ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

МОСКОВСКИЙ ИНЖЕНЕРНО-ФИЗИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

Н.И. Гераскин

КРИТЕРИИ БЕЗОПАСНОСТИ, ОЦЕНКА ЭФФЕКТИВНОСТИ И РИСКА В ЗАДАЧАХ ЗАЩИТЫ ЯДЕРНЫХ ОБЪЕКТОВ И МАТЕРИАЛОВ

Рекомендовано УМО «Ядерные физика и технологии»
в качестве учебного пособия
для студентов высших учебных заведений

Москва 2008

УДК 621.039.58(075)
ББК 31.46я7
Г37

Гераскин Н.И**. Критерии безопасности, оценка эффективности и риска в задачах защиты ядерных объектов и материалов:** *Учебное пособие*. М.: МИФИ, 2008. 96 с.

Пособие посвящено вопросам системного анализа эффективности, безопасности и надежности систем физической защиты (СФЗ), учета и контроля (У и К) объектов с ядерными материалами (ЯМ), а также систем ЯЭУ. Основная цель – дать необходимую теоретическую базу и ознакомить с методами решения задач оценки эффективности, которая трактуется как оптимизационная задача с ограничениями безопасности, учета неопределенностей, возникающих в ядерной энергетике, и при обеспечении безопасного обращения с ЯМ.

Предназначено для студентов, специализирующихся в области учета, контроля ЯМ и физической защиты ядерноопасных объектов, для будущих специалистов ядерного топливного цикла. Оно может быть полезно студентам старших курсов и аспирантам при изучении вопросов оценки эффективности и риска.

Данное пособие рекомендовано студентам, обучающимся по направлению подготовки 140300 «Ядерные физика и технологии».

Пособие подготовлено в рамках Инновационной образовательной программы.

Рецензент канд. техн. наук И.Г. Меринов

ISBN 978-5-7262-1058-2

ОГЛАВЛЕНИЕ

ЗАДАЧИ ОБОСНОВАНИЯ НАДЕЖНОСТИ, БЕЗОПАСНОСТИ И ОЦЕНКИ ЭФФЕКТИВНОСТИ В СИСТЕМЕ ФЗУ И К ЯМ

Данное пособие посвящено вопросам системного анализа эффективности, безопасности и надежности ядерных объектов и в первую очередь систем физической защиты (СФЗ) ядерно-опасных объектов (ЯОО) и систем учета и контроля (У и К) ядерных материалов (ЯМ). В пособии задача оценки эффективности трактуется как оптимизационная задача с ограничениями. Уделяется особое внимание вероятностным методам, что требует знания основ теории вероятностей и статистики. Дается знакомство с методами учета неопределенностей. Приводится общий подход к задачам, позволяющий выбирать решения, учитывая их экономический эффект. Рассматривается ряд основных понятий и методов теории надежности.

Если рассмотреть известную триаду, обеспечивающую безопасное обращение и нераспространение ЯМ и включающую в себя:

- физическую защиту ядерно-опасных объектов;
- учет ядерных материалов;
- контроль ЯМ,

то станет очевидным нетривиальность задачи анализа и оценки эффективности и достаточности СФЗ ЯОО и систем У и К ЯМ, входящих в триаду. Речь, конечно, должна идти о количественной оценке эффективности и достаточности, поскольку в конечном итоге было бы крайне желательно сравнивать различные варианты указанных систем и степень их интеграции, чтобы иметь возможность на основе *количественной* оценки делать однозначный выбор в пользу одного из предлагаемых решений.

Переходя к изучению методов оценки эффективности, неизбежно столкновение с необходимостью оценивать *безопасность* систем и установок, поскольку в конечном счете удовлетворение приемлемому уровню безопасности при минимизации дисконтированных затрат и будет, очевидно, решением поставленной задачи. И если удастся дать приемлемое количественное описание безопасности и правильно соизмерить разновременные затраты на созда-

ние и функционирование систем с возможными потерями в уровне безопасности, то очевидно, что, в конечном итоге, исходные задачи можно будет свести к *оптимизационным задачам*. И тогда потребуется кратко ознакомиться с известными подходами к их решению.

Оценка эффективности, безусловно, включает в себя как подзадачу оценку надежной работоспособности систем, причем не всегда и, более того, почти никогда нельзя моделировать те или иные нештатные ситуации (аварии, сбои, нападения и т.п.) на работающих объектах путем экспериментальных проверок. А это приводит к необходимости ознакомиться с основными понятиями и методами теории *надежности*.

Решая задачи анализа безопасности, надежности и оценки эффективности, ту или иную оптимизационную задачи, к которым возможно удастся свести исходные задачи, придется учесть, что исходная информация известна нам с разной степенью *неопределенности*. Это потребует необходимого знакомства с методами оценки и учета разных видов неопределенной информации как при решении оптимизационных задач, так и в задачах принятия решения.

Таким образом, теоретическая основа курса – вероятностные методы, методы анализа надежности и безопасности, методы решения сложных оптимизационных задач в условиях неопределенности исходной информации.

Глава 1
ПОНЯТИЕ РИСКА. ФАКТОРЫ ВОСПРИЯТИЯ РИСКА

Что такое безопасность? Это – полное или частичное отсутствие опасности. Причем совершенно очевидно, что скорее частичное, чем полное ее отсутствие. Значит, безопасность – это непревышение некоторых барьеров, ограничений некоторого *приемлемого уровня* опасности. Совершенно очевидно, что полное отсутствие опасности от любой функционирующей системы или объекта – нонсенс, невозможное событие.

Любые виды деятельности человека характеризуются наличием опасности (риска) возникновения аварий с серьезными последст-

виями. Для каждого вида деятельности риск специфичен так же, как и меры по его уменьшению. Особенностью объектов ядерной энергетики (ЯЭ) является существование значительных количеств радиоактивных веществ. Специфика риска ядерно-опасных объектов – потенциальная радиологическая опасность для персонала, населения и окружающей среды.

Безопасность – это отсутствие неприемлемого риска

Для того чтобы перейти к дальнейшему рассмотрению аспектов безопасности, надо получить ответы на следующие вопросы:

- что мы считаем опасным, или чего боимся;
- как воспринимается риск индивидуумом и обществом;
- как исторически развивались подходы к обеспечению и оценке безопасности.

На первый вопрос следует ответить, что боимся мы не опасность саму по себе, не аварию или нежелательное событие, а последствия, которые за этим событием наступают. При рассмотрении безопасности ЯЭ и ЯОО, в частности, особую озабоченность вызывают следующие потенциальные последствия:

1) немедленные смертельные случаи и травмы;

2) латентные (скрытые) смертельные случаи и заболевания в настоящем и будущем;

3) материальный ущерб;

4) ущерб для общества и/или его институтов.

Избежать этих последствий с достаточной уверенностью и минимумом затрат, значит, обеспечить безопасность системы или объекта, а в случае СФЗУ и К ЯМ – обеспечить эффективность системы.

Существует количественная мера, позволяющая характеризовать безопасность, – риск R. Введем следующим образом риск от некоторого события:

$$R_i = p_i S_i, \tag{1.1}$$

где p_i – вероятность события; S_i – оценка последствий (ущерба) от события.

Рассмотрим множество возможных событий I, i = 1,…, N. Поскольку очевидно, что возможный ущерб будет включать в себя различные составляющие (экономическую, экологическую, социальную и т.п.), он, безусловно, будет величиной многофакторной, но тогда и риск будет многофакторной характеристикой. А суммарный риск функционирования системы будет суммой рисков всех рассматриваемых возможных событий:

$$\vec{R} = \sum_{i=1}^{N} R_i = \sum_{i=1}^{N} p_i \vec{S}_i \,, \tag{1.2}$$

где $\vec{S}_i$ – вектор возможных последствий данного события, имеющий своими компонентами различные составляющие: экономическую, экологическую, социальную и т.п.

Отметим, что ущерб удобнее всего было бы выражать в денежных единицах, что и постараемся делать в дальнейшем, и тогда риск также имеет размерность стоимости ущерба (рубли, доллары, и т.п.).

Таким образом, главными вопросами рассмотрения безопасности будут:

- как оценить вероятность каждого возможного нежелательного события;
- в чем и как измерять последствия или ущерб от возможного нежелательного события;
- как назначить или оценить границу приемлемого риска $R^{\text{доп}}$.

Так как в случае обоснованных ответов на поставленные вопросы, задача сводится к поиску таких параметров рассматриваемых систем или объектов, при которых выполняется условие:

$$R \le R^{\text{доп}} . \tag{1.3}$$

Введем понятие *допустимого риска* – это допущение того, что система защиты не может обеспечить 100%-ю защиту (безопасность) во всех возможных ситуациях, однако дальнейшее улучшение такой системы не оправдано, так как окажется, что затраты на улучшение превышают доход, выгоду от функционирования системы во всех смыслах. Таким образом, совершенно очевидно, что объективно существует некоторый приемлемый уровень риска, так

как человечество всегда выбирало и осознанно или неосознанно решало, по сути, оптимизационную задачу получения наибольших выгод с наименьшим риском.

На развитие ядерной энергетики (ЯЭ) в целом, включая и ЯОО и обращение с ЯМ, оказывает как реальная, присущая ей безопасность (или уровень риска), так и безопасность как она воспринимается населением (обществом). Поэтому в своих решениях необходимо учитывать субъективные *факторы восприятия риска,* к которым относятся факторы:

управления риском;

масштаба;

привычности риска.

Первый фактор учитывает тот факт, что человек и общество легче воспринимает риск определенного уровня, если имеется возможность им управлять. Примеры: курение, переход дороги в неположенном месте и т.д.

Второй фактор учитывает тот факт, что в целом общество значительно болезненнее воспринимает одновременную гибель 100 человек (например, в авиакатастрофе), чем ежегодную гибель 50 000 человек (например, в автокатастрофах в целом по стране).

Последний фактор очевиден – привычный риск кажется более приемлемым по сравнению с таким же по величине неизвестным риском. Пример: электричество в быту.

Поскольку факторы восприятия риска вполне объективны, можно сделать следующие выводы:

- отношение к риску является во многом психологическим моментом и по природе своей нерационально;
- приемлемость риска будет регулироваться не только объективными причинами, но и тремя вышеприведенными факторами;
- определение приемлемых уровней риска и обеспечение их соблюдения для опасных объектов и систем должно относиться к сфере деятельности регулирующих, а не эксплуатирующих органов;
- критерий безопасности (глобальный как требование к уровню риска) должен определяться стандартом, который по своей природе хотя бы в части своей является субъективным.

Совершено очевидным становится соотношение безопасности и надежности: методы оценки безопасности и риска начинаются там,

где кончается надежная работа (функционирование) объекта в установленных регламентом рамках. Можно сказать, что риск возникает вместе с аварией. Дадим определение понятию авария.

Авария – нештатная ситуация с выходом контролируемых параметров за рамки регламента.

Тогда хищение ЯМ – авария; сбой в работе ФЗ – авария; выход ядерного реактора из-под контроля – авария и т.п.

Исторически были развиты два подхода к оценке безопасности и риска (для ЯЭУ подробнее см. приложение): детерминированный и вероятностный.

Детерминированный подход (в рамках концепции проектной аварии и принципа единичного отказа) подразумевает, что каждая система безопасности должна выполнять заданные функции при любом исходном событии аварии, требующем ее работы, с учетом одного отказа любого элемента. Проектные исходные события, приводящие к аварии, а также пределы, на соблюдение которых направлена защита, устанавливают из накопленного опыта и инженерной интуиции.

При данном подходе, очевидно, неполно учитываются все возможные ситуации и не может быть речи о получении *количественной оценки* безопасности.

Основой *вероятностного подхода* [1] является системный количественный анализ мыслимых сценариев аварий (случаев), а также последовательное исследование каждого случая, включая пути развития процессов и ситуаций, с учетом наложенных отказов элементов системы, масштаба последствий, влияния неопределенностей и человеческого фактора.

Наиболее важными направлениями использования вероятностного анализа являются:

- сравнительный анализ технических решений по установке и системам безопасности (вероятностные оценки позволяют сделать обоснованный выбор между конкурирующими решениями, а также исследовать чувствительность результатов к изменению исходных параметров);
- регламентные проверки систем безопасности (количественные исследования дают возможность определить оптимальную периодичность проверок);

• оценка вклада различных факторов и систем в показатели защищенности и выбор приоритетных направлений ее повышения.

Глава 2
ОСНОВНЫЕ КОЛИЧЕСТВЕННЫЕ КРИТЕРИИ ПРИЕМЛЕМОГО РИСКА И УЧЕТ ЭКОНОМИКИ ПРИ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМ

Количественные оценки риска имеют вероятностный характер. Впервые количественный подход к оценке риска применительно к ядерным установкам был развит в работах Фармера в 1967 г. Поскольку оценка риска в виде (1.2) и решение задачи (1.3) в явном виде затруднительно, поскольку многофакторные последствия S крайне сложно оценить, Фармер предложил подход, согласно которому авария с заданными последствиями считается неприемлемой, если ее вероятность больше определенной допустимой вероятности:

$$p_i \geq p_0 .$$

Если $p_i \geq p_0$, то в систему должны быть внесены изменения, уменьшающие значение вероятности i-го события.

Этот подход, безусловно, позволял учитывать неприемлемость крупных рисков и уходить от возможных спекуляций и неопределенностей в оценке последствий, но не отвечал на вопросы о выборе допустимого значения риска (1.3) и не учитывал многофакторность последствий и риска. Опыт показал, что без привлечения экономических категорий решить комплексно данные проблемы вряд ли возможно.

Рассмотрим на примере метода экономического анализа безопасности (МЭАБ), предложенного Я.В. Шевелевым [2], общие методологические подходы к безопасности, позволяющие решить указанные проблемы. Эти подходы разрабатывались и применялись для обоснования снижения доз облучения ниже дозовых пределов и, тем самым, снижения соответствующего риска, но в каче-

стве методологии МЭАБ как нельзя лучше применим для комплексной оценки эффективности мер безопасности и защиты.

Общество недооценивает объективную необходимость создания опасных для людей и природы производств и объектов. Эта недооценка выражается обычно в требовании: либо гарантировать абсолютную невозможность аварий, либо отказаться от создания таких объектов. Заметим, однако, что цивилизация не только удлинила и украсила жизнь человека, но внесла в нее техногенные опасности. Свести их к нулю можно, только вернув общество к первобытному состоянию. Сфера обращения ядерных материалов – ЯЭ – благодаря высоким технологиям и принятым дорогостоящим мерам защиты может характеризоваться высоким уровнем безопасности. Однако справедливо спросить, до какого уровня оправдан рост расходов на безопасность. Речь идет об оптимизации усилий общества по улучшению безопасности. Заметим при этом, что общество всегда располагает ограниченным потенциалом средств. Все это и поставило проблему разработки универсальных принципов и методов анализа безопасности, а также оптимизации мер по ее обеспечению.

Попробуем ответить на «простой» вопрос: нужно ли знать меру в обеспечении безопасности? Часто главным принципом обеспечения безопасности считают требование обеспечения «нулевой опасности» или «абсолютной безопасности». Можно ли путем увеличения расходов на защиту достичь «абсолютной безопасности»? Покажем, что чаще всего нет.

На рис. 1 приведены две принципиально отличающиеся возможности зависимости риска R от затрат З на защиту:

1) функционирование системы возможно с нулевой опасностью, например пороговое воздействие вредных последствий;

2) функционирование системы невозможно с нулевой опасностью (непрерывная зависимость, т.е. беспороговое воздействие опасных последствий).

Для ядерных объектов характерна вторая кривая: как бы мал ни был уровень радиационного облучения, он будет создавать ненулевой радиационный риск.

Существует точка зрения, что любые затраты на защиту человека оправданы ибо ему нет цены. Это так называемый принцип

ALAPA (as low as practically achieved) – установление уровня опасности настолько низким, насколько это достижимо практически. Подход привлекательный, но не научный и не осуществимый практически. Последовательное применение этого подхода приводит к неэффективному расходованию средств на защиту и к возрастанию опасности.

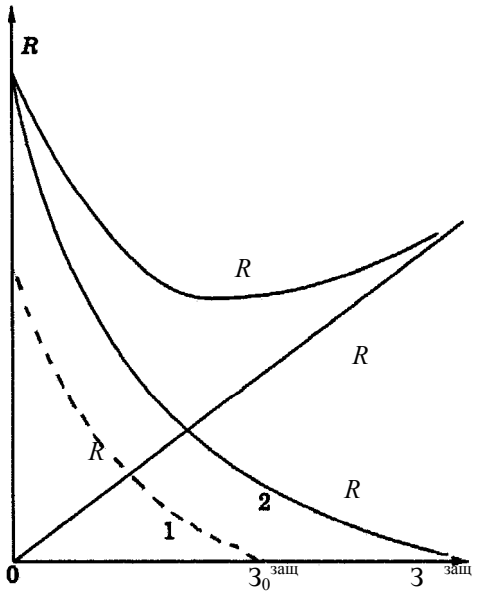

Рис. 1. Зависимость риска от затрат на защиту

Поскольку совершенно безопасных технологий нет вообще, следует учесть, что помимо прямого риска (кривые *1* и *2* на рис.1) есть и косвенный. Косвенный риск обусловлен ростом масштаба затрат (строительные работы, изготовление оборудования и т.п.). Действительно с ростом расходов (затрат) прямая составляющая риска падает, а риск косвенный только растет. Учитывая это, получим для суммарного риска:

$$R = R_{\text{прям}} + R_{\text{косв}}.$$

Очевидно, что, начиная с некоторого уровня затрат, будет происходить возрастание полного риска. Тогда кривая полного риска должна иметь явный минимум при определенном уровне затрат.

Признание невозможности и даже нецелесообразности достижения «нулевой опасности» ставит проблему определения *приемлемого уровня* риска или установления меры в обеспечении безопасности.

Возможно несколько подходов:

- риск считать приемлемым, если новая технология приводит к снижению (не увеличивает) полного риска для общества (следует заметить, что в этом случае рассматриваются целые технологии, он вряд ли применим для отдельных установок и объектов);
- применить оптимизацию расходов на безопасность, в которой критерием оптимальности будет минимум полного риска (см. рис. 1).

Второй подход очень близок к так называемой идеологии принципа ALARA (as low as reasonably achieved) – установлению уровня опасности, которое настолько низко, насколько это *разумно достижимо*.

Можно увидеть, что в обоих случаях установление приемлемого риска исходит из единого критерия – увеличения продолжительности жизни человека или уменьшения уровня риска. Эти подходы разумны в отличие от ALAPA, но не оптимальны. Они разумны для неглобальных технологий (как по масштабу средств, так и по последствиям). Действительно, учет ограниченности средств общества приведет к существенно другим результатам при решении оптимизационной задачи на минимум полного риска. Так как затраты на достаточно дорогостоящие защитные мероприятия могут брать средства из других областей, в частности из тех, где формируется качество жизни. Таким образом, при принятии решения об оптимальных затратах необходимо сопоставление показателей риска и расходов на защиту. Это наиболее последовательно позволяет сделать МЭАБ. Фактически МЭАБ – принцип ALARA с учетом экономических и социальных факторов.

Согласно МЭАБ данное мероприятие, связанное с тем или иным риском, считается оправданным, если получаемый от него приве-

денный к определенному моменту (t = 0) чистый экономический эффект $D(0)$ больше нуля:

$$D(0) = Э(0) - З^{осн}(0) - З^{защ}(0) - У(0), \qquad (2.1)$$

где $Э(0)$ – приведенный к моменту t = 0 полный экономический эффект; $З^{осн}(0)$ – основные приведенные к моменту t = 0 затраты (без затрат на обеспечение безопасности); $З^{защ}(0)$ – приведенные затраты на защиту; $У(0)$ – приведенный ущерб (риск).

Под приведением разновременных затрат мы традиционно понимаем их дисконтирование, т.е. интегрирование соответствующих составляющих затрат по времени с экспоненциальной функцией дисконтирования, например:

$$З(0) = \int_{-\infty}^{\infty} З(t) \cdot \exp(-tp)dt,$$

где p – норматив дисконтирования, а момент приведения выбран t = 0.

Применять дисконтирование в задачах оценки безопасности или нет – определяется не характером показателя, который оценивается в данной задаче – ущерб здоровью или потеря материальных благ, а характером рассматриваемого фактора. Если данный фактор можно считать экономическим, то дисконтирование совершенно необходимо. К каким фатальным ошибкам приводит не учет дисконтирования в этих случаях, отлично показано на конкретных примерах в монографии [2].

Критерием оптимальности мероприятий или технологии с точки зрения безопасности служит максимум величины $D(0)$. А критерием оптимальности конкретной меры защиты (безопасности) на объекте или предприятии (АЭС, хранилище, завод и т.д.), когда основные технологические и экономические характеристики производства фиксированы (т.е. $Э(0) = \text{const}$ и $З^{осн}(0) = \text{const}$), служит минимум величины $З(0)$:

$$З(0) = З^{защ}(0) + У(0). \qquad (2.2)$$

Этот критерий можно сформулировать как минимум обобщенных приведенных затрат (рис. 2).

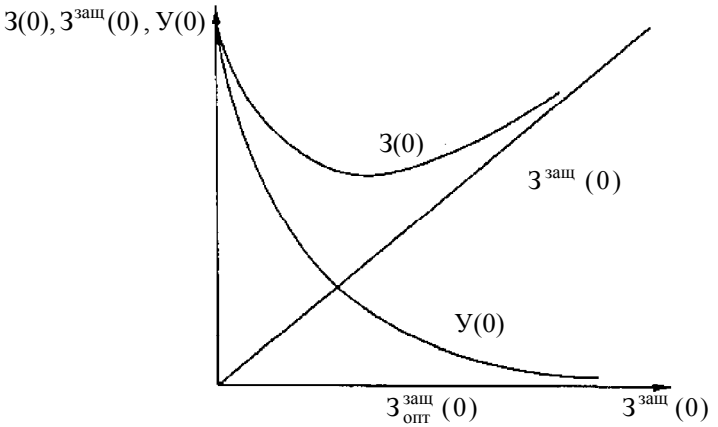

Рис. 2. Зависимость обобщенных приведенных затрат от затрат на защиту

Последний критерий (2.2) иногда используется в другой, эквивалентной форме как максимум приведенного чистого экономического эффекта от данной меры защиты:

$$D^{\text{защ}}(0) = Э^{\text{защ}}(0) - З^{\text{защ}}(0), \qquad (2.3)$$

где $Э^{\text{защ}}(0) = У(0)_{R_{\text{нач}}} - У(0)_{R_{\text{достигнутое}}}$; $R_{\text{нач}}$ и $R_{\text{достигнутое}}$ – риски до и после принятия данной меры защиты.

Величина (2.3) может служить критерием эффективности мер защиты: данная конкретная мера защиты оправдана, если для нее $D^{\text{защ}}(0) \geq 0$.

Один из основных недостатков МАЭБ пока заключен в недостатке исходной информации и недостаточной проработанности количественной (экономической) оценки последствий. Действительно, каким образом и можно ли вообще, всем факторам, вовлекае-

мым в экономический анализ безопасности, обоснованно сопоставить соответствующие цены?

Для ответа на данный вопрос рассмотрим более подробно безопасность как экономический фактор и цену риска.

Что такое экономический фактор? Многие факторы (чистый воздух, пейзаж, и т.п.) могут быть очень сложно учтены при оценке безопасности и только в той своей малой части, в какой они через посредство здоровья отражены в затратах на медицинское обслуживание. Но люди ценят свое здоровье вне зависимости от того, во что оно обходится. А здоровье – экономический фактор так же, как и продолжительность жизни.

Экономическим следует считать любой фактор, удовлетворяющий двум условиям:

- этот фактор может влиять прямо или опосредованно на жизнь человека и общество в целом;
- человек может иметь реальную возможность изменять влияние фактора на жизнь людей и общества.

Таким образом, очевидно, что *безопасность и ее количественная мера – риск являются экономическими факторами*, но только в той своей части, в которой человек в состоянии ими управлять.

Ранее было рассмотрено, как включить безопасность в экономический анализ; локальные задачи оптимизации, возникающие при этом, решаются известными методами (см. гл. 6). Однако глобальный критерий оптимизации усилий всего общества должен включать два показателя – *безопасность и качество жизни*. В комплексе жизненных благ, ценимых человеком, безопасность занимает видное, но самодовлеющее место. Ее вес в жизни человека соизмерим с весами материальных и духовных благ, не удлиняющих жизнь, а повышающих ее качество. Введем величину, характеризующую личную безопасность, – это ожидаемая продолжительность предстоящей жизни или ее обратная величина – личный риск. Переходя к количественным оценкам, следует также учесть, что качество жизни и риск уравновешивают в определенной мере друг друга. Действительно в повседневной практике люди обычно допускают увеличение риска в обмен на качество жизни.

На рис. 3 изображены *1* – кривые постоянного уровня жизни, поэтому они идут не горизонтально, а наклонно; *2* – кривая эконо-

мических возможностей данного общества. Цивилизация удлиняет жизнь, но сделать ее полностью безопасной не может. Оптимальное распределение затрат между безопасностью и качеством жизни дает точка касания двух кривых. Общий наклон кривых в этой точке – коэффициент пересчета равноценных, компенсирующих друг друга изменений качества жизни и безопасности. Это фактически *цена безопасности* при данном уровне развития общества. Таким образом, все факторы, вовлекаемые в экономический анализ, приобретают цены. Цена единицы фактора – мера его возможности изменить уровень жизни при данном уровне развития общества.

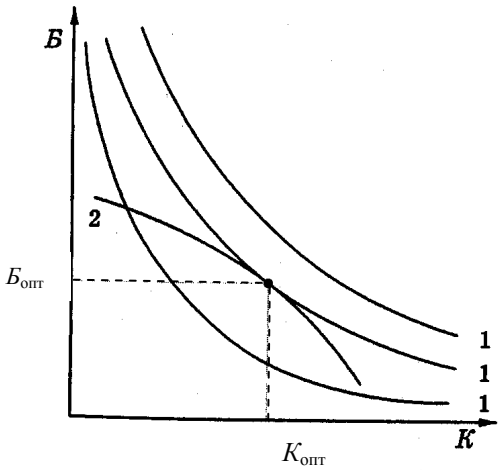

Рис. 3. Безопасность и качество жизни

Есть возможность получить и субъективную цену риска. Наибольшую информацию тут могут дать результаты статистических исследований на тему: какую дополнительную зарплату или иные вполне измеряемые материальные блага человек считает достаточной компенсацией данного дополнительного риска.

Итак, трактуя риск как экономический фактор, используя дисконтированные значения ущерба и затрат, задачу повышения безопасности или повышения эффективности мер безопасности и защиты можно формализовать и свести к оптимизационной задаче.

Глава 3
ОСНОВНЫЕ ПОНЯТИЯ И МЕТОДЫ ТЕОРИИ НАДЕЖНОСТИ

3.1. Классификация методов оценки надежности

Надежность – один из критериев безопасной и эффективной работы любой системы или устройства. Система защиты эффективна только в той мере, в какой она надежна. Понятие надежности очень близко понятию безопасности, однако безопасность включает в себя надежность как совершенно необходимое требование, но не достаточное.

Любой объект, система обладают определенным качеством, т.е. совокупностью свойств, обуславливающих и определяющих пригодность объекта удовлетворять вполне определенные потребности в соответствии с его назначением. Одним из важнейших свойств является *надежность*.

Под надежностью понимается свойство объекта, системы, установки сохранять в установленных пределах во времени значения всех параметров, характеризующих способность выполнять свои основные функции.

Надежность – комплексное свойство, иногда с целью более полного анализа в надежности выделяют отдельные составляющие: безотказность, долговечность, ремонтопригодность и т.д. [3]. Нас же будет интересовать надежность именно как комплексное свойство.

Количественные методы оценки надежности можно разбить на два класса:

- прямые, заключающиеся в непосредственной оценке показателей надежности в результате статистической обработки данных по эксплуатации системы или установки;
- косвенные, заключающиеся в оценке показателей надежности системы или установки, исходя из ее структурной схемы и характеристик составляющих ее элементов.

Очевидно, что первые применимы только на этапе эксплуатации. В свою очередь вторые возможны и на этапе эксплуатации, и на этапе проектирования и создания системы или установки. Ино-

гда косвенные методы называют методами расчета структурной надежности (МРСН).

Методы расчета структурной надежности подразделяют на аналитические и метод статистического моделирования Монте-Карло.

Аналитические менее трудоемки и более оперативны, поэтому они получили более широкое распространения, хотя в последнее время с ростом мощности компьютерных систем все большее внимание уделяется методу Монте-Карло.

В свою очередь аналитические методы подразделяются на:

- *логико-вероятностные* (графоаналитические), булевы методы;
- методы, базирующиеся на теории дискретных марковских процессов.

На практике больше используются логико-вероятностные или так называемые булевы методы, основывающиеся на понятии *минимальных сечений*. Причина в том, что у этих методов большие возможности при оценке сложных многоэлементных структур (например, таких, как ЯЭУ, СФЗ ЯОО и т.п.).

Булевыми эти методы называют потому, что они распространяются на *структурные схемы* объектов, состоящих из элементов, которые могут находится только в двух состояниях: работоспособном ($x = 0$) и неработоспособном или состоянии отказа ($x = 1$). Бинарная переменная x, таким образом, является характеристикой состояния элемента. Это дает возможность применить для исследования объекта алгебру логики, так называемую булеву двоичную алгебру, оперирующую с указанными переменными бинарных элементов.

3.2. Метод минимальных сечений и использование марковских процессов

Очевидно, что состояние системы в целом определяется состоянием ее составляющих элементов и если они бинарные (а в подавляющем большинстве случаев это справедливо), может быть записано в виде следующей двоичной структурной функции:

$$f(x_1, x_2, ..., x_i, ..., x_n) \quad \text{или} \quad n\text{-мерного вектора} \quad \{x_i\},$$

где n – полное число элементов в системе; x_i – двоичная переменная, принимающая значение 0 в работоспособном и 1 – в неработоспособном состоянии.

Множество значений структурной функции $f(0, 0, ..., 0)$, $f(0, 0, ..., 1), ..., f(1, 1, ..., 1)$ образует множество всех возможных состояний системы, отличающихся состоянием составляющих ее элементов. В процессе функционирования система переходит из одного состояния в другое (например, в результате отказов или восстановления некоторых элементов).

Отметим, что если этот процесс моделируется, как случайный дискретный марковский процесс перехода из одного состояния в другое, то можно, используя развитую теорию марковских процессов, рассчитать структурную надежность системы в каждый момент времени.

Легко сообразить, что полное число состояний, в которых может находиться рассматриваемая система будет равно 2^n. Для реального многокомпонентного объекта или системы вряд ли возможно, перебирая «вручную» миллионы и миллионы состояний, задать и исследовать интересующие нас области состояний системы. Для облегчения задачи введем понятие *минимального (критического) сечения*, которое позволяет упростить задачу.

Минимальным сечением называется минимальная группа элементов структурной схемы рассматриваемого объекта (системы), отказ которых приводит к отказу объекта, а восстановление хотя бы одного из этих элементов – к восстановлению объекта относительно указанного отказа. В терминах, принятых в теории надежности, применительно к ядерным объектам (ЯЭУ и др.) минимальное сечение часто называют *критической группой элементов* (КГЭ).

Показано, что если структура системы является монотонной [3], то область неработоспособных состояний может быть задана полным набором минимальных сечений (или КГЭ) – перечнем всех различающихся КГЭ для рассматриваемой структурной схемы. Число таких КГЭ обычно намного меньше полного числа состояний. Не вводя строгого определения понятия монотонности структуры, заметим, что все рассматриваемые нами объекты и системы являются структурно-монотонными.

Напомним, что в терминах теории вероятностей [4] отказ отдельной КГЭ представляет собой произведение вероятностей событий – отказов входящих в нее отдельных элементов. Поскольку отказ системы наступает при отказе хотя бы одной КГЭ из полного набора, то вероятность отказа системы представляет собой сумму событий – отказов отдельных КГЭ. Используя данные обстоятельства, по известным теоремам сложения и умножения вероятностей можно найти количественные (вероятностные по своей природе) показатели эффективности или надежности системы.

Метод КГЭ и его модификации позволяют определить все необходимые показатели надежности и оценить эффективность системы в зависимости от времени эксплуатации при произвольных законах надежности отдельных элементов, например при произвольном законе распределения *наработки элементов на отказ.* Главным допущением и недостатком метода является предположение о *независимости* отказов элементов.

В отличие от метода КГЭ метод расчета структурной надежности системы на основе марковских процессов позволяет получить показатели системы в виде непрерывных функций времени, что невозможно сделать другими методами. Но он кроме независимости отказов обычно применим только в случае экспоненциальных законов наработки на отказ, правда это ограничение касается только восстанавливаемых элементов.

В качестве вероятностной характеристики надежности отдельного элемента введем понятие *наработки на отказ.* Функция распределения $F(t)$ наработки до отказа Θ – вероятность отказа на интервале (0, t). Иногда используют также вероятность безотказной работы $R(t)$, интенсивность отказов $\lambda(t)$ в момент t и среднюю наработку до отказа $\overline{\Theta}$:

$$R(t) = 1 - F(T);\ \lambda(t) = \frac{f(t)}{1 - F(t)}\ ;\ \overline{\Theta} = \int_0^\infty t f(t)dt = \int_0^\infty R(t)dt\ , \qquad (3.1)$$

где $f(t) = F'(t)$ – плотность распределения.

Интенсивность отказов численно равна вероятности того, что объект, проработавший безотказно до момента времени t, откажет в последующую, малую единицу времени.

В период приработки (начальный период работы системы) интенсивность отказов имеет повышенное значение и определяется приработочными отказами. Последние обусловлены наличием в большой партии элементов некоторого количества дефектных образцов.

В период старения интенсивность отказов также резко возрастает и определяется износовыми отказами элементов, которые могут быть обусловлены необратимыми физико-химическими процессами в них. Однако, как правило, все элементы должны сниматься с эксплуатации до начала периода старения.

Элементы, прошедшие период приработки, имеют наиболее низкий уровень интенсивности отказов, который обычно сохраняется примерно постоянным в течение периода нормальной работы. В этот период отказы носят внезапный характер и обуславливаются наличием дефекта в изделии, не проявившегося в период приработки, и внезапной концентрацией нагрузок. В период нормальной работы элемента хорошей моделью для его описания с точки зрения надежности является экспоненциальный закон распределения наработки на отказ.

Для элемента, наработка до отказа которого описывается экспоненциальным распределением, имеем

$$F(t) = 1 - \exp(-\lambda t) \text{ или } f(t) = \lambda \exp(-\lambda t),\ t \geq 0. \qquad (3.2)$$

Тогда в этом случае для вероятности безотказной работы и интенсивности отказов

$$R(t) = \exp(-\lambda t);\ \ \overline{\Theta} = \frac{1}{\lambda};\ \ \lambda(t) = \lambda, \qquad (3.3)$$

где $\overline{\Theta}$ – математическое ожидание случайной величины Θ, т.е. среднее число отказов за время работы элемента.

Метод дискретных марковских процессов наиболее эффективен, когда число элементов, включенных в структурную схему, относи-

тельно невелико. Как уже отмечалось, идея этого метода заключена в моделировании процесса перехода системы из одного состояния в другое – дискретными марковскими процессами [3]. Для таких процессов существует система уравнений Колмогорова – Чепмена, позволяющая найти при ее решении вероятности состояний процесса p_i (фактически это вероятности перехода системы из одного состояния в другое). Размерность этой системы будет равна числу рассматриваемых состояний объекта. Таким образом, в практических расчетах число состояний системы n ограничивается возможностями оперативного решения систем алгебраических уравнений большой размерности. Очевидно, что построение оценок надежности потребуется для всех возможных уровней и режимов работы объекта или системы.

В заключение заметим, что рассматриваемые методы оценок надежности систем на этапе проектирования и косвенной оценки распространяются на достаточно широкий класс систем, при этом основным допущением является предположение о независимости отказов элементов.

Проведение оценок, расчетов и анализа этими методами позволит не только количественно оценить уровень структурной надежности рассматриваемой системы, но и выявить слабые места, выбрать уровень резервирования, обоснованно выбрать периодичность планово-предупредительных ремонтов и получить количественную информацию для оптимизации системы. Практические выводы, вытекающие из количественного анализа надежности, группируются вокруг трех основных способов управления надежностью систем: повышение безотказности элементов, резервирование элементов и каналов системы, обеспечение восстановления элементов после их отказа.

Глава 4
ВЕРОЯТНОСТНЫЙ АНАЛИЗ БЕЗОПАСНОСТИ И ГРАФОАНАЛИТИЧЕСКИЕ МЕТОДЫ

Полный набор критических групп элементов или минимальных сечений возможно получить графоаналитическим методом, или так называемым методом «*дерева отказов*» (ДО). Графоаналитические методы широко используются для следующих целей:

• оценки надежности, безопасности и эффективности систем,

• построения логической схемы объекта,

• идентификации жизненно важных участков защиты (СФЗ) и т.д.

Дерево отказов – графологическая, иерархическая схема объекта (напоминающая перевернутое дерево), которая связывает с помощью ребер графа и логических операторов «И», «ИЛИ» отказы элементов с рассматриваемым отказом всего объекта. При этом вершиной этого дерева является конечное событие – отказ объекта.

После построения дерева отказов проводится его анализ с целью получения полного набора КГЭ, отвечающего данному отказу объекта. В процессе такого анализа последовательно выявляются все *минимальные различающиеся комбинации элементов,* одновременное отказовое состояние которых приводит к вершине дерева – отказу системы (объекта).

Анализ начинается с поиска таких комбинаций, состоящих из одного элемента, затем из двух, трех и т.д. элементов. Так, на примере ядерной энергетической установки, приведенной на рис.4, легко выделить семь КГЭ, образующих полный набор для рассматриваемого отказа ЯЭУ.

При этом основное число этого полного набора для рассматриваемого отказа состоит из одного элемента, и две КГЭ состоят из двух элементов.

Из приведенного простого примера совершенно очевидна разница в способе включения элемента в структурную схему объекта: последовательное (элементы *3* и *4*) и параллельное (элементы *1* и *2*) включение (рис. 5).

При последовательном способе учета включения элементов в структурную схему система работоспособна, если работоспособны оба элемента; при параллельном, если работоспособен хотя бы один элемент. При построении дерева отказов будут использоваться логические операторы «ИЛИ» для последовательного способа включения, обозначающие, соответственно, сумму событий, и операторы «И», обозначающие, соответственно, произведение событий отказов рассматриваемых элементов.

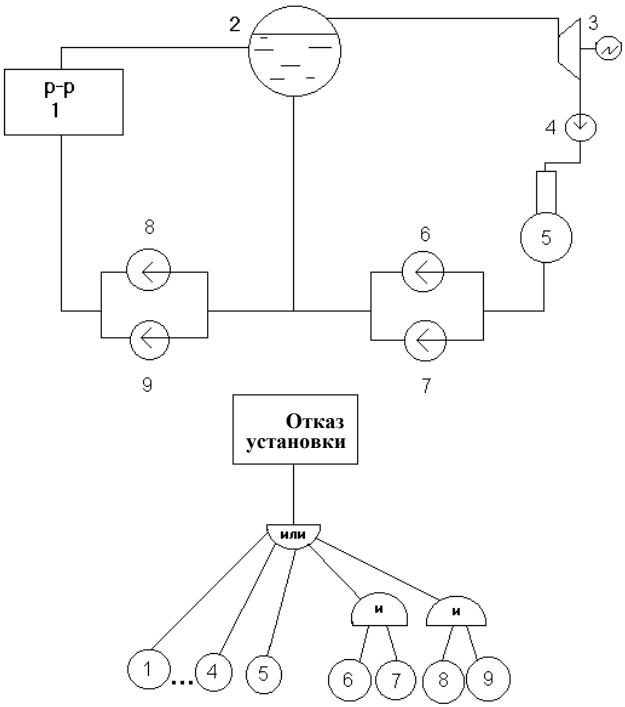

Рис. 4. Пример построения дерева отказов для ЯЭУ. Элементы установки: *1* – реактор; *2* – сепаратор; *3* – турбоагрегат; *4* – конденсатный насос; *5* – деаэратор; *6–9* – питательные насосы (основные и резервные)

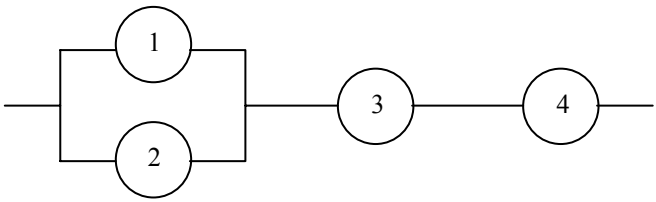

Рис. 5. Параллельное и последовательное включение элементов

Для простых деревьев отказов (содержащих относительно малое количество элементов и логических операторов) выбор минималь-

ного сечения нетрудно вести вручную. Для анализа сложных деревьев отказов целесообразно использовать специальные алгоритмы и программы. В основу таких программ может быть положен, например, следующий алгоритм, использующий метод идентификации КГЭ с помощью простых чисел. Каждому первичному отказу дерева присваивается одно простое число натурального ряда, начиная с единицы (1, 2, 3, 5, 7, …). Программа, основываясь на логике конкретного дерева отказов, определяет все комбинации первичных отказов, приводящих к отказу системы, и представляет их в виде произведения простых чисел. Отбор из них КГЭ проводится на основе известной теоремы о единственности разложения числа на простые множители.

Для получения итоговой количественной оценки необходимо знать характеристики надежности каждого элемента системы и способы их включения. Ранее были введены такие характеристики, как наработка до отказа или вероятность безотказной работы элемента. Мы совершенно справедливо предположили, что экспоненциальный закон распределения для многих элементов наших систем и установок будет хорошим приближением или будет вполне справедлив. Из распределений дискретных величин для описания характеристик элементов обычно используется биномиальное распределение [1]:

$$P_{m,n} = C_n^m \cdot p^m \cdot q^{n-m}, \qquad (4.1)$$

где $q = 1 - p$.

Физический смысл применения биномиального распределения очевиден [4]. Система из n элементов функционирует на заданном интервале времени, причем вероятность отказа одного элемента равна p. В этом случае $P_{m,n}$ – вероятность того, что число отказавших элементов будет равно m. Или другая интерпретация: при n испытаниях прибора наблюдается ровно m срабатываний. Рассмотрим несколько численных примеров.

Пример 1. Рассмотреть систему из 36 одинаковых рабочих органов (рабочие органы СУЗ ЯЭУ, элементы системы ФЗ и т.п.) и вычислить вероятность «зависания» любого одного, двух и трех одновременно при поступлении сигнала на срабатывание. Считать

элементы системы независимыми друг от друга, вероятность несрабатывания принять равной $p = 10^{-4}$.

Ответ. Искомая вероятность равна $P_{m,n} = 3{,}6 \cdot 10^{-4}$; $0{,}63 \cdot 10^{-5}$; $0{,}71 \cdot 10^{-8}$.

В табл. 1 приведены интенсивности некоторых возможных исходных событий на ЯОО. Сравним некоторые из приведенных событий.

Пример 2. Сравнить вероятности возникновения за срок службы ЯОО (например,АЭС) воздействий, обусловленных природными явлениями или деятельностью человека. Согласно предположению считать, что справедливо экспоненциальное распределение для рассматриваемых событий.

Рассмотреть следующие события: падение самолета, максимально расчетное землетрясение, потеря внешнего энергоснабжения, пожар. Искомые интенсивности взять из табл. 1.

Ответ. Вероятности искомых событий составляют $3 \cdot 10^{-5}; 3 \cdot 10^{-3}; 0{,}7; 0{,}95$ соответственно.

Таблица 1

Интенсивности исходных событий на ЯОО

Наименование исходного события	Интенсивность возникновения, год$^{-1}$
Аварии, связанные с эффектами реактивности (все случаи)	10^{-4}
Потеря внешнего электропитания, в том числе на время более 30 мин	$2 \cdot 10^{-1}$ $4 \cdot 10^{-2}$
Разрыв корпуса реактора	$\leq 10^{-6}$
Падение самолёта	$\leq 10^{-6}$
Максимальное расчётное землетрясение	10^{-4}
Пожар	10^{-1}

Говоря об анализе дерева отказов отметим, что отказ элемента может произойти в режиме как работы, так и ожидания. Среди отказов в режиме ожидания различают *функциональные отказы*, после которых элемент не способен выполнить возлагаемые на него функции, и *ложные срабатывания*, характерные, как правило, для элементов управляющих систем. Ложные срабатывания крайне не-

желательны главным образом из-за того, что они нарушают нормальный режим эксплуатации объекта.

Отметим также, что отказы могут быть выявляемыми и скрытыми. Выявляемые отказы обнаруживаются в момент их возникновения за счет предусмотренных средств контроля. Скрытые отказы не выявляются в момент возникновения и обнаруживаются при проведении проверок работоспособности или поступлении требования на срабатывание системы.

Количественный анализ достаточно прост, если известны КГЭ, проанализированы все виды отказов (построено ДО) и известны характеристики надежности входящих в систему элементов. Действительно, для безотказной работы системы в течение времени t необходимо, чтобы все элементы, входящие в КГЭ, работали безотказно в течение времени t.

Если через $R(t)$ обозначить вероятность безотказной работы системы, а через $R_i(t)$ – вероятность безотказной работы элемента, то, пользуясь известными теоремами теории вероятности, для последовательно и параллельно соединенных элементов можно получить соответствующие расчетные формулы. Для последовательного соединения элементов имеем

$$R(t) = \prod_i R_i(t)\,, \tag{4.2}$$

а в случае экспоненциального закона получим

$$\lambda(t) = \sum_i \lambda_i(t)\,. \tag{4.3}$$

Таким образом, для последовательного соединения элементов вероятности перемножаются, а интенсивности складываются.

Для параллельного включения элементов учтем, что такое соединение приведет к отказу только в случае отказа всех входящих в него элементов. Имеем

$$F(t) = \prod_i F_i(t) \quad \text{или} \quad R(t) = 1 - \prod_i (1 - R_i(\mathrm{t}))\,. \tag{4.4}$$

Таким образом, для параллельного соединения элементов перемножаются вероятности отказа.

Характеристика надежности элемента с экспоненциальным распределением наработки до отказа и простейших систем приведены в табл. 2. В случае экспоненциального распределения функция распределения $F(t)$ наработки до отказа равна $F(t) = 1 - \exp(-\lambda t)$.

Таблица 2

Характеристика надёжности элемента с экспоненциальным распределением наработки до отказа и простейших систем

Объект	Характеристика надежности	Обозначение	Формулы для вычисления
Элемент	Вероятность отказа на интервале $(0, t)$	$F(t)$	$1 - \exp(-\lambda t)$
	Вероятность безотказной работы на интервале $(0, t)$	$R(t)$	$\exp(-\lambda t)$
	Интенсивность отказов	$\lambda(t)$	$\lambda(t) = \lambda$
	Средняя наработка до отказа	$\overline{\theta}$	$1/\lambda$
Система с последовательным соединением	Вероятность отказа на интервале $(0, t)$	$F_c(t)$	$\approx \sum_i F_i(t)$
	Вероятность безотказной работы на интервале $(0, t)$	$R_c(t)$	$\prod_i R_i(t)$
	Интенсивность отказов	$\lambda_c(t)$	$\sum_i \lambda_i(t)$
Система с параллельным соединением невосстанавливаемых элементов	Вероятность отказа на интервале $(0, t)$	$F_c(t)$	$\prod_i F_i(t)$
	Вероятность безотказной работы на интервале $(0, t)$	$R_c(t)$	$1 - \prod_i (1 - R_i(t)$

Графоаналитические методы широко используются также в вероятностном анализе безопасности. Как уже отмечалось, в основе вероятностного подхода лежит системный количественный анализ мыслимых сценариев аварий (случаев), а также последовательное

исследование каждого случая, включая пути развития процессов и ситуаций, с учетом наложенных отказов элементов системы, последствий и влияния неопределенностей и человеческого фактора. Среди наиболее важных направлений использования вероятностного анализа [5] были отмечены:

сравнительный анализ технических решений и исследования чувствительности результатов к изменениям исходных параметров;

регламентные проверки систем безопасности и оценка вклада различных факторов и систем в показатели защищенности.

Основой, организующим началом вероятностного анализа является графоаналитический метод «дерева событий» (ДС), а не отказов, как при анализе надежности. При анализе уязвимости и проектировании СФЗ ЯОО дерево событий принято также называть «логической схемой».

За начальную точку дерева событий берется исходное событие и в зависимости от состояния систем и элементов, влияющих на протекание аварийной ситуации, осуществляется логический перебор различных путей развития аварии (ветвей дерева событий) и ее последствий. Для построения дерева событий необходимо выполнить ряд действий:

- определиться с характеристиками нежелательных последствий;
- знать структуру установки и характеристики всех элементов;
- выделить жизненно важные системы, влияющие на развитие аварии.

Итак, обобщим сказанное о ДО и ДС.

Дерево отказов – графологическая иерархическая схема объекта, связывающая с помощью ребер графа и логических операторов отказы элементов с отказом установки (объекта).

Нежелательные последствия при анализе надежности и безопасности ЯОО:

- отказ установки;
- авария.

Дерево событий (логическая схема) – графическое представление возможных сочетаний событий, в результате которых могут

сложиться определенные обстоятельства или произойти события (нежелательные последствия).

Нежелательные последствия при анализе СФЗ:

- кража ЯМ;
- саботаж или диверсия, способные создать угрозу здоровью и безопасности.

При оценке эффективности СФЗ логическая схема является средством, позволяющим определять возможные цели саботажа или кражи на объектах со сложной структурой.

Очевидно, что, как и в случае с деревом отказов, при построении дерева событий 2^n путей развития аварии системы из n независимых элементов. Однако чаще всего элементы не являются независимыми, так как находятся в функциональной связи. Таким образом, учитывая функциональные связи и отбрасывая отдельные пути, анализ ДС упрощается. Принципиально важно при построении ДС учесть возможные отказы по общей причине и ошибочные действия персонала. Если дерево событий построено достаточно подробно, то для аварии могут быть определены все возможные пути ее развития, нежелательные последствия и оценен риск.

Пример дерева событий приведен на рис. 6.

Отметим, что верхние ветви после разветвления соответствуют работоспособному состоянию системы, а нижние – неработоспособному состоянию. На рис.6, *а* – общий случай, а на рис.6, *б* – упрощенное дерево для случая зависимых отказов ($q_{C/B} = q_{D/B} = 1$); где q – вероятность отказа элемента $(1 - q \approx 1,$ поскольку $q << 1)$; $P(A)$ – вероятность или интенсивность исходного события.

Исследование по методу ДС является итерационным по своей сути, поскольку предполагает выделение определяющих по последствиям аварийных цепочек и тщательный их повторный анализ.

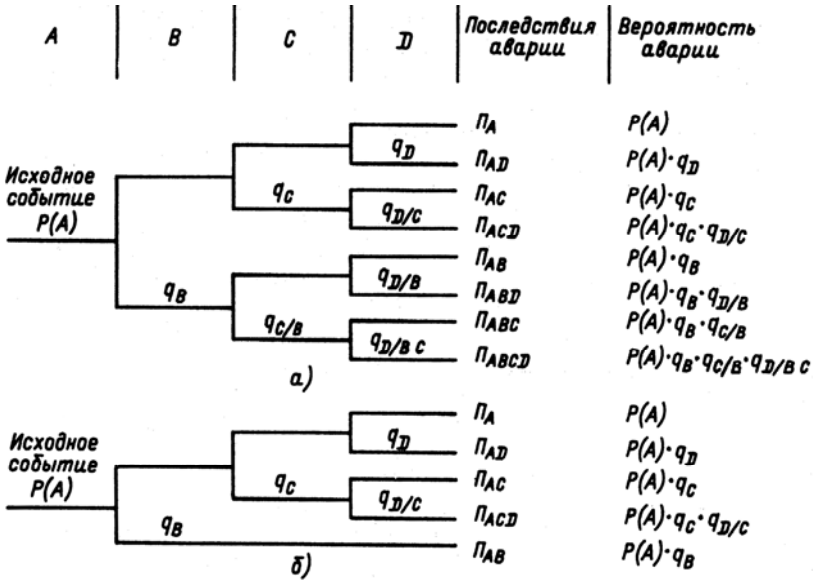

Рис. 6. Вид дерева событий

Пример 3. Построить последовательность событий, дерево событий и найти вероятности аварий для случая потери электропитания собственных нужд ЯОО на время более 30 мин. Считать, что ЯОО имеет две независимые аварийные системы и авария наступает при несрабатывании ($p = 10^{-4}$) любой из них. Другие исходные данные взять из табл. 1.

Ответ. $4\cdot10^{-6}; 4\cdot10^{-10}$.

Анализ и количественная оценка безопасности и эффективности любой сложной системы, к которым относятся и СФЗ ЯОО, и СУ и К ЯМ, и ЯЭУ, может в настоящее время проводится только на основе:

1) вероятностных оценок, например доверительных оценок вероятностей нежелательных событий;

2) экспертных (субъективных) оценок общепринятых показателей.

Рассмотрим примеры этих подходов, иллюстрирующие современное состояние этой проблемы.

В качестве первого примера рассмотрим следующую задачу: Найти ограничение на вероятность нежелательного события на ЯОО, исходя из доверительных оценок и с учетом масштабов распространенности ЯМ. При такой постановке задачи масштаб распространенности ЯМ – фактически масштаб использования ЯМ и он, очевидно, будет определяться масштабом развития ядерной энергетики (ЯЭ) в целом.

Нежелательные события (диверсия, террористический акт, крупная кража, авария и т.д.), очевидно, следует считать редкими событиями. Для описания распределения плотности вероятности редких событий обычно используется закон Пуассона [4].

Если случайная величина X может принимать только целые неотрицательные значения $m = 0, 1, 2, 3, \ldots$ с вероятностью:

$$P_m = P(X = m) = \frac{\lambda^m e^{-\lambda}}{m!}, \qquad (4.5)$$

где λ – параметр, то говорят, что она распределена по закону Пуассона. Это закон редких событий, вероятность которых p мала, а число n велико.

Как известно, математическое ожидание и дисперсия случайной величины, распределенной по закону Пуассона, совпадают и равны значению параметра $\lambda = pn$.

Заметим, что ущерб от нежелательных событий (аварий) на ЯОО в силу своей многофакторности может носить социальный, экономический и экологический характер.

Глобальный социальный риск и ущерб вытекают из опасности глобального характера последствий тяжелых аварий, большой неопределенности в размерах их реального вреда, возможной потери человеческих ценностей, не поддающейся экономической оценке, существующей общественной неприемлемости даже умеренного риска радиоактивного облучения населения и загрязнения среды.

Экономико-экологический риск и ущерб определяются повреждением дорогостоящих ядерных материалов, реактора, ядерного