного описания функцией надёжности).

Экономическая эффективность и надёжность работы системы определённого класса зависит от фактического состояния её эле-

ментов и качества ТОиР в процессе эксплуатации оборудования. С этой точки зрения оптимальная периодичность плановых ремонтов определяется минимизацией затрат на ремонт при заданном уровне надёжности и безопасности системы. В основе минимизации затрат на ремонт лежит модель стоимости оборудования.

#### 4.1.2. Модель стоимости оборудования

В общем виде стоимость оборудования определенного класса систем определяется соотношением [39]:

$$C_c = C_o + C_I + C_R, \quad (4.1)$$

где  $C_c$  – стоимость оборудования класса «с»;  $C_o$  – остаточная стоимость;  $C_I$  – сумма инвестиций в оборудование (инвестиционная стоимость), направленная на снижение риска;  $C_R$  – ожидаемые потери, связанные с реализацией операционного риска (стоимость риска).

Остаточная стоимость оборудования описывается выражением [39]:

$$C_o = C_{\text{бал}} - C_{\text{и}},$$

где  $C_{\text{бал}}$  – балансовая стоимость оборудования;  $C_{\text{и}}$  – стоимость износа оборудования;

$$C_{\text{и}} = C_{\text{бал}} \cdot N_a \cdot T_3 / 100 \%,$$

где  $N_a$  – норма амортизации для каждого года эксплуатации в процентах;  $T_3$  – число лет эксплуатации оборудования.

Стоимость инвестиций в оборудование принимается равной стоимости плановых ремонтов и замен оборудования:

$$C_I = C_{\text{п}}, \quad (4.2)$$

где  $C_{\text{п}}$  – стоимость плановых ремонтов и замен оборудования, в которую входит капитальный ремонт, как один из видов плановых ремонтов. Капитальный ремонт в начале цикла входит в схему цикла обслуживания, которая ограничена межкапитальными ремонтами, а капитальный ремонт в конце цикла не входит в схему цикла.

Ожидаемые потери, связанные с реализацией операционного риска:

$$C_R = C_a + C_{\text{т}}, \quad (4.3)$$

где  $C_a$  – затраты на ремонт и восстановление оборудования в результате аварии;  $C_T$  – потери возможного нарушения технологического процесса.

Для  $C_R$  справедливо соотношение [40]:

$$C_R = PE \cdot LGE \cdot C_{EI}, \quad (4.4)$$

где  $PE$  – вероятность возникновения отказа оборудования (вероятность аварии);  $LGE$  – уровень возможных потерь, характеризующий «тяжесть» и полноту восстановления оборудования,  $LGE \in [0,1]$ ;  $C_{EI}$  – стоимость «под риском», определяемая индикатором  $EI$  [40]:

$$C_{EI} = k_R \cdot EI, \quad (4.5)$$

где  $k_R$  – коэффициент нормировки, связывающий величину ожидаемых потерь и индикатор стоимости  $EI$ .

#### 4.1.3. Модель восстановленной стоимости ремонтного цикла и условие оптимальности

Рассмотрим ремонтный цикл длительностью  $T_c$  от одного капитального ремонта до другого (рис. 4.1).

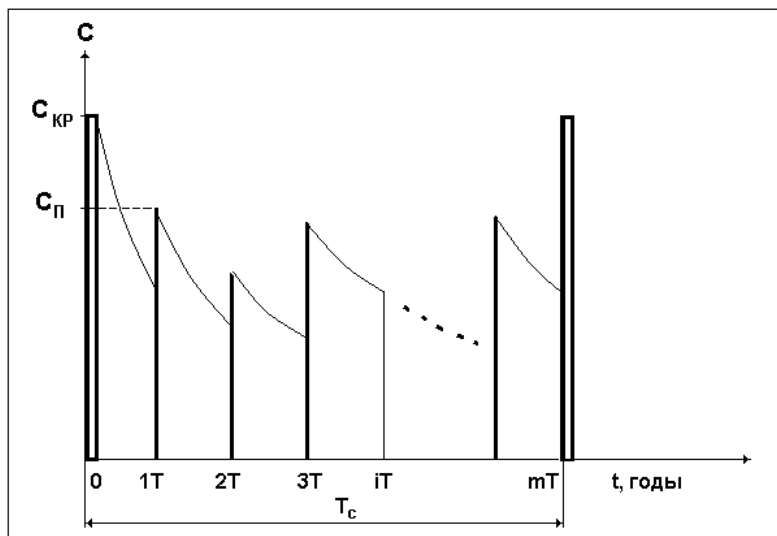


Рис. 4.1. Схема ремонтного цикла



Если принять остаточную стоимость оборудования  $C_o = \text{const}$  на момент  $t = 0$ , то её можно не учитывать внутри оптимизируемого цикла. Тогда восстановленная стоимость оборудования  $C$  будет определяться только дисконтированными инвестиционной и рисковой составляющими:

$$C = C_{\text{Ид}} + C_{\text{Рд}}, \quad (4.6)$$

где

$$C_{\text{Ид}} = C_{\text{КР}} + \sum_{i=1}^{m-1} C_{\text{П}i} / (1 + k_{\text{д}})^i, \quad (4.7)$$

$C_{\text{Ид}}$  – дисконтированная инвестиционная составляющая цикла;  $k_{\text{д}}$  – коэффициент дисконтирования потока инвестиций;  $C_{\text{КР}}$  – затраты на капитальный ремонт;  $C_{\text{П}i}$  – затраты на плановый ремонт на шаге  $i$ .

Дисконтированная рисковая составляющая цикла  $C_{\text{Рд}}$  (при непрерывном дисконтировании), приведённая к началу цикла [17, с.3]:

$$C_{\text{Рд}} = \sum_{j=1}^m C_{\text{Р}j} \exp \{k_{\text{дР}} (m - j)\}, \quad (4.8)$$

где  $C_{\text{Р}j} = PE_j \cdot LGE_j \cdot C_{\text{ЕИ}j}$  – затраты на восстановление отказавшего оборудования и потери от возможного нарушения технологического процесса на шаге  $j$ ;  $k_{\text{дР}} = k_{\text{д}} + r_{\text{Р}}$  – коэффициент дисконтирования рисковой составляющей с учётом коэффициента  $r_{\text{Р}}$  восстановления оборудования.

Если для  $j$ -го шага рисковой составляющей цикла принять допущения:  $PE_j = \text{const}$ ;  $LGE_j = \text{const}$ ,  $C_{\text{ЕИ}j} = k_{\text{Р}} \cdot C_{\text{П}}(i - 1)$ , где индикатор  $\text{ЕИ}_j$  являются затраты  $C_{\text{П}}(i - 1)$  на плановый ремонт в инвестиционной составляющей цикла на предыдущем шаге;  $k_{\text{Р}}$  – отношение среднегодовых затрат на восстановление оборудования в случае аварийных отказов (включая нарушение технологического процесса) к среднегодовым затратам на плановый ремонт, то

$$C_{\text{Рд}} = PE \cdot LGE \cdot k_{\text{Р}} \cdot \sum_{i=1}^m C_{\text{П}}(i - 1) \exp \{k_{\text{дР}} \cdot i\}, \quad (4.9)$$

где  $C_{\text{П}}(0) = C_{\text{КР}}$ ,  $m = |T_c / T|$ ,  $T = 1/n_p$  – интервал периодичности плановых ремонтов/обслуживания;  $n_p$  – число плановых ремонтов в год.

Для оптимизации сроков проведения плановых ремонтов введем понятие удельной восстановленной стоимости оборудования. Удельная восстановленная стоимость оборудования внутри цикла, состоящего из  $m$  шагов, равна

$$c_B = C / (mT) = [C_{\text{КР}} + \sum_{i=1}^{m-1} C_{\text{П}i} / (1 + k_d)^i + \\ + PE \cdot LGE \cdot k_R \cdot \sum_{i=1}^m C_{\text{П}}(i-1) \exp\{k_{\text{дР}} \cdot i\}] / (mT). \quad (4.10)$$

Оптимальная периодичность плановых ремонтов определяется минимизацией удельной восстановленной стоимости:

$$\min_j c_B = \min_j [C_{\text{КР}} + \sum_{i=1}^j C_{\text{П}i} / (1 + k_d)^i + \\ + PE \cdot LGE \cdot k_R \cdot \sum_{i=1}^j C_{\text{П}}(i) \exp\{k_{\text{дР}} i\}] / (iT).$$

Если это выражение разделить на  $C_{\text{КР}}$ , то условие оптимальности примет вид

$$T_{\text{опт}} = (jT)_0 = \\ = \min_j [1 + \sum_{i=1}^j k_{\text{ПК}i} / (1 + k_d)^i + PE \cdot LGE \cdot k_{\text{ПК}i} \sum_{i=1}^j \exp\{k_{\text{дР}} i\}] / (jT), \quad (4.11)$$

где  $k_{\text{ПК}i} = C_{\text{П}i} / C_{\text{КР}}$  – доля стоимости плановых ремонтов от стоимости капитального ремонта.

#### 4.1.4. Модели вероятности отказа и уровня возможных потерь при отказе оборудования

Вероятность безотказной работы компонента оборудования определяется соотношением [41]:

$$P(T) = \exp\left(-\int_0^T \lambda(t) dt\right)$$

где  $\lambda(t)$  – интенсивность отказов. Для малых значений  $\lambda$  вероятность безотказной работы определяется выражением

$$P(T) = 1 - \int_0^T \lambda(t) dt .$$

Вероятность отказа оборудования на интервале  $[0, T]$  определяется соотношением:

$$PE = 1 - P(T) = \int_0^T \lambda(t) dt. \quad (4.12)$$

На практике [42] интенсивность отказа аппроксимируют линейной зависимостью от времени

$$\lambda(t) = \lambda_0 + kt,$$

где  $\lambda_0$  – начальное значение интенсивности отказов;  $k$  – коэффициент старения оборудования.

Тогда для вероятности отказа оборудования на интервале  $[0, T]$  получим выражение

$$PE = \lambda_0 T + kT^2 / 2. \quad (4.13)$$

Уровень потерь LGE при отказе компонента оборудования в настоящей модели определяется функцией распределения  $F_x$  случайной величины  $x$  (см. п. 3.3). Для уровня потерь LGE можно записать:

$$LGE = F_x = \Phi(u(x)), \quad (4.14)$$

где  $\Phi(u)$  – табулированная функция Лапласа [27].

#### 4.1.5. Модель расчёта коэффициента восстановления компонента

Вероятность неработоспособности  $p(t)$  в момент времени  $t$  для восстанавливаемой системы (компонента) определяется соотношением [41]:

$$p(t) = 1 - G(t),$$

где  $G(t)$  – функция готовности, определяемая соотношением [41]:

$$G(t) = (\mu/(\lambda + \mu)) [1 + (\lambda/\mu) \exp\{-(\lambda + \mu)t\}],$$

$\lambda$  и  $\mu$  – интенсивность отказов и интенсивность восстановлений соответственно.

Предположим, что дисконтирование затрат на восстановление оборудования осуществляется в соответствии с изменением вероятности  $p(t)$ . Аппроксимируем изменение  $p(t)$  от коэффициента восстановления  $r_R$  экспоненциальной зависимостью. Тогда неизвестный коэффициент восстановления  $r_R$  можно найти из уравнения

$1 - (\mu/(\lambda + \mu))[1 + (\lambda/\mu) \exp\{-(\lambda + \mu)t\}] = a \exp(r_R t),$  (4.15)  
 где  $a$  – некоторая константа.

Параметр экспоненциального сглаживания  $r_R$  (коэффициент восстановления) можно найти графически путём построения линии экспоненциального тренда функции  $p(t)$ . Пример такого построения показан на рис. 4.2. Из рисунка видно, что  $r_R = 0,0492$ , точками обозначены значения правой части приведённого выше уравнения.

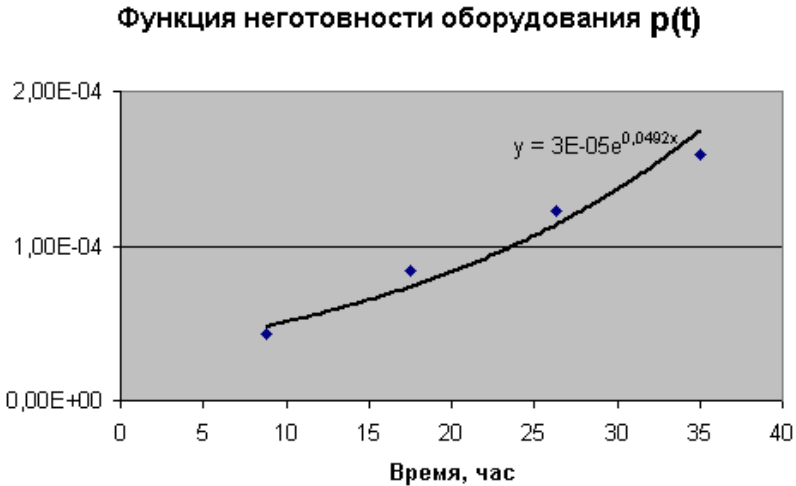


Рис. 4.2. Пример функции неготовности оборудования и её экспоненциального тренда

#### 4.1.6. Оценка работоспособности моделей, анализ их чувствительности к неопределённости параметров

Работоспособность оптимизационных моделей проверялась на отдельных компонентах системы технического водоснабжения (насос СТВ) и управляющей системы безопасности (предохранительный клапан системы УСБ-Т). В табл. 4.1 приведены исходные данные по параметрам надёжности компонент и параметрам ремонтного цикла.

## Исходные данные

Наименование параметров модели	Значения для ПТК УСБ-Т	Значения для насоса СТВ
$n_p$ – число плановых ТОиР в год	2	2
$\lambda_0$ – интенсивность отказов, 1/ч	1,41E-04	7,33E-07
$t_b$ – время восстановления, ч	8	24
$k_d$ – коэффициент дисконтирования	0,2	0,2
LGE, отн.ед.	1	1
$r_R$ , отн.ед.	0,014	0,011
$k$ , 1/год <sup>2</sup> – коэффициент старения оборудования	0,1	0,2
$k_R$ – коэффициент нормировки ожидаемых потерь	0,3	0,8

Стоимостные параметры цикла  $k_{ПКi} = C_{Pi} / C_{КР} = 0,1$  на всех временных интервалах  $T$  ремонтного цикла. Для средних ремонтов  $k_{ПКi} = 0,5$ ; для капитальных ремонтов  $k_{ПКi} = 1$ .

Удельная восстановленная стоимость  $c_B(j)$  рассчитывалась по формуле (см. (4.11)):

$$c_B(j) = [1 + \sum_{i=1}^j k_{ПКi} / (1 + k_d)^i] + PE \cdot LGE \cdot k_R \sum_{i=1}^j k_{ПКi} \exp\{k_{dR} i\} / (jT),$$

Вероятность отказа оборудования PE вычислялась по формуле (4.13).

На рис. 4.3 и рис. 4.4 представлены кривые удельной восстановленной стоимости, полученные для указанных выше параметров модели. Из этих рисунков следует, что оптимальная длительность ремонтного цикла составляет 7,5 года для насоса СТВ и 5 лет для ПТК УСБ-Т.

Модель оказалась чувствительной к изменению параметра нормировки  $k_R$ . Так, увеличение  $k_R$  с 0,3 до 1, привело к уменьшению оптимального значения длительности ремонтного цикла с 5 лет до 3,5 лет (рис. 4.5).

Также была выявлена высокая чувствительность модели к изменению коэффициента дисконтирования  $k_d$ . Увеличение  $k_d$  на 67 %

(со значения  $k_d = 0,15$ ) привело к уменьшению оптимального значения длительности ремонтного цикла на 3 года. (см. рис. 4.6).

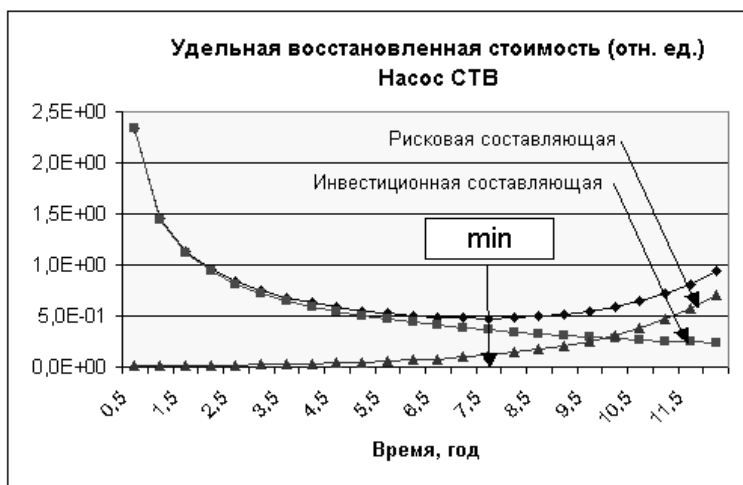


Рис. 4.3. Удельная восстановленная стоимость для насоса СТВ

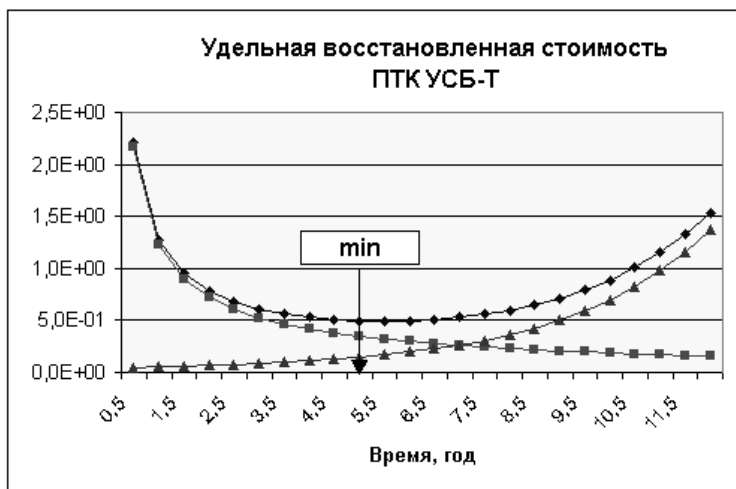


Рис. 4.4. Удельная восстановленная стоимость для ПТК УСБ-Т

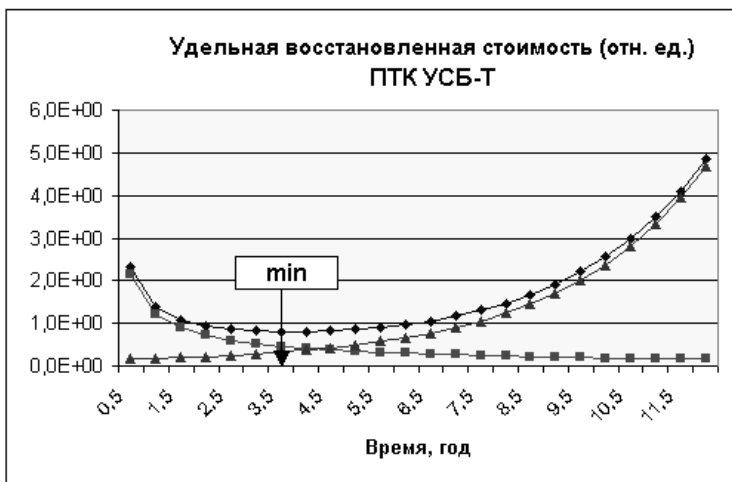


Рис. 4.5. Удельная восстановленная стоимости ПТК USB-T для  $k_R = 1$

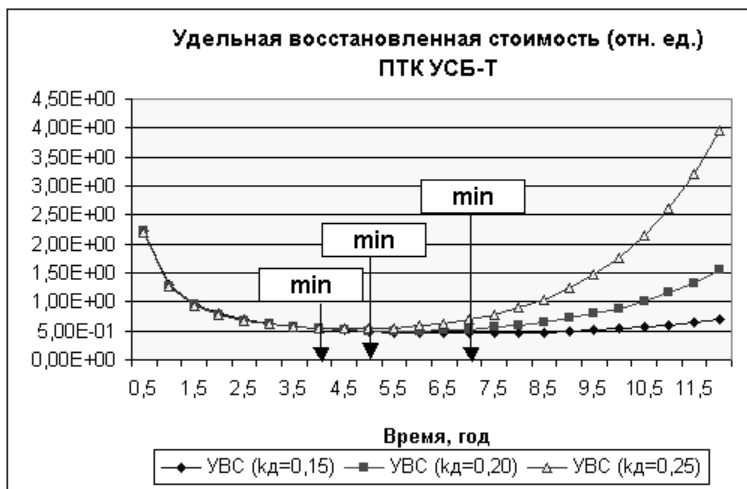


Рис. 4.6. Чувствительность удельной восстановленной стоимости ПТК USB-T к изменению коэффициента дисконтирования  $k_d$

Исследование показали, что модель адекватно реагирует на изменение стоимостных характеристик цикла (рис. 4.7). Отмечается, что увеличение инвестиций и увеличение их частоты внутри цикла

не приводит к значительному увеличению оптимального значения длительности ремонтного цикла.

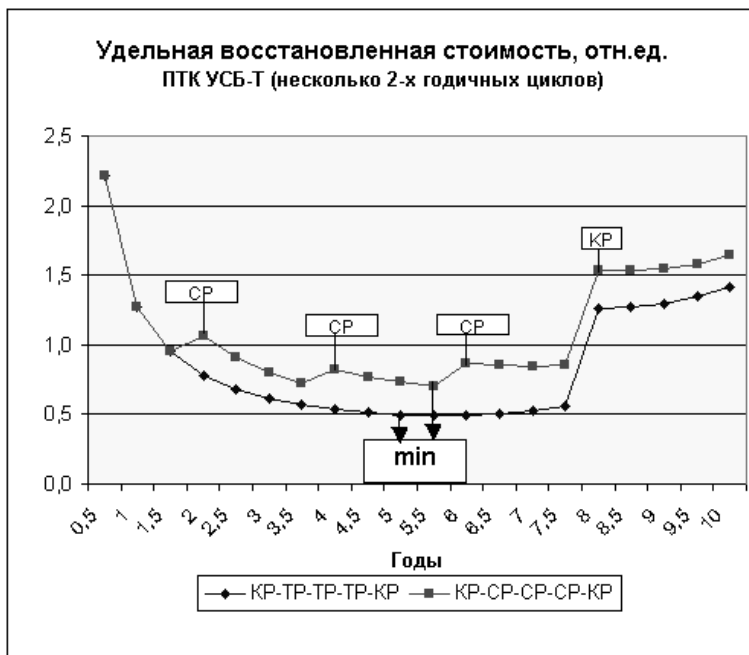


Рис. 4.7. Чувствительность модели к изменению стоимостных характеристик цикла

## 4.2. Применение моделей оптимизации для оценки длительности ремонтного цикла системы технического водоснабжения АЭС

### 4.2.1. Система технического водоснабжения (СТВ)

- В состав СТВ входят [43]:
- подводящий канал от пруда – охладителя;
- береговая насосная станция (БНС);
- магистральные водоводы и трубопроводы к потребителям;



- повысительная насосная;
- сливные трубопроводы и водоводы от потребителей до сбросного канала;
- сбросный канал (ПЛК);
- необходимая арматура, КИПиА, обеспечивающий контроль и управление.

Схема основных подсистем СТВ показана на рис. 4.8.

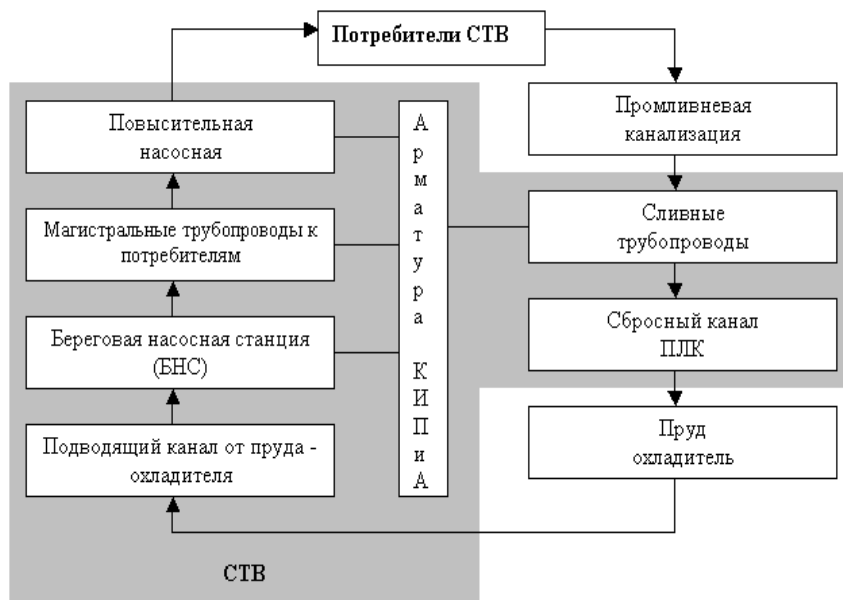


Рис. 4.8. Состав СТВ

В режиме планового расхолаживания реактора основными потребителями технической воды являются:

- насосы продувки и расхолаживания;
- промышленный контур реакторного отделения;
- технологические конденсаторы;
- дренажный узел машинного зала;
- аварийные питательные насосы (АПЭН);
- установка сжигания «гремучей смеси» (УСГС).

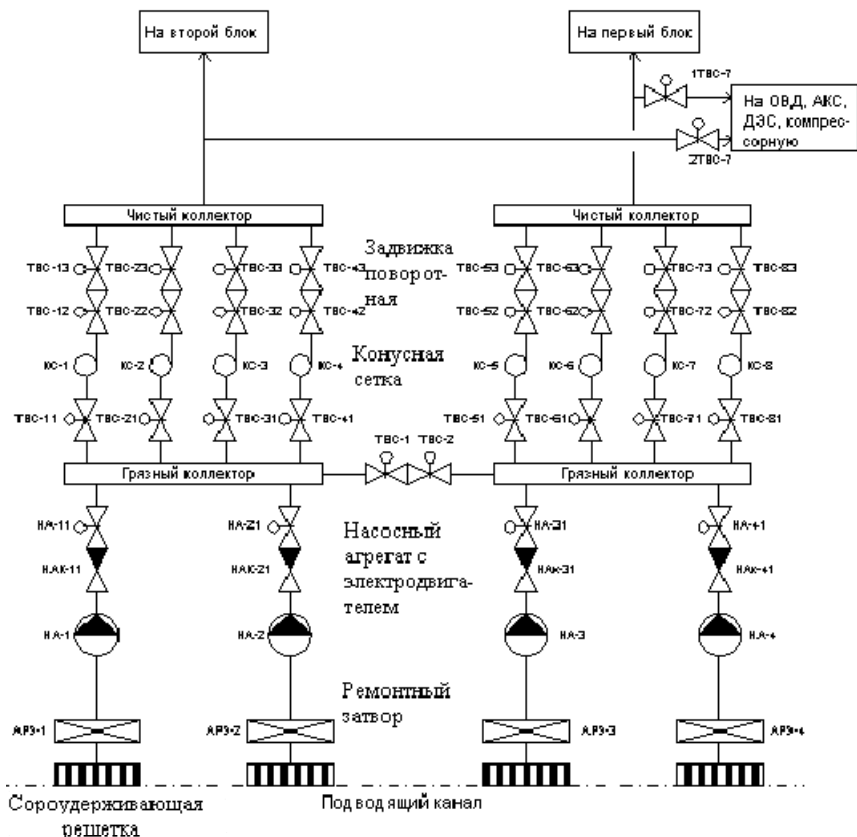


Рис. 4.9. Принципиальная схема СТВ [44]

В режиме локализации аварий необходимо непрерывно подавать воду к следующим потребителям:  
теплообменникам контура СУЗ;

- теплообменникам охлаждения бассейна выдержки;
- холодильникам системы контроля целостности технологических каналов (КЦТК);
- охладителям воздуха из-под плитного настила;
- электродвигателям насосов системы аварийного расхолаживания (САОР);
- дренажному узлу машинного зала;

- АПЭН;
- теплообменникам УСГС;
- теплообменникам системы спецвентиляции;
- дизель-генераторной станции;
- азотно-кислородной станции;
- компрессорной станции собственных нужд.

Принципиальная схема СТВ приведена на рис. 4.9 [44].

Подключенные, вспомогательные, управляющие и обеспечивающие системы на рисунке не показаны.

#### 4.2.2. Исходные данные для моделирования

Исходные данные для моделей оптимизации и оценки длительности ремонтного цикла оборудования СТВ приведены в табл. 4.2, где введены обозначения:

(1\*)  $\lambda$ , 1/ч – интенсивность отказов;

$T_r$ , ч – время восстановления работоспособности;

(2\*)  $k_{OK}$  – коэффициент затрат на техническое обслуживание (доля от стоимости капитального ремонта);

$k_{OK} = C_o / C_k$ ,  $C_o$  – стоимость затрат на техническое обслуживание;  $C_k$  – стоимость капитального ремонта;

(3\*)  $k_{TK}$  – коэффициент затрат на текущий ремонт (доля от стоимости капитального ремонта);

$k_{TK} = C_t / C_k$ ,  $C_t$  – стоимость затрат на текущий ремонт;  $C_k$  – стоимость капитального ремонта;

(4\*)  $k_{СК}$  – коэффициент затрат на средний ремонт (доля от стоимости капитального ремонта);

$k_{СК} = C_c / C_k$ ,  $C_c$  – стоимость затрат на средний ремонт;  $C_k$  – стоимость капитального ремонта.

Временные и стоимостные характеристики ремонтного цикла получены с реального блока АЭС. Характеристики надёжности оборудования получены из справочника [45] и материалов диссертации [46], затем корректировались с учётом информации о реальных параметрах надёжности оборудования АЭС с реактором РБМК. Пример такой информации приведён в табл. 4.3.

Таблица 4.2

**Перечень элементов СТВ и исходные данные для оптимизации  
длительности ремонтного цикла**

№ п/п	Стационарное обозначение	Наименование элемента	Тип, марка, модель	Кол-во элементов в системе на очередь	Характеристики надежности (1*)		Ремонт			Характеристики ремонтного цикла, мес.				КОК (2*)	КТК (3*)	кСК (4*)
					Lambda, 1/4	Tг, ч	текучий	на 1 шт. руб. (без НДС)	капитальный	ТО	ТР	СР	КР			
1	НА-3	Насос аппаратный	100И-4/63А (40в-16)	4	1,30E-05	96	27285	131312	187588	1	12	24	48	0,10	0,15	0,7
2	НА-3	Электродвигатель 1250 кВт 375 об/мин	ВАН-173-56-16УЗ	4	1,38E-05	48	7804		37882	1	12	24	48	0,10	0,21	0,5
3	НА-31	Затворы поворотные дисковые	ИА 9904-1000	4	6,30E-05	72	13463	74673	124454	1	12	24	48	0,10	0,11	0,6
4	ТВС-51,...	Затворы поворотные дисковые	ИА 9904-800	8	6,30E-05	72	8976	49782	82970	1	12	24	48	0,10	0,11	0,6
5	ТВС-1	Затворы поворотные дисковые	ИА 9904-1200	2	6,30E-05	72	13755	76289	127149	1	12	24	48	0,10	0,11	0,6
6	ТВС-18	Задвижка Ду 250 Ру до 2,5 мПа		8	5,75E-05	48	4436	6352	10586	1	12	24	48	0,10	0,42	0,6
7	НАК-11	Обратный клапан (выемная часть) Ду1000 Ру2,5-6,4 мПа	ПТ4407-1000М1-02	4	4,50E-05	48	12227	17445	29075	1	12	24	48	0,10	0,42	0,6
8	КС-1	Конусные сетки		8	8,75E-05	72	6871		89313	1	12	24	48	0,10	0,08	0,5

Окончание табл. 4.1

№ п/п	Стационарное обозначение	Наименование элемента	Тип, марка, модель	Кол-во элементов в системе на очередь	Характеристики надежности (1*)		Ремонт			Характеристики ремонтного цикла, мес.			КОК (2*)	КТК (3*)	КСК (4*)		
					Lambda, 1/ч	Tг, ч	текущий	средний	капитальный	ТО	ТР	СР				КР	
9		Арматура разная БНС-2				1,20E-04	24			не 1 шт. руб. (без НДС)		1	12	24	48	0,10	0,5
10	НЗ-11	Затворы плоские колесные	Ду1200	16		5,75E-05	72	14090	20129	33548		1	12	24	48	0,10	0,6
11	ВС-1-8	Сетки водо-очистительные	ТЛ-3000	16		1,40E-04	48	6871		89313		1	12	24	48	0,10	0
12	ЦНС-7	Циркуляционный насос	ОПВ-145Э	12		5,75E-06	96		172575	246536		1	12	24	48	0,10	0,7
13	ЦНС-8	Электродвигатель 1250 кВт 375 об/мин	АВ-17-39-16	12		1,15E-05	60	7804		37882		1	12	24	48	0,10	0
14	КР-1	Компрессор водоотриемника	УКП-1/10			3,45E-05	96	37510	98504	124996		1	12	24	48	0,10	0,8
15	НБ-1	Напорный бассейн 1 очереди	Открытый насыпного типа	1		1,40E-04	120					1	12	24	48	0,10	0,5

**Характеристики отказов оборудования СТВ блока АЭС  
с реактором РБМК за 1976-2009 гг.**

Оборудование	Описание деффекта	Время восстановления
ЦН-9	Отключение ЦН-9 токовой отсечкой из-за повреждения кабеля ААШВ (3*150) в месте перехода кабеля из к/о в колодец (трещина бумажной изоляции из-за изгиба при монтаже)	1 сут
ЦН-7	Отключение ЦН-7 из-за КЗ кабеля ААШВ (3*185) в месте прохода через металлическую проходку из к/о в шинный коридор	1 сут
3ЦН-6	Разрушение механизма разворота лопастей 3ЦН-6 из-за разрушения подшипника 8426Л (механический износ шариков, разрушение сепаратора, заклинивание)	5 сут
3ННТ-3	Выход из строя насоса повышения напора тех-воды 3ННТ-3 бл.3	1 сут
4ЦН-1, 4ЦН-2	Выход из строя электродвигателей насосов 4ЦН-1,2 в результате их включения при обратном вращении	7 сут
3НА-3	Отказ в работе 3НА-3 (срезало шпильки)	5 сут
3НА-2	Неуспешное опробывание после ремонта 3НА-3	3 сут
4НА-3	Самопроизвольное включение 4НА-3 из-за отказа контактора выключателя ВЭМ-6 при сборке схемы в рабочее положение	8 ч
4ЦН-5	Отключение насоса 4ЦН-5 ложной работой от КЗ на землю	8 ч
4ЦН-3	Повреждение сегментов подшипника электродвигателя насоса 4ЦН-3	3 сут
НА-1, НА-2	Несанкционированное срабатывание АВР НА-1 по снижению давления	1 сут
ЦН-11	Аварийный останов ключом управления ЦН-11 из-за попадания масла на обмотки электродвигателя	2 сут
НА-2	Аварийный останов ключом управления НА-2 из-за попадания масла на обмотки электродвигателя	2 сут

Оборудование	Описание деффекта	Время восстановления
ЦН-8	Отключение ЦН-8 земляной защитой из-за пробоя изоляции силового кабеля на корпус в месте подключения к электродвигателю	1 сут
НА-2	Аварийный останов НА-2 из-за повышения уровня масла в нижней маслованне	1 сут
ЦН-4	Несанкционированное отключение ЦН-4 земляной защитой из-за пробоя изоляции обмоток статора электродвигателя	2 сут
4ЦН-5	Отключение электродвигателя 4ЦН-5 действием токовой защиты из-за КЗ в разделке силового кабеля у ЭД	1 сут
3НА-3	Отключение ЭД 3НА-3 действием токовой защиты из-за КЗ в коробке выводов ЭД	1 сут
4НА-1	Отключение ЭД 4НА-1 действием защиты от замыканий на землю из-за КЗ в коробке выводов ЭД	1 сут
4НА-3	Отключение ЭД 4НА-3 действием токовой защиты из-за КЗ в обмотке статора	2 сут
4НА-1	Отключение ЭД 4НА-1 действием токовой защиты из-за КЗ в соединительной муфте силового кабеля	1 сут
4НА-2	Отказ в работе насоса 4НА-2 вследствие разрушения вала насосного агрегата	5 сут
4ЦН-4	Отключение ЭД 4ЦН-4 действием токовой защиты из-за КЗ силового кабеля в коробке вводов	1 сут
НА-3	Отказ в работе НА-3 вследствие разрушения вала насосного агрегата	5 сут
4НА-2	Отказ в работе насоса 4НА-2 вследствие разрушения защитного кольца рабочего колеса насосного агрегата	5 сут
ЦН, НА	Засорение дрейсенной трубопровода подачи технической воды на насосы ЦН и НА со стороны «чистого» коллектора	1 сут
3НА-1	Внеплановое отключение персоналом насоса 3НА-1 из-за повышения уровня масла в нижней маслованне ЭД вследствие нарушения герметичности трубки м/о	1 сут

### 4.2.3. Результаты моделирования

Оптимизация длительности ремонтного цикла оборудования СТВ проводилась на основе условия оптимальности (4.11). Во всех расчётах полагалось, что следующие параметры были постоянными:

- интервал периодичности плановых ремонтов/обслуживания  $T = 0,5$  года;
- коэффициент нормировки ожидаемых потерь  $k_R = 1$  (максимальное значение);
- коэффициент дисконтирования потока инвестиций  $k_d = 0,15$ ;
- уровень возможных потерь  $LGE = 1$  (максимальный уровень);
- коэффициент старения оборудования  $k = 0,1 \text{ год}^{-2}$ .

Результаты оптимизации длительности ремонтных циклов представлены в табл. 4.4, где обозначено:

КР – капитальный ремонт;

ТР – текущий ремонт;

СР – средний ремонт;

$T_{\text{опт}}$  – оптимальная длительность ремонтного цикла;

$K_{\text{нг}}(T_{\text{опт}})$  – коэффициент неготовности при длительности цикла  $T_{\text{опт}}$  (чем меньше  $K_{\text{нг}}$ , тем надёжнее компонент);

ЕИ ( $T_{\text{опт}}$ ) – отношение удельной восстановленной стоимости к стоимости инвестиций при длительности цикла  $T_{\text{опт}}$ , характеризует «инвестиционную затратность» цикла (чем меньше ЕИ, тем дешевле ремонтный цикл).

На рис. 4.10 и 4.11 представлены графики показателей эффективности  $Z$  стратегий КР-ТР-СР-ТР-КР и КР-ТР-ТР-ТР-КР соответственно.

Показатель эффективности  $Z$  для элементов системы СТВ, представленных в табл. 4.4, вычислялся в соответствии со следующими соотношениями:

$$Z = 0,5(X + Y);$$
$$X = (K_{\text{нг max}} - K_{\text{нг}})/(K_{\text{нг max}} - K_{\text{нг min}});$$
$$Y = (EI_{\text{max}} - EI)/(EI_{\text{max}} - EI_{\text{min}}).$$

На этих же рисунках показаны области эффективных решений, соответствующие «наименьшим» значениям критерия  $Z$  (чем меньше  $Z$ , тем «лучше»).



Таблица 4.4

**Результаты оптимизации длительности ремонтных циклов**

Станционное обозначение	Наименование элемента	Стратегия ТОиР: КР-ТР-СР-ТР-КР, цикл 4 года			Стратегия ТОиР: КР-ТР-ТР-ТР-КР, цикл 4 года		
		$T_{\text{опт}}$ , лет	$K_{\text{нр}}$ ( $T_{\text{опт}}$ )	ЕИ ( $T_{\text{опт}}$ )	$T_{\text{опт}}$ , лет	$K_{\text{нр}}$ ( $T_{\text{опт}}$ )	ЕИ ( $T_{\text{опт}}$ )
НА-3	Насос аппаратный	7,5	1,46E-03	1,34	7,5	1,46E-03	1,30
НА-3	Электродвигатель 1250 кВт 375 об/мин	7,5	7,30E-04	1,34	7,5	7,30E-04	1,32
ТВС-51, ...	Затвор поворотный дисковый	3,5	2,34E-03	1,31	3,5	2,34E-03	1,25
ТВС-18	Задвижка Ду 250, Ру до 2,5 мПа	5,5	9,95E-04	1,65	3,5	1,56E-03	1,31
НАК-11	Обратный клапан (выемная часть) Ду1000 Ру 2,5-6,4 мПа	5,5	9,95E-04	1,52	5,5	9,95E-04	1,53
КС-1	Конусная сетка	3,5	2,34E-03	1,49	3,5	2,34E-03	1,47
	Арматура разная БНС-2	5,5	4,98E-04	1,90	5,0	5,48E-04	1,76
НЗ-11	Затвор плоский колесный	5,5	1,49E-03	1,67	3,5	2,34E-03	1,32
ВС-1-8	Сетка водоочистительная	5,5	9,95E-04	2,09	4,5	1,22E-03	1,76
ЦНС-7	Циркуляционный насос	9,5	1,15E-03	1,38	7,5	1,46E-03	1,16
ЦНС-8	Электродвигатель 1250 кВт 375 об/мин	7,5	9,12E-04	1,29	7,5	9,12E-04	1,28
КР-1	Компрессор водоприемника	5,5	1,99E-03	1,43	3,5	3,12E-03	1,18
НБ-1	Напорный бассейн 1 очереди	5,5	2,48E-03	2,13	4,5	3,03E-03	1,79

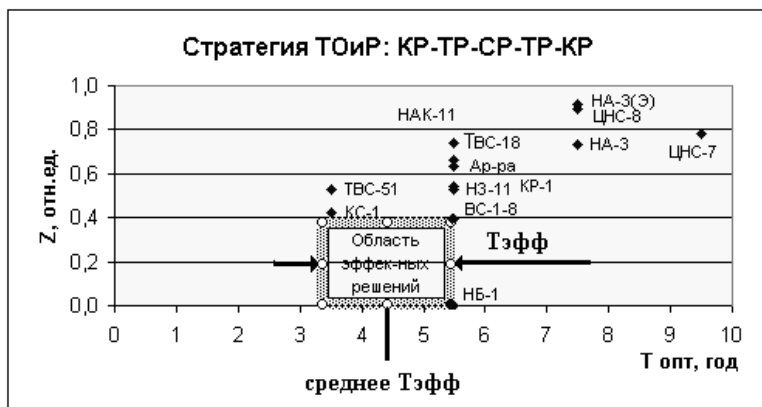


Рис. 4.10. Показатель эффективности стратегии КР-ТР-СР-ТР-КР для элементов оборудования СТВ

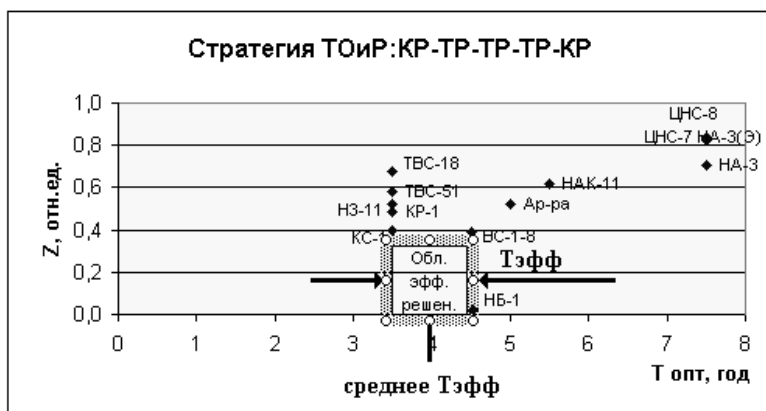


Рис. 4.11. Показатель эффективности стратегии КР-ТР-ТР-ТР-КР для элементов оборудования СТВ

Таким образом, среднее значение длительности цикла  $T_{эфф} = 4,5$  года для стратегии ТОиР: КР-ТР-СР-ТР-КР и  $T_{эфф} = 4$  года для стратегии КР-ТР-ТР-ТР-КР.

В табл. 4.5 представлены минимальные стоимостные характеристики 4-летнего цикла КР-ТР-СР-ТР-КР для компонент СТВ. В стоимость планового обслуживания и ремонта стоимость последнего КР (в цепочке КР-ТР-СР-ТР-КР) не входит.

Таблица 4.5

**Минимальные стоимостные характеристики 4-летнего цикла КР-ТР-СР-ТР-КР для компонент СТВ  
и величины операционного риска за 4-летний оптимизируемый период**

№ п/п	Стационарное обозначение	Наименование элемента	Тип, марка, мо- дель	Кол-во элементов в систе- ме на очередь	Ремонт			Минимальная стоимость планового обслуживания и ремонта (4-лет. цикл)	Операци- онный риск (4-лет. цикл)
					Текущий	средний	капиталь- ный		
					на 1 шт. руб. (без НДС)			тыс. руб.·N шт.	
1	НА-3	Насос аппаратный	100и-4/63А (40в- 16)	4	27285	131312	187588	892,1	793,5
2	НА-3	Электродвигатель 1250 кВт 375 об/мин	ВАН-173-56- 16УЗ	4	7804		37882	175,9	154,9
3	НА-31	Затворы поворотные дисковые	ИА 9904-1000	4	13463	74673	124454	1165,2	357,5
4	ТВС-51, ...	Затворы поворотные дисковые	ИА 9904-800	8	8976	49782	82970	1553,6	476,6
5	ТВС-1	Затворы поворотные дисковые	ИА 9904-1200	2	13755	76289	127149	595,2	182,6
6	ТВС-18	Задвижка Ду 250 Ру до 2,5 мПа		8	4436	6352	10586	93,1	370,1

Окончание табл. 4.5

№ п/п	Стационарное обозначение	Наименование элемента	Тип, марка, модель	Кол-во элементов в системе на очередь	Ремонт			Минимальная стоимость планового обслуживания и ремонта (4-лет. цикл)	Операционный риск (4-лет. цикл)
					текущий	средний	капитальный		
					на 1 шт. руб. (без НДС)			тыс. руб. N шт.	
7	НАК-11,	Обратный клапан (выемная часть) Ду 1000 Ру 2,5-6,4 мПа	ПТ4407-1000М1-02	4	12227	17445	29075	127,9	403,0
8	КС-1	Конусные сетки		8	6871		89313	2198,9	1069,8
9		Арматура разная БНС-2							
10	НЗ-11	Затворы плоские колесные	Ду1200	16	14090	20129	33548	590,4	2419,5
11	ВС-1-8	Сетки водоочистительные	ТЛ-3000	16	6871		89313	695,8	4255,3
12	ЦНС-7	Циркуляционный насос	ОПВ-145З	12		172575	246536	3402,5	1605,7
13	ЦНС-8	Электродвигатель 1250 кВт 375 об/мин	АВ-17-39-16	12	7804		37882	527,7	407,3
14	КР-1	Компрессор водоприемника	УКП-1/10		37510	98504	124996	167,9	378,1
15	НБ-1	Напорный бассейн 1 очереди	Открытый насыпного типа	1					
16	<b>ИТОГО</b>								<b>12186,2</b>

В общей стоимости ТОиР не учтены затраты на обслуживание напорного бассейна НБ-1 и арматуры БНС, ввиду отсутствия стоимостных характеристик обслуживания.

В колонке «Операционный риск» цветом выделены компоненты СТВ с наибольшим уровнем расчётного операционного риска. Можно предположить, что именно эти компоненты СТВ требуют приоритетного обслуживания. Однако для принятия окончательного решения необходимы экспертные оценки ОР всех компонент СТВ с учётом мнения специалистов – эксплуатационщиков.

### **Выводы**

1. Исследования модели показали, что риск-ориентированная модель чувствительна к изменениям стоимостных характеристик, показателей надёжности элементов оборудования и адекватно реагирует на их изменения.

2. Результаты оптимизации позволили установить среднее значение оптимальной длительности цикла системы  $T_{эфф} = 4,5$  года для стратегии ТОиР: КР-ТР-СР-ТР-КР и  $T_{эфф} = 4$  года для стратегии КР-ТР-ТР-ТР-КР. Этот результат совпал с длительностью ремонтного цикла СТВ, установленный опытным путём для АЭС с реактором РБМК.

### **Тесты для самоконтроля**

1. Какая из ниже перечисленных переменных не входит в формулу ожидаемых потерь, связанных с реализацией операционного риска?

- Вероятность возникновения отказа оборудования (PE).
- Стоимость износа оборудования (С<sub>и</sub>).
- Стоимость под риском (С<sub>ЕП</sub>).

2. Верно ли следующее утверждение: дисконтированная рискованная составляющая оптимального ремонтного цикла растёт со временем?

- Да.
- Нет.

3. Верно ли следующее утверждение: дисконтированная инвестиционная составляющая оптимального ремонтного цикла убывает со временем?

- Да.
- Нет.

4. Каково условие оптимальной периодичности плановых ремонтов для моделей, рассмотренных в этом разделе?

- Минимизация рискованной составляющей ремонтного цикла.
- Минимизация удельной восстановленной стоимости.
- Минимизация затрат на плановые ремонты.

5. От каких переменных зависит функция готовности компонента оборудования?

- От интенсивности отказов.
- От интенсивности отказов и интенсивности восстановлений.

6. Является ли система технического водоснабжения важной для безопасности АЭС?

- Да.
- Нет.
- Не знаю, в лекции об этом не говорилось.

7. Какова средняя эффективная длительность ремонтного цикла, полученная для системы технического водоснабжения АЭС?

- 3 года.
- 4 – 4,5 года.
- 5 – 5,5 лет.
- более 6 лет.

## Заключение

Управление риском – новая отрасль знаний, а управление операционным риском на атомных станциях – только подходит к первому этапу организационного управления. Поэтому в настоящее время нет работ, объединяющих различные подходы, или дано обобщённое представление о методах, моделях и системах управления рисками. В разделах 2 и 3 изложен процессный подход к управлению риском. Но существуют и развиваются другие подходы к анализу риска, моделированию рискованных событий и комплексному управлению сложной системой, к которой относятся АЭС.

**Метод «Анализ вида и последствий отказов» (АВПО)** применяется для качественного анализа опасности рассматриваемой технической системы. Существенной чертой этого метода является рассмотрение каждого аппарата (установки, блока) или составной части системы (элемента) на предмет того, как он стал неисправным (вид и причина отказа) и какое было бы воздействие отказа на техническую систему.

**Метод «Анализ вида, последствий и критичности отказа» (АВПКО)** расширяется до количественного анализа вида, последствий и критичности отказа. В этом случае каждый вид отказа ранжируется с учетом двух составляющих критичности: вероятности (или частоты) и тяжести последствий отказа. Определение параметров критичности необходимо для выработки рекомендаций и приоритетности мер безопасности и оценки риска.

Результаты анализа представляются в виде таблиц с перечнем оборудования, видом причин возможных отказов, частотой, последствиями, критичностью, средствами обнаружения неисправности (сигнализаторы, приборы контроля и т.п.) и рекомендациями по уменьшению опасности (риска).

**Логико-графические методы анализа «деревьев отказов» и «деревьев событий».** При анализе «деревьев отказов» (АДО) выявляются комбинации отказов оборудования, ошибок персонала и внешних (техногенных, природных) воздействий, приводящих к аварийной ситуации. Метод используется для анализа возможных

причин возникновения аварийной ситуации и расчета ее частоты (на основе знания частот исходных событий). При анализе дерева отказа определяются минимальные сочетания событий, определяющие возникновение или невозможность возникновения аварии (так называемые, минимальное пропускное и отсечное сочетания).

Анализ «дерева событий» (АДС) – алгоритм построения последовательности событий, исходящих из анализа развития аварийной ситуации (исходного события). Частота каждого сценария развития аварийной ситуации рассчитывается путем умножения частоты основного события на условную вероятность конечного события (например, аварии с разгерметизацией трубопровода). Одним из первых, кто начал развивать данный подход, был д.ф.-м. н., проф. Р.Т. Исламов.

**Метод вероятностного анализа безопасности (ВАБ)** нацелен на детальный анализ реального состояния исследуемого энергоблока АЭС, включая важные для безопасности системы, результаты их проверок и испытаний, регламент и организацию эксплуатации, надежность выполнения действий эксплуатационным персоналом и позволяет выявлять факторы, наиболее влияющие на безопасность. В зависимости от поставленных целей ВАБ делится на три уровня:

уровень 1 – определение вероятности повреждения активной зоны реактора энергоблока;

уровень 2 – определение вероятности выхода радиоактивности в окружающую среду при нарушении нормальной эксплуатации энергоблока;

уровень 3 – определение возможных негативных последствий выхода радиоактивности в окружающую среду вследствие нарушения нормальной эксплуатации энергоблока АЭС для населения и окружающей среды.

Для решения указанных выше задач необходимо иметь итоговое расчетное выражение, позволяющее рассчитать частоту повреждения активной зоны, вероятность выхода радиоактивных веществ, коэффициент неготовности оборудования и т.д. Это выражение (вероятностная модель безопасности) может быть представлено, например, в виде вероятностного многочлена.



Непосредственное получение вероятностного многочлена практически невозможно из-за громоздкости расчетных выражений. Поэтому вероятностную модель строят в несколько этапов:

- построение вербальной (словесной) модели (т.е. модели на основе качественного анализа систем, нейтронно-физических и тепло – гидравлических расчетов);
- построение графической модели (т. е. совокупности «деревьев событий», «деревьев отказов» или графов другого вида);
- построение логической модели (с применением функций алгебры логики);
- построение вероятностной модели (расчетное выражение, для определения требуемых характеристик);
- расчет показателей безопасности и риска;
- анализ неопределенности, значимости, чувствительности модели.

Ведущим специалистом по вероятностному анализу безопасности является д.т.н., проф. Г.А. Ершов.

**Общий логико-вероятностный метод (ОЛВМ).** Создателем научной школы ОЛВМ являются д.т.н., проф. И.А. Рябинин и д.т.н., проф. А.С. Можаяев. Этот метод применяется для структурно-логического моделирования и расчета показателей надежности, безопасности и риска сложных систем. Процедура анализа сложной системы предусматривает выполнение следующих основных этапов.

1. Составляется сценарий развития опасности, представляющий собой логико-вероятностную модель функционирования системы. Сценарий представляется в виде графа и содержит события трех видов: инициирующие (ИС), промежуточные, конечное состояние. Промежуточные события получаются путем логической комбинации двух или более событий. Комбинации событий представляются в виде конъюнкций и дизъюнкций событий. Конечное событие описывает опасное состояние системы.

2. Составляется функция опасности системы  $y(z_1, \dots, z_n)$ , ее аргументами являются ИС, а значением – конечное (опасное) событие. Каждый кратчайший путь опасного функционирования (КПОФ) представляет собой минимальный набор ИС, конъюнкция которых

приводит к опасному состоянию. Функция опасности системы представляет собой дизъюнкцию КПОФ.

3. Функция опасности системы приводится к одной из трех форм: совершенной, ортогональной, бесповторной дизъюнктивной нормальной форме (ДНФ). Затем функция опасности системы заменяется вероятностной функцией  $P\{y(z_1, \dots, z_m)\}$  следующим образом:

$z_i$  заменяется на  $P\{z_i = 1\} = p_i$ ;

$z'_i$  заменяется на  $P\{z'_i = 1\} = q_i = 1 - p_i$ ,

где  $p_i$  – вероятность наступления  $i$ -го ИС;  $z'_i$  – отрицание  $z_i$ .

4. Ищется значение вероятностной функции (ВФ):

$$\text{ВФ}(y) = P\{y(z_1, \dots, z_m) = 1\}.$$

ВФ определяет степень риска, присутствующего в системе.

Следует обратить внимание на то, что все выше перечисленные подходы – суть методы сценарного анализа. У каждого из них есть свои достоинства и недостатки. Но, пожалуй, главный недостаток – они не очень хорошо приспособлены к процессам управления. Этим они и отличаются от процессного подхода, описанного в данном учебном пособии. В управлении АЭС мало уметь рассчитывать вероятности тех или иных негативных событий. Нужно ещё оценить затраты на их устранение (предотвращение). А для этого уже давно разработан метод функционально-стоимостного анализа (ФСА); относительно недавно – процессный подход и оптимизация затрат на основе оценки риска.

Согласно исследованию, проведенному «Агентством по ядерной энергии ОЭСР», полные капитальные затраты для ядерных энергоблоков, включая строительство, крупное переоборудование и вывод из эксплуатации, составляют более 60 процентов затрат на генерирование энергии [47]. Также отмечается, что высоки эксплуатационные и ремонтные затраты. Опыт таких стран, как Германия и Соединенные Штаты, показывает, что эксплуатационные и ремонтные затраты атомной электростанции могут быть значительно снижены за счет совершенствования менеджмента, в частности, риск-менеджмента. В близкой перспективе ядерная энергетика сохранит свою конкурентоспособность, развивая систему управления рисками и интегрированные системы корпоративного управления. За этим – будущее.

## Библиография

1. Закон Российской Федерации «О безопасности» от 6 марта 1992 г. № 2446-1.
2. Общие положения обеспечения безопасности атомных станций. ОПБ-88/97 НП-001-97 (НПФЗГ-01-011-97).
3. Серия норм по безопасности, МАГАТЭ, № NS-G-1.12, Вена, 2006.
4. Отчёт по безопасности Государственной корпорации по атомной энергии «Росатом». М.: Комтехпринт, 2009.
5. Букринский А.М. Новая структура стандартов МАГАТЭ по безопасности.  
<http://www.proatom.ru/modules.php?name=News&file=article&sid=1900>
6. Цели регулирования при обеспечении ядерной безопасности // АЯЭ, № 6273, ОЭСР, 2008.
7. Основные санитарные правила обеспечения радиационной безопасности (ОСПОРБ-02).
8. Санитарные правила проектирования и эксплуатации атомных станций (СП АС-03).
9. Правила радиационной безопасности при эксплуатации атомных станций (ПРБ АС-99); Нормы радиационной безопасности (НРБ-99/2009).
10. Гордон Б.Г. К дискуссии о регулировании безопасности  
<http://www.proatom.ru/modules.php?name=News&file=article&sid=2008>
11. Ковалевич О.М., Гаврилов С.Д. Проблемы применения Федерального закона «О техническом регулировании» к деятельности по использованию атомной энергии// Вопросы атомной науки и техники, 2002.
12. Банковские риски: Учебное пособие / Под ред. д-ра экон. наук, проф. О.И. Лаврушина и д-ра экон. наук, проф. Н.И. Валенцевой. М.: КНОРУС, 2007.
13. Ковалевич О.М. К вопросу об определении «степени риска» // Вестник Госатомнадзора России, 2004. № 1. С. 41–49.
14. The International Convergence of Capital Measurement and Capital Standards: a Revised Framework // «Basel II Framework», 2004.
15. ГОСТ Р 51901.1-2002. Менеджмент риска. Анализ риска технологических систем. ГОССТАНДАРТ РОССИИ
16. Ватагин М.Ю. Условно ядерные небалансы. К десятилетию любования стоимостным дисбалансом ядерного топлива.  
<http://www.proatom.ru/modules.php?name=News&file=article&sid=2227>
17. Энциклопедия финансового риск-менеджмента / Под ред. А.А. Лобанова и А.В. Чугунова. М.: Альпина Пабlishер, 2003.

18. Сазыкин Б.В. Какие модели управления нужны российскому банку? // Банковские технологии, 2002. №9.
19. Самад-Хан А., Спивак Г. Современный подход к управлению операционными рисками // Банковское обозрение, 2008. №12.
20. Острейковский В.А. Теория систем. М.: Высшая школа, 1997.
21. Сазыкин Б.В.. Методика анализа банковских операционных рисков. //Труды научных сессий МИФИ. Научная сессия МИФИ-2004. Т.13 Экономика и управление. Международное научно-технологическое сотрудничество. М.: МИФИ, 2004. С.35-36.
22. Стандарты управления рисками. FERMA. Федерация Европейских Риск Менеджеров. 2003.
23. Международная конвергенция измерения капитала и стандартов капитала: новые подходы, июнь 2004 г. (Перевод ЦБР рекомендаций Базельского комитета по банковскому надзору «The International Convergence of Capital Measurement and Capital Standards: a Revised Framework», «Basel II Framework»).
24. International convergence of capital measurement and capital standards. A revised framework comprehensive version. Basel committee on banking supervision. June 2006.
25. Мушик Э., Мюллер П. Методы принятия технических решений: Пер. с нем. М.: Мир, 1990.
26. Reynolds D., Syer D. The actuarial approach to loss distributions. //ALGO research Quarterly, 2002. V. 5. № 2. P. 31-37.
27. Гнеденко Б.В. Курс теории вероятностей. М.: Наука, 1988.
28. The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data Collected. Basel Committee on Banking Supervision, March 2003.
29. Powojowski M., Reynolds D., Tuenter H. Dependent events and operational risk. // Algo Research Quarterly, 2002. V. 5. № 2. P. 65-73.
30. Roehr A. Modelling operational Losses. //ALGO Research Quarterly, 2002. V. 5. № 2. P. 53-64.
31. Круглов В.В., Дли М.И., Голунов Р.Ю. Нечёткая логика и искусственные нейронные сети: Учеб. пособие. М.: Физматлит, 2001.
32. Zadeh L.A. Fuzzy Logic – Computing With Words. // IEEE Transactions on Fuzzy Systems, 1996. V. 4. P. 103-111.
33. Оценка бизнеса: Учебник/ Под ред. А.Г. Грязновой, М.А. Федотовой. – 2-е изд., перераб. и доп. М.: Финансы и статистика, 2004.
34. Козлов А.А., Хмельёв А.О. Качество кредитной организации: стоимость процессов. //Деньги и кредит, 2003. № 7.
35. Максутов Ю.Г., Алехин Р.В. Использование методики ФСА для определения себестоимости банковских продуктов. // Аудит и финансовый анализ, 2000. № 2.

36. Jordan J, Rosengren E. Using Loss to Quantify Operational Risk. April 2003 ([www.bis.org](http://www.bis.org)).
37. Сазыкин Б.В. Новые подходы в управлении операционными рисками банка.// Методические материалы семинара ИБД АРБ. Февраль 2007.
38. Шендрик Н.Н. Планирование объемов ремонтов оборудования для блоков АЭС с учетом его фактического состояния (<http://www.prostoev.net/modules/myarticles/article.php?storyid=52>)
39. Фролова Т.А.. Экономика предприятия: конспект лекций. Таганрог: Изд-во ТРТУ, 2005. ([http://www.aup.ru/books/m170/3\\_5.htm](http://www.aup.ru/books/m170/3_5.htm)).
40. Сазыкин Б.В. Управление операционным риском в коммерческом банке. М.: Вершина, 2008.
41. Лекции по надежности. ( <http://www.prostoev.net/search.php>).
42. Ершов М.С., Скреплев И. В. Модели планирования ремонтов и замен промышленного электрооборудования. // Промышленная энергетика, 2005. № 11. С.46-51.
43. Отчет «Атомэнергопроект». Научно-исследовательская работа: Углубленная оценка безопасности энергоблока. Система технического водоснабжения. Инв.№ 1517-63Т, 2004.
44. Отчет «Атомэнергопроект». Научно-исследовательская работа: Углубленная оценка безопасности энергоблока Система технического водоснабжения. Инв. № 1517-51Т, Изм.1
45. Розанов М.Н. Надёжность электроэнергетических систем: Справочник. М.: Энергоатомиздат, 2000.
46. Самохин Д.С. Оценка показателей надёжности элементов оборудования и персонала объектов ядерных технологий по нечётко-вероятностным моделям: Автореферат диссертации учёной степени кандидата технических наук. Обнинский государственный университет атомной энергетики. Обнинск, 2009.
47. Савелли Ф. Экономика ядерной энергетики в странах ОЭСР // Ядерное общество, 2000. № 5-6. (<http://nppdec.by.ru/docs/nuksoc/005636.htm>)

**КЛАССЫ НАПРАВЛЕНИЙ ДЕЯТЕЛЬНОСТИ АЭС  
И КЛАССЫ СОБЫТИЙ**

<b>Класс</b>	<b>Направления деятельности (РД ЭО 0348-02)</b>
1	Организация эксплуатации атомной станции
2	Эксплуатация территории, зданий, сооружений, устройств
3	Эксплуатация гидротехнических сооружений и водное хозяйство
4	Эксплуатация тепломеханического оборудования и тепловых сетей
5	Эксплуатация специального оборудования атомной станции
6	Эксплуатация электрического оборудования и сетей
7	Оперативно-диспетчерское управление производством и потреблением тепловой и электрической энергии
<b>Класс</b>	<b>События /источники рисков (US NRC, ROP, 2007)</b>
1	Контроль проекта
2	Воздействие и защита от внешних факторов
3	Контроль конфигурации (оборудование остановлено/работает)
4	Работа оборудования (надёжность/готовность)
5	Качество процесса и процедур управления
6	Работа персонала (ошибки, злоупотребления, кадровая политика, безопасность труда)

**ПРИМЕРЫ СТРУКТУРНЫХ МОДЕЛЕЙ БИЗНЕС-ПРОЦЕССОВ**

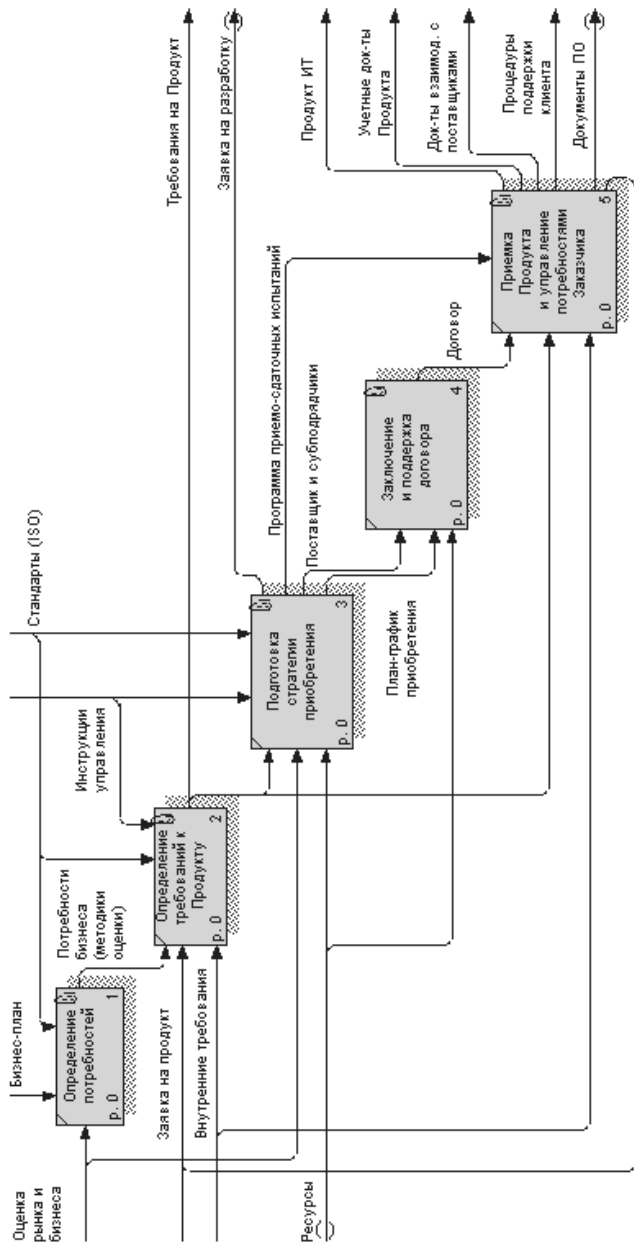


Рис. П2.1. А11 «Приобретение необходимого ПО и оборудования (Продукта)»

(Здесь и далее на рисунках не показаны механизмы реализации бизнес-функций, чтобы не затруднять структурные модели)

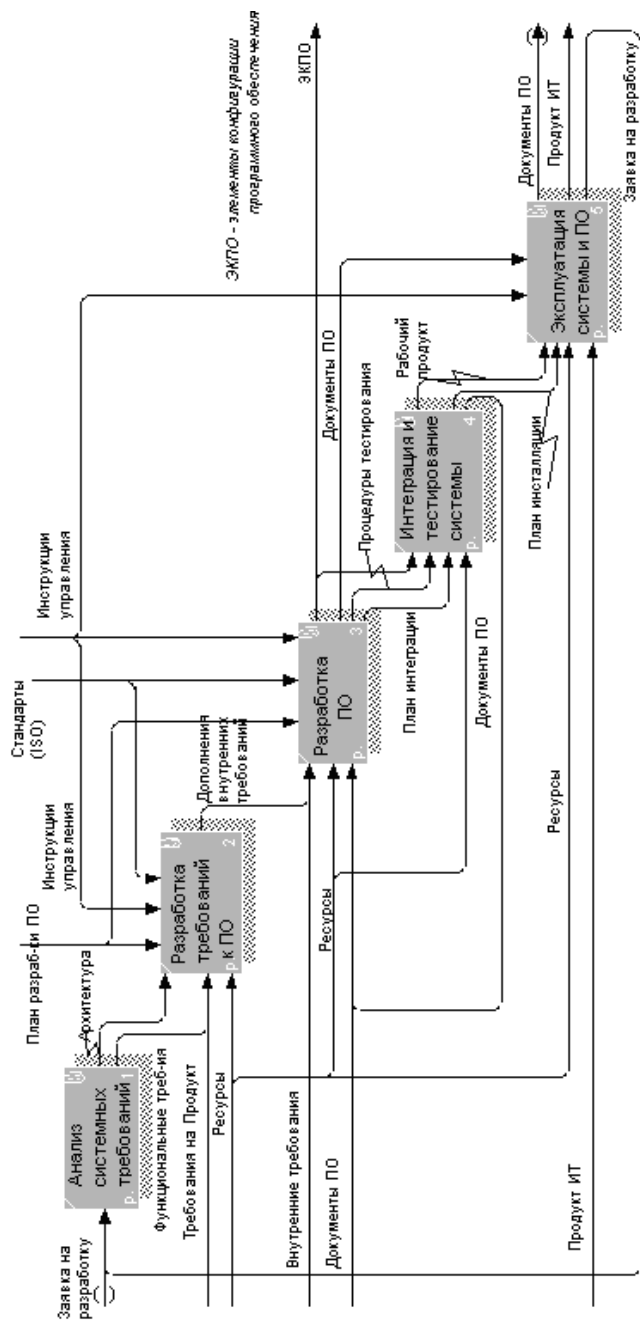


Рис. П2.2. А12 «Разработка ПО и эксплуатация»



## Примеры анкеты и результаты ответов эксперта для БФ «Определение требований к Продукту»

Таблица П2.1. Оценка индикаторов технологического риска

№ п/п	Вопрос для оценки фактора	Да = 0, Нет = 1	Балл
1	Определяются ли различные точки зрения (финансовая, юридическая, техническая, управленческая, техническая) на требования к Продукту, отвечающему нуждам Заказчика?	-	0
2	Требования регулярно пересматриваются в соответствии с нуждами Заказчика?	-	0
3	Анализируются ли требования безопасности, надежности, сопровождаемости и эффективности Продукта?	-	0
4	Соответствуют ли требования на Продукт стандарту ИСО 8402	1	2
5	Утверждается ли документ требований (спецификация) на Продукт?	1	2
	ИТ	2	4

144

Таблица П2.2. Оценка индикаторов событийного риска

№ п/п	Вопрос для оценки фактора	Да=0, Нет=1	Балл
1	Возможны ли НЕКВАЛИФИЦИРОВАННЫЕ или ЗЛОУМЫШЛЕННЫЕ действия персонала при реализации БФ?	-	0
2	Чувствительна ли БФ к последствиям УПРАТЫ в результате аварий и катастроф? (т.е трудно ли восстановить БФ?)	-	0
3	Существует ли зависимость от «НЕЗАМЕНИМЫХ» исполнителей?		
4	Зависит ли БФ от юридически некорректных документов?	1	2
5	Имели ли место случаи невыполнения должностных обязанностей при реализации БФ?	-	-
	ИС	1	2
	Операционный риск ПОР	-	<b>0,325</b>