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, $i = 1,\ldots, N$. 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.

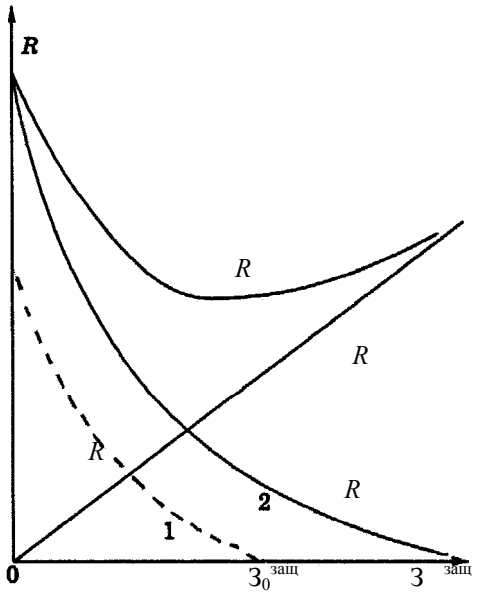

Рис. 1. Зависимость риска от затрат на защиту

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).

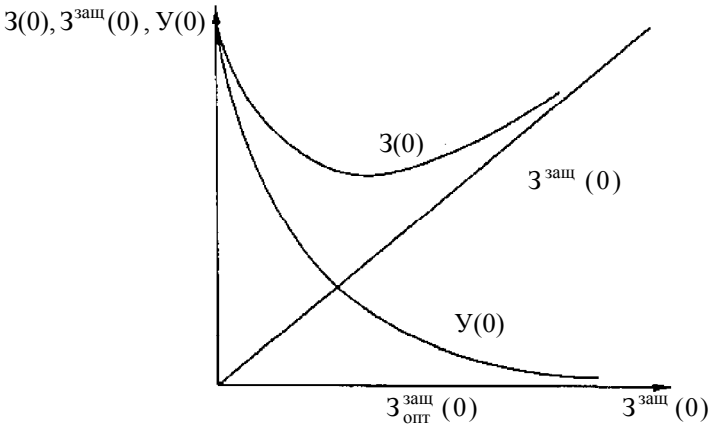

Рис. 2. Зависимость обобщенных приведенных затрат от затрат на защиту

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.

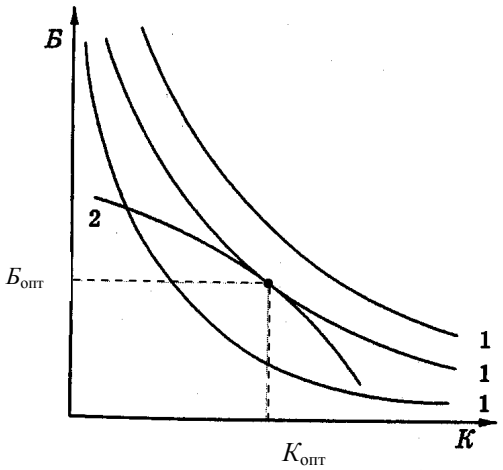

Рис. 3. Безопасность и качество жизни

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.

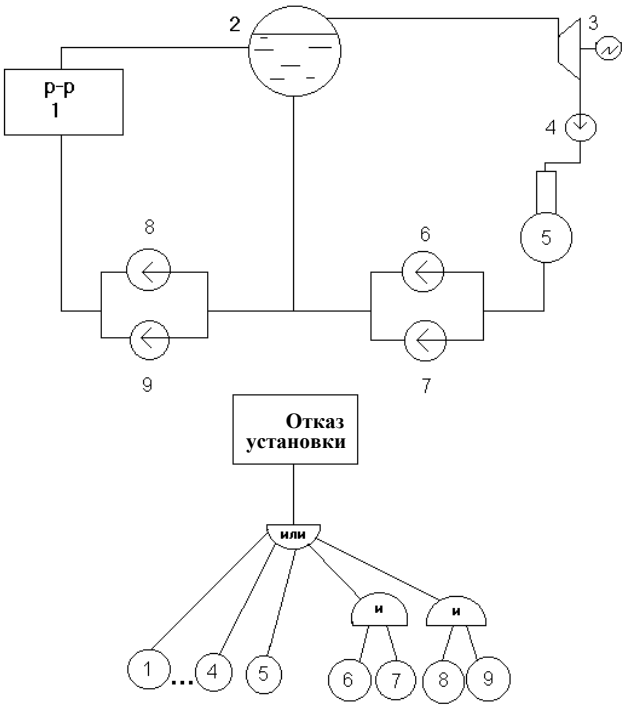

Рис. 4. Пример построения дерева отказов для ЯЭУ. Элементы установки: *1* – реактор; *2* – сепаратор; *3* – турбоагрегат; *4* – конденсатный насос; *5* – деаэратор; *6–9* – питательные насосы (основные и резервные)

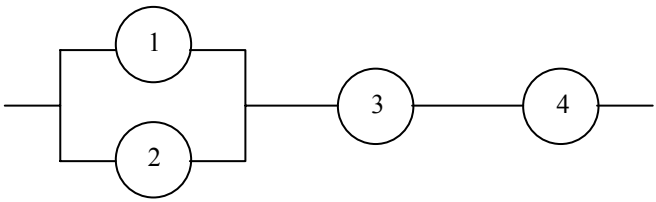

Рис. 5. Параллельное и последовательное включение элементов

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.

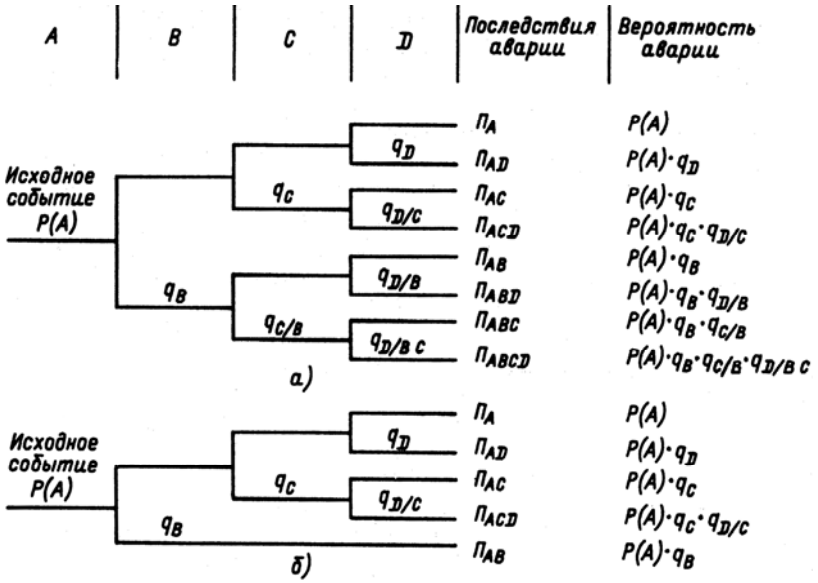

Рис. 6. Вид дерева событий

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

энергоблока, самой АС, промышленных и жилых объектов за пределами объекта, выводом из использования земельных площадей.

Из социального критерия следует требование: *в течение прогнозируемого периода развития ядерных технологий (это примерно 50 лет) и не зависимо от числа ЯОО в доверительном интервале вероятностей не должны происходить значительные аварии (нежелательные события).* Таким образом, потребуем, чтобы ожидаемая величина числа аварий в переделах одного или более среднего квадратического отклонения (корня квадратного из дисперсии) не выходила за значение, равное единице.

Или, исходя из (4.5), имеем

$$\lambda + k\sqrt{\lambda} < 1, \tag{4.6}$$

где k – множитель перед среднеквадратическим отклонением, $k = 1, 2, 3, \ldots$.

Очевидно, что, зная оценку для n, легко из (4.6) найдем искомую оценку вероятности p. В данном случае n – фактор масштаба развития ядерных технологий к концу рассматриваемого периода, и он может быть задан числом реакторолет на конец рассматриваемого периода. По различным оценкам эта величина близка к $3 \cdot 10^5$. Тогда при различных k получаем табл. 3.

Таблица 3

Вероятность нежелательных событий

k	Λ	$\overline{P} = \lambda/n$	Доверительный интервал	Вероятность двух и более событий
1	<0,38	$<10^{-6}$	0,68	0,07
2	<0,17	$<6 \cdot 10^{-7}$	0,95	0,014
3	<0,09	$<3 \cdot 10^{-7}$	0,997	0,004

Выбор $k > 1$ можно оправдать следующими рассуждениями, вытекающими из социального критерия. Если принять $k = 1$ и подсчитать суммарную вероятность появления двух и более аварий, то при выполнении условия (4.6) получим из (4.5)

$$\sum_{m=2}^{\infty} P_m \approx \frac{\lambda^2}{2} \approx 0{,}07. \qquad (4.7)$$

Такое 7%-ное значение вероятности возникновения многочисленных аварий хотя и соответствует математическому ожиданию числа аварий, меньшему единицы, все же неприемлемо. Это либо должно выразиться в увеличении величины доверительного интервала (см. табл. 3), что является естественным решением, либо требует дополнительных ограничений на величину (4.7), исходя из *психологически* приемлемого значения вероятности многочисленных аварий, что в свою очередь трудно формализуемо.

Другим примером вероятностного подхода может служить методология, разработанная в РНЦ «Курчатовский институт» совместно с Брукхевенской национальной лабораторией (БНЛ), США [6]. Анализ доступной информации показывает, что в настоящее время не существует методологии и ее реализации в программном виде, которая могла бы выполнять количественную оценку эффективности СФЗ и работать с большими неопределенностями в частотах или вероятностях начальных событий. Наиболее близким по целям является пакет программ ASSESS (см. гл. 5), но он способен работать только с точечными оценками (математическими ожиданиями) частот событий. Однако исследования с точечными оценками часто мало информативны и могут привести к ошибочным заключениям, если данные по частотам (вероятностям) исходных событий определены со значительной неопределенностью. В программном пакете «Вероятностная экспертно советующая система» (ВЭСС) [6] используется специальная статистическая методология, соответствующая принципам оценки и применения «скудных знаний», с использованием методов построения и анализа деревьев событий и деревьев отказов и метода квантильных оценок неопределенностей.

В основе вероятностного подхода к анализу рассматриваемых редких событий лежит методика построения и анализа деревьев событий и отказов, позволяющая описать логику отказа или успеха в функционировании системы в виде булевых алгебраических уравнений. Каждой булевой переменной можно поставить в соответствие некоторую неотрицательную функцию, которая определяет вероятность реализации определенного значения этой булевой пе-

ременной. С использованием таких функций булевы алгебраические уравнения преобразуются в уравнения для определения вероятности событий в функционировании системы, в зависимости от вероятностей исходных событий. Уравнения для определения вероятности итоговых событий в зависимости от вероятности исходных событий всегда могут быть представлены в виде суммы функций случайных величин, которые описывают логику связи событий вида «ИЛИ». В свою очередь, каждая функция (слагаемое) может быть представлена в виде произведения функций исходных величин, которое описывает логику связи событий вида «И».

В основе аналитического метода квантильных оценок высокоэнтропийных логарифмических распределений плотности вероятности лежит тот факт, что для широкого класса симметричных распределений $f(X)$ случайной величины X с энтропийным коэффициентом $k > 1{,}7$ интегральные кривые функций распределения вероятностей $F(X)$ в области 0,05-го и 0,95-го квантилей пересекаются с друг другом в очень узком интервале значений $|X - X_0|/\sigma(X) = = 1{,}6 \pm 0{,}05$, где X_0 является центром распределения и совпадает с его медианой и математическим ожиданием. Из этого следует, что значения 0,05-го и 0,95-го квантилей распределения, математического ожидания и среднеквадратического отклонения (СКО) подчинены приближенным соотношениям:

$$X_{0,05} = X_0 - 1{,}6 \cdot \sigma(X); \;\; X_{0,95} = X_0 + 1{,}6 \cdot \sigma(X). \qquad (4.8)$$

Применяя эти соотношения при определенных (рассчитанных) значениях СКО и математического ожидания, можно получить оценку значений границ 90%-го доверительного интервала в виде квантилей 0,05 и 0,95. В процессе выполнения совместных работ с БНЛ пакет ВЭСС прошел апробацию и был применен для анализа эффективности усовершенствованных систем УиК и ФЗ центрального хранилища РНЦ КИ. Из-за малости статистики отказов математическое ожидание частоты отказов в основном определялось в соответствии со спецификацией производителя оборудования. Два значения – верхняя граница неопределенности и математическое ожидание – используются для оценки дисперсии, которая вычисляется в соответствии с принципами оценки «скудных» знаний (см.

гл. 8). Полученные результаты [13] по своему характеру существенно отличаются от точечных оценок.

Таблица 4

Пример результатов итоговых событий

Событие	Математическое ожидание с 90%-м доверительным интервалом
Несанкционированный доступ в весовую комнату	$1{,}1 \cdot 10^{-8} < 1{,}52 \cdot 10^{-5} < 1{,}1 \cdot 10^{-4}$
Ошибка при обнаружении несанкционированных перемещений ЯМ	$0{,}0329 < 0{,}00922 < 0{,}1604$
Ошибка персонала при покидании здания в случае аварийной эвакуации	$0{,}014 < 0{,}127 < 0{,}493$

Примером второго подхода, когда используются экспертные оценки общепринятых показателей, является предложенная в [7] методология использования *оценок контрольного вопросника*, исследующего работу и методы в области У и К ЯМ на уровне предприятия и отрасли в целом. В этом подходе отражены все очевидные характерные черты методологии экспертных оценок.

Рассмотрим этот пример подробнее: группа специалистов Центра международной торговли и безопасности (университет шт. Джорджия, США) разрабатывает вопросник для экспертных оценок эффективности систем У и К ЯМ, при этом должны быть объективно решены следующие важнейшие задачи:

- определение и строгое обоснованное ранжирование элементов, необходимых для эффективной системы У и К ЯМ;
- создание единой согласованной шкалы баллов для качественной и количественной оценки систем У и К ЯМ;
- решение вопроса о корректном усреднении и использовании весовых коэффициентов при получении комплексной оценки.

Прелагаемый подход включает контрольный вопросник, анализирующий системы У и К ЯМ на двух уровнях:

первый уровень включает анализ конструкций, процедур и практических методов конкретной площадки, а также практических

работ, направленных на обеспечение безопасного хранения и обращения с ЯМ;

второй уровень представляет в основном оценку структур государственного и официально-бюрократического уровня, протоколов и действий, направленных на обеспечение юридических и практических основ обращения с ЯМ (компонентами этого уровня являются структура инспекций, системы информации, структура нормативов и т.п.).

Примеры вопросов из разрабатываемого вопросника:

1) из раздела «Контроль»:

- работает ли персонал в зонах, где материал 1-й категории используется или хранится под наблюдением;
- обязательно ли правило двух в зонах, где хранится или используется материал 1-й категории;

2) из раздела «Контроль на входе/выходе»:

- обязан ли персонал носить нагрудные знаки;
- обязан ли весь персонал проходить через биометрические устройства.

Однако совершенно очевидно, что анализ результатов опроса, проведенного по данной методике, позволит оценить работы в *юридической, нормативной и официально-бюрократической* сфере при разработке полных и эффективных систем У и К ЯМ и ФЗ ЯОО, но не конкретные процедуры и тем более *не проектно-технические решения* отдельных систем. Даже для решения поставленных задач вопросник должен постоянно обновляться и совершенствоваться, что признают и авторы подхода и что приведет к невозможности ретроспективного сравнения полученных оценок.

Глава 5
ПРИМЕНЕНИЕ ГРАФОАНАЛИТИЧЕСКИХ И ВЕРОЯТНОСТНЫХ МЕТОДОВ ПРИ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ФЗ ЯОО

Рассмотрим особенности физической защиты ЯОО как системы с целью выявления специфических черт, которые будут иметь изложенные ранее подходы и методы применительно к оценке эффективности СФЗ.

Проектирование эффективной системы физической защиты требует методического подхода, позволяющего проектировщику сопоставлять цели СФЗ с имеющимися ресурсами и затем производить оценку предлагаемого проекта. Разработка СФЗ без такой тщательной оценки может привести к неоправданному расходованию ценных ресурсов и средств на средства защиты, в которых нет необходимости, или, что еще хуже, к неспособности системы обеспечить адекватную защиту участков объекта, имеющих критическое значение.

Очевидно, что на первом этапе разработки СФЗ ЯОО определяются цели системы защиты [8]. Для этого проектировщик должен:

- понимать все ведущиеся на объекте работы и характерные для данного объекта условия;
- определить характер существующих угроз;
- определить вероятные цели злоумышленников (диверсантов).

Разработка проекта СФЗ должна производиться в соответствии с поставленными целями физической защиты и в то же время с учетом ограничений, накладываемых необходимостью ведения работ на объекте, а также соображениями безопасности и экономическими факторами.

Основными функциями системы физической защиты являются:

- обнаружение противника (злоумышленника);
- задержка противника;
- развертывание сил ответного реагирования (вооруженной охраны).

Допустим, вся необходимая информация об объекте собрана, подготовлен предварительный проект СФЗ объекта. Как происходит его оценка? Анализ и оценка проекта СФЗ начинается с пересмотра и изучения целей, которым должна соответствовать система физической защиты. Производится проверка выполнения системой ФЗ требуемых функций, таких, как обнаружение противника, пропускной контроль, задержка доступа к цели, обеспечение связи сил ответного реагирования и время их развертывания.

Однако следует заметить, что для рабочей, «взведенной» системы физической защиты реального работающего ядерно-опасного объекта невозможны натуральные исчерпывающие испытания. В целях реальной оценки минимально необходимого уровня эффек-

тивности СФЗ ЯОО должны быть применены более сложные косвенные методы анализа и оценки. Природа защищаемых ядерноопасных объектов не позволяет проводить испытания с инсценировкой действий группы диверсантов, проникающих внутрь охраняемого периметра и похищающих ядерные материалы, и боевым развертыванием сил ответного реагирования. Так как непосредственное испытание всей системы в целом недопустимо, методика оценки эффективности системы должна основываться на данных об испытаниях и характеристиках отдельных элементов подсистем системы физической защиты.

Конечным результатом анализа должна являться количественная характеристика эффективности системы физической защиты, имеющая, безусловно, вероятностную природу, – это так называемая *уязвимость*.

Такой анализ в случае его проведения должен не только дать количественную оценку уязвимости, но помочь выявить в случае необходимости все слабые места системы защиты. Видно что по сути задача оценки уязвимости является задачей вероятностного анализа и может быть решена известными способами. Так, безусловно, возможно применение минимальных сечений (или КГЭ) и метода марковских цепей, а формализация и структуризация задачи возможны графоаналитическими методами определения, например для построения схемы последовательности действий диверсантов. Возникающие локальные оптимизационные задачи решаются, как правило, методами динамического программирования. Приведенный в этой главе краткий обзор алгоритмов и программ позволит лучше понять место упомянутых методов в задаче оценки уязвимости СФЗ [8, 9].

1. Модель EASI. В целях анализа систем физической защиты было разработано много компьютерных моделей. EASI – одна из простейших моделей для оценки вероятности прерывания последовательности действий диверсантов. EASI – простая в обращении модель, демонстрирующая количественные результаты изменения параметров физической защиты на определенном маршруте. В модели используются значения параметров обнаружения, задержки, развертывания сил ответного реагирования и установления связи, с помощью которых рассчитывается результат – вероятность пере-

хвата (прерывания последовательности действий) на данном маршруте.

Исходные данные модели EASI:

- значение вероятности обнаружения для каждого датчика на маршруте;
- вероятности установления аварийной связи с охраной;
- значение времени задержки для каждого элемента (рис.7) и среднее квадратическое отклонение для каждого из этих значений;
- значение времени развертывания сил ответного действия и среднее квадратическое отклонение для этого значения.

Результатами расчета по заданным исходным данным и схеме, приведенной на рис. 8, являются значения вероятности перехвата или вероятности прерывания последовательности действий диверсантов до совершения ими хищения или акции саботажа. Следует заметить, что для анализа всех возможных маршрутов диверсантов и определения наиболее уязвимых маршрутов требуются более сложные модели и программы.

Другой инструмент – расчет времени задержки, а затем выставление вероятностей.

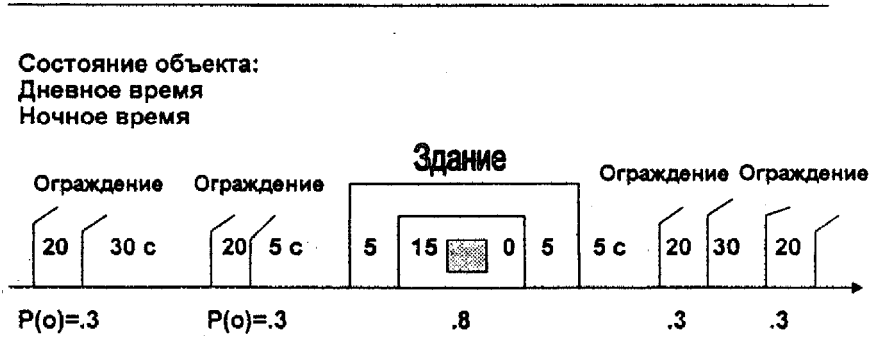

Рис. 7. Расчет времени задержки

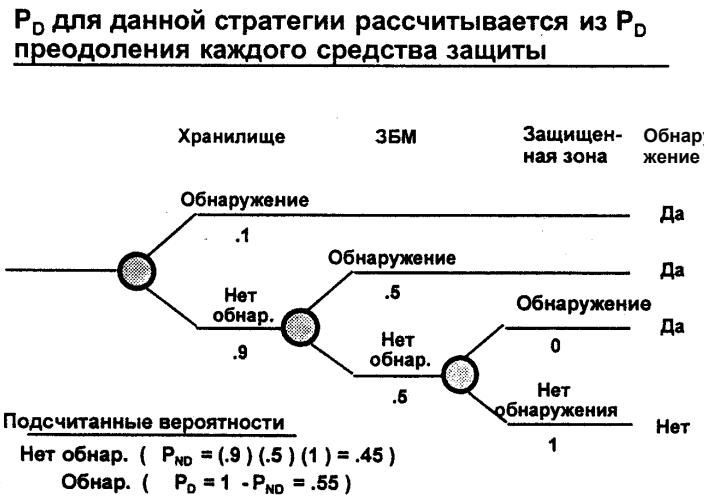

Рис. 8. Логическая схема и расчет вероятности обнаружения и перехвата

2. Модель и программа SAVI используются для оценки эффективности системы физической защиты ядерно-опасного объекта. Модель позволяет определить наиболее уязвимый маршрут на схеме последовательности действий диверсантов. Анализ с помощью модели SAVI начинается с идентификации цели диверсантов и построения соответствующей логической схемы последовательности действий диверсантов с учетом индивидуальных характеристик объекта. Необходимо определить значение времени развертывания сил ответного действия, значение вероятности обнаружения и время задержки для каждого элемента защиты указанной на схеме последовательности действия диверсантов. Вся эта информация используется в качестве исходных данных для работы программы. Программа рассчитывает десять наиболее уязвимых маршрутов в порядке, соответствующем степени их уязвимости. Результаты могут быть также представлены в виде графиков и карты маршрутов. График чувствительности системы позволяет получить информацию о степени зависимости эффективности системы физической защиты от времени развертывания сил ответного действия. График уязвимости позволяет узнать вероятность перехвата и время, остающееся после перехвата, для десяти наиболее уязвимых маршру-

тов с учетом указанного времени реакции ответных действий. Анализ результатов позволяет указать, какие из входных данных должны быть использованы для дальнейшего анализа чувствительности системы физической защиты на наиболее уязвимых маршрутах.

Применяемый в модели SAVI алгоритм вычисления вероятности перехвата реализуется при двух достаточно консервативных допущениях:

- диверсантам известны характеристики системы защиты;
- диверсанты используют оптимальные стратегии проникновения.

Примеры построения схемы последовательности действий диверсантов (СПДД), схема объекта и обобщенная СПДД, используемая программой SAVI, приведены на рис. 9, 10.

На рисунках введены следующие обозначения для обобщенных элементов защиты: DOR – двери; FEN – ограждение; GAT – ворота; ISO – изолированная зона; PER – проходная для персонала; SUR – поверхность; TSK – целевая задача; VEH – проходная для транспортных средств.

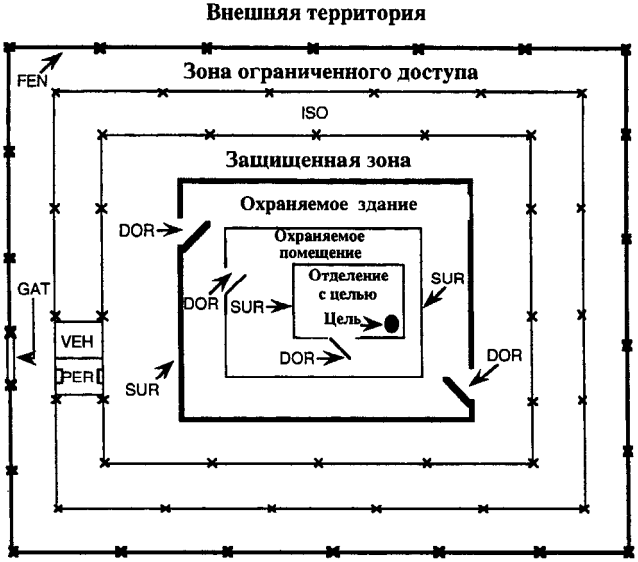

Рис. 9. Пример планировки объекта и СФЗ

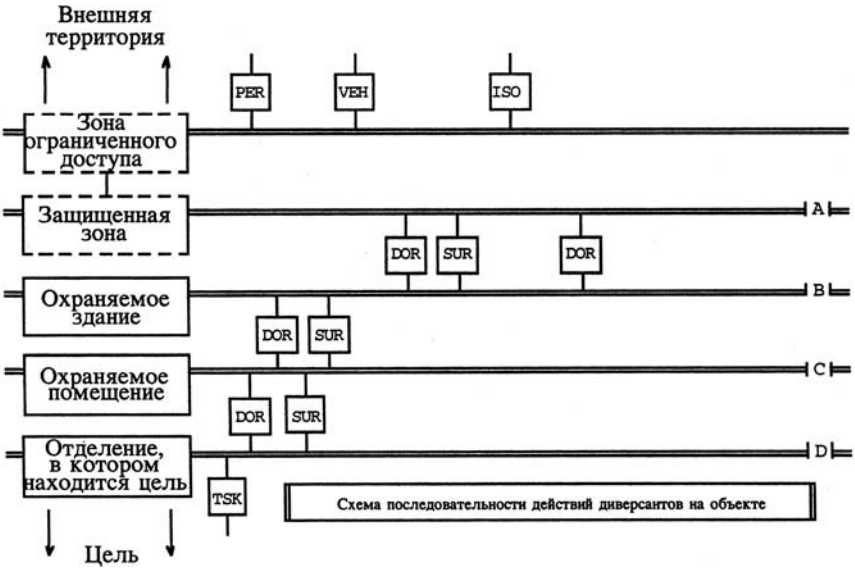

Рис. 10. Пример СПДД, построенной с учетом характеристик объекта

Для того чтобы произошел своевременный перехват диверсантов, необходимо выполнение следующих условий:

- диверсанты должны быть обнаружены;
- они должны быть обнаружены прежде, чем они достигнут той критической точки маршрута, где оставшееся время задержки меньше времени развертывания сил реагирования.

Следовательно, оптимальная стратегия очевидна – избежать обнаружения до тех пор, пока не достигнута критическая точка маршрута, после чего следует свести к минимуму время на прохождение (время задержки) оставшейся части маршрута. На СПДД маршрут представлен как определенная последовательность элементов защиты, расположенных на территории объекта, заканчивающаяся целью диверсантов.

Оценочным показателем эффективности системы физической защиты, используемым в модели SAVI, является вероятность перехвата. Вероятность перехвата определяется как вероятность прерывания последовательности действий диверсантов силами ответного реагирования до завершения стоящей перед диверсантами целевой

задачи. Таким образом, модель SAVI позволяет только частично оценить эффективность СФЗ. Другой важнейший фактор, необходимый для более полного определения эффективности СФЗ ЯОО, – оценка возможностей сил ответного действия, т.е. расчет вероятности того, что силы ответного действия способны успешно нейтрализовать диверсантов после своевременного перехвата. Оценка этой вероятности и добавлена в систему Минобороны США ASSESS.

3. ASSESS – аналитическая система и программное обеспечение для оценки эффективности систем защиты и обеспечения безопасности (модель, разработанная Министерством обороны США). Это – наиболее мощная компьютерная система, позволяющая проводить глобальный анализ системы физической защиты объекта. Программа позволяет рассматривать внешних и внутренних противников и моделировать угрозу от сговора противников. Модуль, позволяющий анализировать угрозу со стороны внешнего противника (диверсантов), – разработан в рамках методики SAVI. Модуль ET позволяет находить наиболее уязвимый сценарий для внутреннего противника. Модуль BATLE разработан для оценки результата перехвата и схватки сил реагирования и диверсантов.

4. Модель ВЕГА, позволяющая оценивать уязвимость СФЗ объекта и разработанная в России (ГУП «Элерон»), использует методику цепей Маркова. Подробнее об этой модели можно узнать в пособии [10].

Глава 6
ОЦЕНКА ЭФФЕКТИВНОСТИ УЧЕТА И КОНТРОЛЯ. МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФИЗИЧЕСКИХ ИНВЕНТАРИЗАЦИЙ

Периодическая физическая инвентаризация и контрольные проверки – неотъемлемый элемент системы учета и контроля ядерных материалов.

В настоящее время периодичность контролей, проверок и инвентаризаций определяется директивно, независимо от характера работ в хранилище и от принятых мер и затрат по сохранению учетных единиц (УЕ). Поэтому актуальна задача: можно ли форма-

лизовать и на научной основе обоснованно выбрать величину межинвентаризационного периода?

Фактически речь идет о методике количественной оценки эффективности физической инвентаризации (ФИ). Применение такой методики позволило бы оценить целесообразность использования различных процедур инвентаризаций, объем и характер контрольных проверок (адресных и выборочных), определить рациональные промежутки времени между контрольными проверками в зависимости от интенсивности работ в хранилище и эффективности СФЗ.

Постановка и решение такой задачи возможны, если измерять количество информации и оценивать закон ее изменения во времени с учетом всех факторов, перечисленных ранее [11]. Измерением количества информации занимается теория информации [15], где для этого введено понятие информационной энтропии.

Информационная энтропия рассматриваемой системы УЕ может быть определена для произвольного момента времени, используя модельные временные зависимости вероятностей бездефектного состояния отдельных УЕ, рассчитанных с учетом различных факторов, влияющих на их состояние.

В промежутках между физическими инвентаризациями информационная энтропия, очевидно, может возрастать вследствие проницаемости СФЗ, а также возможного появления дефектных УЕ при проведении персоналом работ в хранилище. Это означает потерю определенного количества информации в системе учета и контроля о ЯМ.

Физические инвентаризации и контрольные проверки позволяют получать дополнительное количество информации и приводят к уменьшению величины информационной энтропии до требуемого уровня. Очевидно, что при адресных проверках энтропия системы снижается только за счет проверенных конкретных УЕ. При выборочных проверках, когда УЕ отбираются случайным образом, уменьшение величины энтропии обусловлено получением информации как о непосредственно проверенных УЕ, включенных в выборку, так и о непроверенных УЕ, принадлежащих генеральной совокупности.

6.1. Эффективность инвентаризаций на основе понятий теории информации [11]

Понятие инвентаризации по существу означает совокупность процедур, цель которых заключается в получении информации о состоянии УЕ, хранящихся в зоне баланса ЯМ. При этом одинаково важной является как положительная информация, когда фактические и учетные данные соответствуют друг другу, так и информация об отмеченных отклонениях. В последнем случае на основании полученной информации принимаются меры по устранению найденных расхождений.

Несомненно, целесообразно проведение инвентаризаций таким образом, чтобы в результате получить возможно более полную и качественную информацию о состоянии УЕ, а также обеспечить поддержание степени наших знаний о состоянии всех УЕ в зоне баланса ДМ на определенном уровне.

Учетная единица может находиться в двух состояниях:

бездефектном, когда отсутствуют отклонения от нормального состояния УЕ и все фактические контрольные параметры совпадают с учетными данными;

дефектном, когда по крайней мере один фактический контрольный параметр не совпадает с учетными данными.

Причинами, приводящими к дефектному состоянию УЕ в хранилище, могут быть ошибки персонала при ведении учетной документации и при обращении с контейнерами (перепутывание индексов при считывании, нарушение пломб при работах с контейнерами и др.), а также хищение ЯМ.

Указанные причины в большинстве случаев имеют вероятностный характер: могут быть оценены вероятности неверной записи при считывании с входной документации, ошибок при считывании номера контейнера, выбитого на его поверхности и т.д. В принципе вероятностные характеристики могут быть приписаны и возможности осуществления злоумышленных действий по хищению ЯМ без реагирования систем физической защиты.

По существу, все работы с УЕ в хранилище можно разбить на две группы:

1) проводимые в рамках производственного процесса непосредственно с УЕ, которые могут привести к ошибкам и дополнительной неопределенности в учете ЯМ;

2) связанные с контрольными проверками и инвентаризацией УЕ, которые наоборот направлены на наведение порядка в учете, устранение ошибок и снижение неопределенности в знаниях персонала о состоянии УЕ.

Так, если на хранение поставили контейнеры с ненарушенной пломбировкой, то через некоторое время нельзя сказать, что у этих контейнеров пломбировка осталась целой, поскольку в хранилище проводились работы, которые могли привести к повреждению пломб у части УЕ. Внесение нарушений можно считать случайным событием, и с течением времени неопределенность наших знаний о состоянии контейнеров будет возрастать. Однако после контрольной проверки пломбировки всех контейнеров уровень наших знаний о состоянии пломбировки скачком повышается практически до 100%. При этом для такого уровня знания, полученного в результате проведенной контрольной проверки, несущественно, выявлены или нет дефекты в пломбировке контейнеров. Главное, что при проверке получена 100%-ная информация о состоянии пломбировки, и по результатам проверки возможно принятие соответствующего решения.

Для количественной оценки объема и качества информации о случайных событиях развита математическая теория информации [15]. Эта теория позволяет определять количество информации, получаемое в каком-либо опыте со случайными величинами, а также количественно сравнивать информативность различных таких опытов.

Объем информации, заключенный в сообщении о каком-либо событии, в рамках теории информации определяется как изменение уровня знаний о вероятности этого события после приема сообщения.

Согласно теории информации количество информации S, получаемое в опыте (наблюдении) с M возможными исходами, записывается в виде

$$S = -\sum_{i=1}^{M} p_i \log_2 p_i , \qquad (6.1)$$

где p_i – вероятность i-го исхода опыта.

Учтем, что величину S принято называть информационной энтропией опыта, а количество информации определяется разностью величин априорной и апостериорной информационной энтропии опыта. Если различные исходы опыта равновероятны (в этом случае опыт до его проведения является наиболее неопределенным), то $p_i = 1/M$ и согласно (6.1) $S = \log_2 M$. Основание логарифма обычно берется равным 2 с тем, чтобы энтропия опыта с двумя равновероятными (типа «да» или «нет») исходами равнялась бы единице. В дальнейшем изложении опустим двойку в основании логарифма.

Отметим основные свойства информационной энтропии:

- энтропия не может принимать отрицательных значений, так как выражение $p\log p$ равно нулю лишь при $p = 0$ или $p = 1$, то энтропия опыта принимает минимальное значение $S = 0$ при полной определенности исхода опыта, когда один исход имеет вероятность 1, а остальные 0;
- наибольшее значение энтропия имеет в случае, когда исход опыта является наиболее неопределенным: в частном случае двух исходов это имеет место при вероятности каждого исхода равной 1/2.

Применяя введенное понятие о количестве информации к проблеме информативности инвентаризаций УЕ, запишем количественное выражение для степени нашего незнания о состоянии УЕ в хранилище в момент времени t в виде

$$S(t) = -\sum_{i} \left[p_i(t) \log p_i(t) + (1 - p_i(t)) \log(1 - p_i(t)) \right], \qquad (6.2)$$

где $p_i(t)$ – вероятность нахождения УЕ с номером i в бездефектном состоянии.

Суммирование в (6.2) ведется по всем УЕ. Чем меньше величина S, тем более полной информацией обладаем.

При использовании понятия информационной энтропии для количественной оценки эффективности инвентаризаций и определения необходимой частоты ее проведения необходимо задать предельно допустимый уровень степени неосведомленности о состоянии УЕ – S_{crit}, выше которого не допустима эксплуатация хранилища, а также алгоритм определения вероятностей $p_i(t)$ для каждого контейнера в зависимости от интенсивности и характера работ в хранилище и состояния физической защиты.

Для реализации предполагаемой процедуры с целью количественной оценки степени информированности о состояниях УЕ предлагается в базу данных о каждой УЕ дополнительно вести еще один параметр p_i, характеризующий вероятность нахождения рассматриваемой УЕ в бездефектном состоянии. Значение p_i вводится в момент постановки УЕ на учет и изменяется в соответствии с характером работ в помещениях хранилища, режимом и условиями хранения УЕ.

Значение p_i, естественно, уменьшается со временем, приводя к возрастанию энтропии вследствие посещения помещений хранилища персоналом при проведении каких-либо работ (профилактических, ремонтных и др.), в результате которых не исключена вероятность:

- повреждения пломбировки, штрихкодов, перепутывания местоположения УЕ;
- ошибок персонала при выполнении работ по съему информации с УЕ, оформлению документации и вводу ее в оперативные базы данных;
- злоумышленных и диверсионных действий при длительном хранении УЕ.

Другими словами, все работы в рамках производственного цикла с УЕ или в близи УЕ приводят к возрастанию неопределенности знаний о состоянии системы, мерой которой является *информационная энтропия системы*.

Рассмотрим кратко алгоритм определения зависящих от времени вероятностей p_i.

Будем считать, что вероятность $p_i(t)$ УЕ с номером *i* находится в момент *t* в бездефектном состоянии и определяется произведением трех сомножителей, каждый из которых имеет смысл парциальной вероятности независимого события:

$$p_i(t) = p_i^{pd}(t)\, p_i^{per}(t)\, p_i^{bas}(t), \qquad (6.3)$$

где $p_i^{pd}(t)$ – вероятность нахождения УЕ в бездефектном состоянии, обеспечиваемая средствами СФЗ; $p_i^{per}(t)$ – парциальная вероятность нахождения УЕ в бездефектном состоянии, определяемая зависимостью p_i от числа посещений персоналом помещений хранения; $p_i^{bas}(t)$ – вероятность правильного отображения сведений об УЕ в базе данных в процессе принятия УЕ на хранение; *t* – время нахождения УЕ в хранилище, отсчитываемое с момента последней проверки состояния ЯМ прямыми методами.

Для описания парциальных вероятностей $p_i^{pd}, p_i^{per}, p_i^{bas}$ должны использоваться модельные зависимости, содержащие *феноменологические параметры*. Так, зависимость от времени величины p_i^{pd} логично принять в виде

$$p_i^{pd}(t) = \begin{cases} 1 - bt & \text{при } 0 \le t \le 0{,}5/b; \\ 0{,}5; & \text{при } t \ge 0{,}5/b. \end{cases}$$

В этом соотношении сделано предположение о линейном характере вероятности p_i^{pd} от времени вплоть до момента, когда эта вероятность принимает значение 0,5. Значение 0,5 в принятой модели соответствует нулевой информации системы учета и контроля о состоянии УЕ. Если поставить УЕ в бокс в полной целостности, завести правильные сведения о УЕ в базу данных и исключить открывание бокса, то УЕ будут находиться только под охраной СФЗ; выбранная модельная зависимость означает, что через время 0,5/*b* в такой ситуации дефектное и бездефектное состояния будут равновероятны. Естественно, время 0,5/*b* имеет достаточно большое значение. Разумеется, можно выбрать и другой вид модельной зави-

симости $p_i^{pd}(t)$. Можно предложить и ряд зависимостей для двух других парциальных вероятностей, входящих в (6.3). Следует только заметить, что вероятность $p_i^{per}(t)$ зависит от времени неявно, через количество рабочих дней, когда хранилище с ЯМ посещал персонал после последней проверки. А вероятность p_i^{bas} будет определяться вероятностью ошибок персонала при введении информации в базу данных и количества символов, вводимых в базу данных, и явно от времени зависеть не будет.

6.2. Алгоритм определения вероятности p_i при выборочных проверках

При проведении выборочных проверок все УЕ делятся на два типа. К первому относятся те УЕ, которые в результате случайной выборки оказываются в числе проверяемых. Для этой группы УЕ изменение значений вероятностей p_i осуществляется непосредственно.

Ко второму типу относятся те УЕ, которые непосредственной проверки не проходят. Расчет вероятностей для УЕ, принадлежащих проверяемой подсистеме, но не попавших в число проверенных при выборочной проверке, производится по следующей методологии: по результатам выборочной проверки, осуществляемой по случайному закону, корректируются априорные вероятности конфигураций проверяемой подсистемы, по найденным апостериорным вероятностям конфигураций находится энтропия системы после опыта S_{out} и по ней, наконец, определяются апостериорные вероятности p_i^+ для УЕ, не попавшие в число проверяемых.

Приведем расчетные формулы для каждого из этих этапов. Формулы справедливы для выборки с близкими значениями p_i.

Сделаем это сначала для случая, когда при выборочной проверке проверяется вся совокупность контрольных параметров.

Находим S_{in} – энтропию проверяемой подсистемы перед проверкой:

$$S_{in} = -\sum_{i=1}^{N} \{p_i \log p_i + [1 - p_i] \log[1 - p_i]\}. \quad (6.4)$$

Здесь суммирование производится по всем УЕ проверяемой подсистемы. По найденному значению S_{in} находим p – среднюю вероятность бездефектного состояния УЕ из проверяемой подсистемы:

$$S_{in} = -N\{\overline{p} \log \overline{p} + [1 - \overline{p}] \log[1 - \overline{p}]\}. \quad (6.5)$$

По найденным средним $\overline{p}$ вычисляются величины $W(N, D, n, d)$ – скорректированные вероятности типов конфигураций исходной подсистемы:

$$W(N, D, n, d) = \frac{1}{\Sigma} (\overline{p})^{(N-D)} (1 - \overline{p})^{D} \binom{N}{D} w(N, D, n, d),$$

где $w(N, D, n, d) = P(X = d) = \dfrac{\binom{D}{d}\binom{N-D}{n-d}}{\binom{N}{n}}$ – функция гипергеометрического распределения.

После нахождения величин $W(N, D, n, d)$ находится S_{out} – скорректированная по результатам проверки энтропия тех УЕ, которые принадлежат проверяемой подсистеме, но не попали в число проверяемых:

$$S_{out} = -\left(\frac{N-n}{N}\right) \sum_{D=d}^{N-n+d} W(N, D, n, d) \log\left\{\binom{N}{D}^{-1} W(N, D, n, d)\right\}. \quad (6.6)$$

Вероятность после проверки p_i^+ для УЕ, принадлежащих проверяемой подсистеме, но не попавших в число проверяемых, находится согласно следующему алгоритму.

Сначала из соотношения

$$\frac{1}{N-n} S_{out} = -p^+ \log p^+ - \left(1-p^+\right)\log\left(1-p^+\right) \tag{6.7}$$

находится величина p^+, которая имеет смысл средней апостериорной вероятности бездефектного состояния для рассматриваемых УЕ, по которой могут быть рассчитаны индивидуальные значения вероятностей p_i^+. Индивидуальные значения вероятностей p_i^+ можно найти, например, с помощью выражения [11]:

$$p_i^+ = +\theta\left[\frac{p^+ - \overline{p}}{1-\overline{p}}\right](1-p_i), \tag{6.8}$$

где коэффициент θ близок к единице и определяется из условия неизменности энтропии проверяемой системы S_{out} после вычисления p_i^+, т.е. из условия

$$S_{out} = -\sum_i \left\{p_i^+ \log p_i^+ + \left[1-p_i^+\right]\log\left[1-p_i^+\right]\right\}. \tag{6.9}$$

Суммирование здесь производится по УЕ, принадлежащим проверяемой подсистеме, но не попавших в число проверяемых.

По результатам выборочной проверки присваиваются новые значения p_i^+ всем элементам подсистемы и определяется новое значение энтропии S^+ всей системы УЕ. Если значение S^+ меньше допустимого $S_0 = S_{\text{crit}}$, то наши знания о системе находятся на приемлемом уровне.

Качественно зависимость информационной энтропии от времени показана на рис. 11. За начало отсчета принят произвольный момент времени.

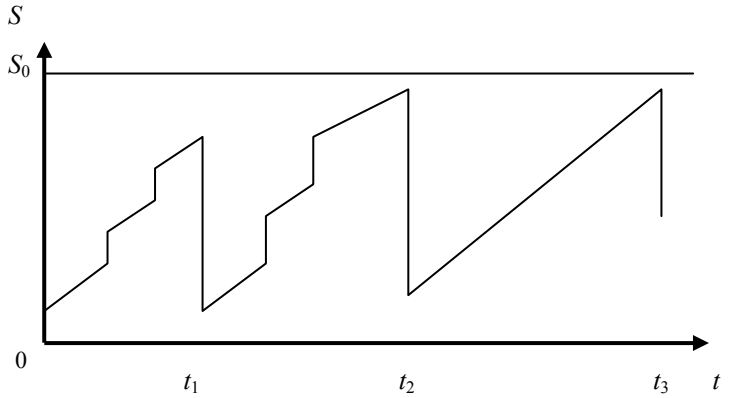

Рис. 11. Зависимость информационной энтропии от времени

Наклонные линии на рисунке соответствуют составляющей, связанной с эффективностью системы физической защиты. Небольшие скачки энтропии вверх получаются из-за увеличения энтропии в результате работ в хранилище. Уменьшение энтропии связано с контрольными проверками (моменты времени t_1, t_2, t_3 на рис. 11). Продолжительность между контрольными проверками может быть различной в зависимости от интенсивности работ в хранилище и объема предыдущей выборочной проверки. Третий участок времени ($t_2 - t_3$) соответствует отсутствию работ в хранилище, когда изменение энтропии определяется только эффективностью СФЗ.

Глава 7
ОЦЕНКА ЭФФЕКТИВНОСТИ КАК ОПТИМИЗАЦИОННАЯ ЗАДАЧА. МЕТОДЫ ОПТИМИЗАЦИИ, ПРИМЕНЯЕМЫЕ ПРИ АНАЛИЗЕ БЕЗОПАСНОСТИ И ЭФФЕКТИВНОСТИ

Из гл. 2, 3 и 5 достаточно ясно вытекает, что задача оценки эффективности системы, по сути, является оптимизационной. Действительно, если есть характеристика системы, которую необходимо улучшить, и есть естественные ограничения, отражающие условия функционирования системы и/или ограниченность средств, на-

правляемых на решение задачи, то фактически приходим к необходимости найти решение *оптимизационной задачи с ограничениями*. Например, задачи (2.2) и (2.3) или задача об улучшении (минимизации) уязвимости ЯОО при ограничении выделенных средств на элементы ФЗ, или задача оптимальной стратегии нарушителя. В данной главе будут разобраны общие подходы к формализации подобных оптимизационных задач и приведены сведения о некоторых наиболее распространенных способах их решения.

Формализация оптимизационной задачи с ограничениями требует следующих шагов:

1) выбор критерия;

2) выбор управляющих параметров;

3) выбор и формализация ограничений задачи;

4) выбор метода решения задачи.

На самом деле явно или неявно будет существовать еще один шаг: учет неопределенностей исходной информации, но это тема будет освещена в гл. 8.

Выбор критерия оптимальности или целевой функции представляет собой выбор характеристики системы (обычно это функция или функционал), улучшение которой (максимизация или минимизация) является для нас целью данной задачи. Иногда критерий оптимальности называют оптимизируемым функционалом или критерием качества.

Выбор управляющих параметров. Изменением значений выбранных параметров задачи можно добиться изменения целевой функции и выполнения ограничений задачи. Такие управляющие параметры в дальнейшем будем называть управлениями.

Выбор и формализация ограничений задачи. Ограничения задачи должны быть выбраны таким образом, чтобы их выполнение, с одной стороны, обеспечивало выполнение условий задачи, а с другой – отражало возможность существования и безопасного функционирования рассматриваемой системы. Совершенно очевидно, что управляющие параметры (управления) практических задач всегда имеют естественные границы своих возможных значений, и поэтому эти естественные границы также являются ограничениями задачи.

Выбор метода решения задачи. Как это будет показано, выбор метода зависит от природы рассматриваемой задачи.

В общем виде математическая постановка оптимизационной задачи состоит в определении наибольшего или наименьшего значения критерия оптимальности при выполнении заданных условий, а точнее, в определении такого вектора управлений $\vec{u}$, который доставляет наилучшее (минимальное или максимальное) значение критерию оптимальности $F_0(\vec{u})$ при выполнении ограничений задачи:

$$\begin{gathered}\text{найти такие } \vec{u}\text{, при которых:} \\ \min F_0(\vec{u}), \\ F_i(\vec{u}) \le F_i^{\text{доп}},\end{gathered} \tag{7.1}$$

где $F_i^{\text{доп}}$, i =1,...,n, – известные допустимые значения ограничений оптимизационной задачи (7.1).

Изучением оптимизационных задач, разработкой методов их решения занимается специальная математическая дисциплина – *математическое программирование.* В зависимости от свойств целевой функции и функций ограничений математическое программирование можно рассматривать как ряд самостоятельных дисциплин, занимающихся изучением и разработкой методов решения определенных классов задач.

Прежде всего, задачи математического программирования делятся на задачи *линейного* и *нелинейного* программирования. При этом, если все функции, входящие в задачу (7.1), – линейные, то соответствующая задача является задачей *линейного программирования*. Если же хотя бы одна из указанных функций – нелинейная, то соответствующая задача является задачей *нелинейного программирования*.

Линейное программирование. Наиболее изученным разделом математического программирования является линейное программирование. Для решения задач линейного программирования разработан целый ряд эффективных методов, алгоритмов и программ [12].

Общей задачей линейного программирования называется задача, которая состоит в определении минимального (максимального) значения функции:

$$F_0 = \sum_{j=1}^{n} c_j x_j,$$

$$\sum_{j=1}^{n} a_{ij} x_j \le b_i \qquad (i = 1, ..., k), \tag{7.2}$$

$$\sum_{j=1}^{n} a_{ij} x_j = b_i \quad (i = k+1, ..., m), \tag{7.3}$$

$$x_j \ge 0 \quad (j = 1, ..., l; \quad l \le n), \tag{7.4}$$

где a_{ij}, b_i, c_j – заданные постоянные величины и $k \le m$.

Из вида задачи ясно, что целевая функция и ограничения представляют собой линейные формы относительно неизвестных управлений *x*.

Канонической (или основной) формой задачи линейного программирования называется задача, которая состоит в определении максимального значения функции F_0 при выполнении только условий типа (7.3) и (7.4), где k = 0 и l = n. Совокупность чисел (управлений) $X = (x_1, x_2, ..., x_n)$, удовлетворяющих ограничениям задачи (7.2)-(7.4), называется допустимым решением (или *планом*). Показано [11], что допустимое множество планов данной задачи – выпуклый многомерный многогранник. Наиболее эффективным и известным способом решения подобных задач является так называемый *симплекс-метод.* В основе расчетной схемы симплекс-метода лежит идея упорядоченного перебора вершин допустимого многогранника. Известны крайне эффективные алгоритмы и программы, реализующие идею симплекс-метода [11].

Нелинейное программирование. В реальной жизни задачи линейного программирования крайне редки. В практике оценки эффективности сложных систем, к которым относятся задачи, рассматриваемые в данном пособии, – линейные задачи вряд ли возможны вообще. Среди задач нелинейного программирования наи-

более глубоко изучены задачи *выпуклого программирования.* Это задачи, в результате решения которых определяется минимум выпуклой (или максимум вогнутой) функции, заданной на выпуклом замкнутом множестве. К этому достаточно широкому классу задач могут быть отнесены многие реальные практические задачи, такие, как оптимальный выбор компоновки реакторной установки, задачи повышения безопасности ядерных установок и многие другие. Для решения задач выпуклого программирования разработаны методы множителей Лагранжа, градиентные методы и другие. Используя, например, градиентные методы, можно найти решение практически любой задачи нелинейного программирования. Однако в общем случае применение этих методов позволяет определить только точку локального экстремума.

Мы достаточно подробно остановились на линейном программировании потому, что многие задачи нелинейного программирования (например, задачи выпуклого программирования) могут быть эффективно решены *последовательной линеаризацией* исходной задачи, т.е. исходная нелинейная задача с помощью так называемых *коэффициентов чувствительности* на небольшом участке фазового пространства управлений $\vec{u} \in U$ сводится к последовательности задач линейного программирования, решаемых на каждом шаге такой итерационной процедуры одним из вариантов симплекс-метода. Коэффициентами чувствительности функционалов задачи (7.1) называются величины

$$\overrightarrow{H_i} = \frac{\delta F_i(\vec{u})}{\delta \vec{u}}; \quad i = 0, 1, ..., n.$$

В зависимости от задачи коэффициенты чувствительности могут быть определены аналитически (например, с помощью теории малых возмущений) или численно.

Отдельными классами задач математического программирования являются задачи целочисленного и параметрического программирования.

В задачах *целочисленного программирования* неизвестные могут принимать только целочисленные значения. В задачах учета и контроля ЯМ это могут быть, например, УЕ.

В задачах *параметрического программирования* целевая функция или функция, определяющая область возможных изменений управлений, либо то и другое зависят от некоторых неопределенных параметров.

Выделяется также очень важный класс задач так называемого *стохастического программирования*: если в целевой функции или в функциях, определяющих область возможных изменений управлений, содержатся случайные величины. Подробнее вернемся к этому классу задач при рассмотрении темы «Учет неопределенностей» (см. гл. 8).

В отдельный класс нелинейных задач обычно выделяют задачи, решение которых возможно методами, основанными на последовательном анализе вариантов. Нас будет, в частности, интересовать так называемые задачи *динамического программирования*. Дело в том, что именно к задаче *динамического программирования* сводится задача определения маршрута нарушителя при условии использования им оптимальной стратегии (гл. 5).

Общая идея методов последовательного анализа вариантов интуитивно кажется почти очевидной, задача отыскания оптимального вектора управлений, доставляющего минимум целевой функции $F_0(\vec{u})$, должна быть тем проще, чем уже допустимая область изменения аргумента $\vec{u}$. Если ограничения настолько жесткие, что это множество состоит из нескольких точек и эти точки легко отыскать, то задача сводится к простому перебору нескольких чисел. Можно привести и другой пример: допустим, что требуется найти кратчайший путь между двумя точками, соединенными узким коридором – допустимой областью движения. Тогда собственно оптимизационная задача почти тривиальна – любой из путей в нем будет практически оптимален. Однако если захотим для поиска решений подобных задач использовать описанные выше методы, то либо вообще ничего не получится, либо практически очевидная процедура превратится в чрезвычайно громоздкий вычислительный алгоритм. В математике первые идеи методов последовательного анализа вариантов были высказаны А.А. Марковым. Позже подробно обсуждались в работах Вальда и были продолжены в исследованиях Р. Айзекса и Р. Беллмана. В результате последний из этих американских математиков пришел к созданию *динамического*

программирования. Методы оптимизации, основанные на идее последовательного анализа вариантов, в большой степени используют природу изучаемых задач.

Динамическое программирование. Предположим, что некоторая физическая система S находится в некотором начальном состоянии $S_0 \in \overline{S}_0$ и является управляемой. Благодаря осуществлению некоторого управления U *система переходит из начального состояния* S_0 в конечное состояние S_{fin}. При этом качество каждого из реализуемых управлений U характеризуется значением функции $W(U)$. Задача состоит в том, чтобы из множества возможных управлений найти такое U^*, при котором функция $W(U)$ принимает наилучшее (экстремальное) значение $W(U^*)$. Сформулированная задача и является общей задачей динамического программирования.

Пример 4. Для повышения эффективности СФЗ ЯОО (минимизации уязвимости или максимизации защищенности) намечен ряд мероприятий и выделена сумма капиталовложений в размере S тыс. руб. Использование x_i руб для каждого i-го мероприятия обеспечит прирост защищенности, определяемый значением нелинейной функции $f_i(x_i)$.

Математическая постановка задачи состоит в определении наибольшего значения функции

$$F = \sum_{i=1}^{n} f_i(x_i) \tag{7.5}$$

при условиях

$$\sum_{i=1}^{n} x_i = S \quad \text{и} \quad x_i \geq 0 \quad (i = 1, ..., n). \tag{7.6}$$

Сформулированная задача является задачей нелинейного программирования. В том случае, когда известно, что $f_i(x_i)$ – выпуклые функции, ее решение можно найти, например, методом множителей Лагранжа. Если же функции $f_i(x_i)$ не являются таковыми, то известные методы не позволяют определить глобальный макси-

мум целевой функции. Однако решение задачи (7.5) - (7.6) можно найти с помощью динамического программирования. Для этого исходную задачу нужно рассмотреть как многошаговую [12]. Вместо того чтобы рассматривать допустимые варианты распределения капиталовложений между n мероприятиями и оценивать их эффективность, будем исследовать эффективность вложения средств в одно, два мероприятия и т.д., наконец, в n мероприятий. Таким образом, получим n этапов (шагов), на каждом из которых состояние системы описывается объемом средств, подлежащих освоению в k мероприятиях ($k = 1,\ldots, n$).

Решения об объемах капиталовложений, выделяемых для k-го мероприятия, и являются управлениями. Задача состоит в выборе таких управлений, при которых целевая функция (7.5) принимает наибольшее значение.

Рассмотрим теперь в общем виде решение таких задач. Сформулируем необходимые условия и предположения применимости метода динамического программирования (схема Беллмана). Будем считать, что состояние рассматриваемой системы на k-м шаге определяется выбранным управлением на данном шаге и состоянием системы в k-1 шаге и не зависит от того, каким образом система пришла в k-1 состояние.

Далее будем считать, что если в результате реализации k-го шага обеспечен определенный выигрыш или доход, также зависящий от исходного состояния системы в начале шага (k-1 состояние) и от выбранного управления u_k и равный $W_k(X^{(k-1)}, u_k)$, то общий выигрыш за n шагов составляет

$$F = \sum_{k=1}^{n} W_k(X^{(k-1)}, u_k). \qquad (7.7)$$

Мы сформулировали два условия, которым должна удовлетворять рассматриваемая задача динамического программирования. Первое условие обычно называют *условием отсутствия последействия*, а второе – условием *аддитивности* целевой функции. Выполнение для задачи первого условия позволяет сформулировать для нее принцип оптимальности Беллмана.

Принцип оптимальности Беллмана. Каково бы ни было состояние системы перед очередным шагом, надо выбирать управление на этом шаге так, чтобы выигрыш на данном шаге плюс оптимальный выигрыш на всех последующих шагах был максимальным.

Отсюда следует, что оптимальную стратегию управления можно получить, если сначала найти оптимальную стратегию управления на *n*-м шаге, затем на двух последних *n*-м, (*n*-1)-м и т.д. вплоть до первого шага.

Введем некоторые дополнительные обозначения и дадим математическую формулировку принципа оптимальности. Обозначим: $F_n(X^0)$ – максимальный выигрыш, получаемый за *n* шагов при переходе системы из начального X^0 в конечное состояние $X^{(n)}$ при реализации оптимальной стратегии управления $U=(u_1,u_2,...,u_n)$, а через $F_{n-k}(X^k)$ – максимальный выигрыш (доход), получаемый при переходе из любого состояния X^k в конечное состояние $X^{(n)}$ при оптимальной стратегии управления на оставшихся *n-k* шагах. Тогда

$$F_n(X^0)=\max_{u_{k+j}}[W_1(X^0,u_1)+....+W_1(X^{(n-1)},u_n)], \tag{7.8}$$

$$F_{n-k}(X^{(k)})=\max_{u_{k+1}}[W_{k+1}(X^{(k)},u_{k+1})+....+F_{n-k-1}(X^{(k+1)})], \tag{7.9}$$

$$k=0,1,...,n-1.$$

Последнее выражение представляет собой математическую запись принципа оптимальности и носит название *основного функционального уравнения* Беллмана или рекуррентного соотношения. Используя данное уравнение, находим решение рассматриваемой задачи динамического программирования, начиная с $k=n-1$ и последовательно осуществляя итерационный процесс расчета состояний системы для каждого шага, выбирая оптимальные решения, на каждом шаге рассматривая всевозможные допустимые состояния системы и используя рекуррентное соотношение (7.9) для нахождения предыдущего состояния системы. Таким образом, в резуль-

тате последовательного прохождения всех этапов от конца к началу определяем максимальное значение выигрыша за n шагов и для каждого из них находим условно оптимальное управление.

Численный метод Беллмана достаточно эффективен, показано [12], что число вычислений при его использовании не может быть меньше, чем на порядок менее числа вычислений при простом переборе вариантов.

Глава 8
УЧЕТ НЕОПРЕДЕЛЕННОСТЕЙ ПРИ ОЦЕНКАХ ЭФФЕКТИВНОСТИ И ВЫБОРЕ РЕШЕНИЙ. ВЫБОР РЕШЕНИЙ В УСЛОВИЯХ РИСКА И НЕОПРЕДЕЛЕННОСТИ

Существуют различные подходы к проблеме выбора (принятия) решений в условиях риска и неопределенности, каждый их которых имеет свои положительные и отрицательные стороны. Цель данной главы на достаточно простых примерах проиллюстрировать ряд существующих подходов к учету неопределенностей и отметить их особенности.

Задачи выбора решений обычно различаются тем, принимает решение индивидуум или группа, и тем, производится выбор решения при определенности, риске или неопределенности.

При этом следует заметить, что индивидуум – человек или группа лиц (например, организация), имеющие единый интерес, служащий мотивом принятия решения. Всякая группа индивидуумов, противоречия между которыми разрешаются открытым конфликтом или компромиссом, – группа. Учет противоречий группы – отдельная задача, рассматриваемая в так называемой теории игр. В дальнейшем будем разбирать только индивидуальные решения.

Говорят, что имеет место выбор решения: 1) при определенности; 2) при риске; 3) при неопределенности.

1. Выбор решения при определенности, если каждое действие неизменно приводит к однозначному исходу. В этом случае имеем подзадачу выбора критерия качества и решение оптимизационной задачи:

$$\text{найти такие } \vec{u}\text{, при которых}\quad \min F_0(\vec{u}),\quad F_i(\vec{u}) \le F_i^{\text{доп}}, \tag{8.1}$$

т.е. решение сводится к вполне определенной оптимизационной задаче (см. гл. 7).

2. Выбор решений при риске, если каждое действие приводит к одному из множества частных исходов, каждый из которых имеет известную вероятность появления.

Формализуем задачу выбора при риске и сведем ее к аналогу оптимизационной задачи (8.1). Пусть $\vec{\vartheta}_j \in \{\vartheta\}$, *j*-й – набор исходных параметров с известными вероятностными характеристиками, тогда задача запишется в виде:

$$\text{найти такие } \vec{u}\text{, при которых}\quad \min F_0(\vec{u}, \vec{\vartheta}_j),\quad F_i(\vec{u}, \vec{\vartheta}_j) \le F_i^{\text{доп}}(\vec{\vartheta}_j). \tag{8.2}$$

Тогда, зная вероятностные характеристики реализации того или иного $\vec{\vartheta}_j \in \{\vartheta\}$ из множества возможных исходов, можно свести задачу (8.2) к задаче (8.1), применяя, например, метод детерминированного аналога, суть которого состоит в следующем.

Если известны корреляционные матрицы для вероятностно распределенных исходных параметров $\vec{\vartheta}_j \in \{\vartheta\}$, то исходная задача (8.2) может быть представлена как задача *стохастического программирования* с вероятностными ограничениями. Разработаны и совершенствуются методы решения таких задач [16]. Используя, например, метод последовательной линеаризации (см. гл. 7) с помощью соответствующих коэффициентов чувствительности на каждом шаге линеаризации исходной задачи, можно разделить детерминированные и стохастические переменные и построить так называемый *детерминированный аналог* исходной стохастической задачи, т.е. свести исходную задачу к задаче типа (8.1), но с изме-

ненными допустимыми значениями ограничений и решать ее относительно математического ожидания критерия $F_0(\vec{u})$:

$$\text{найти такие } \vec{u} \text{, при которых}$$
$$\min M\{F_0(\vec{u})\},$$
$$F_i(\vec{u}) \le F_i^{\text{доп}} + Q_i,$$

где Q_i – рассчитанные запасы на выполнение соответствующих ограничений, которые находятся из вероятностных условий типа:

$$P\left\{F_i(\vec{u}, \vec{\vartheta}_j) \le F_i^{доп}(\vec{\vartheta}_j)\right\} \ge p_0,$$

где p_0 – заданная вероятность выполнения данного вероятностного ограничения.

3. Выбор решения при неопределенности, если каждое действие приводит к одному из множества частных исходов, вероятности которых неизвестны или даже не имеют смысла.

Принято выделять следующие типы неопределенностей исходных данных:

- *вероятностно-распределенные*;
- *собственно неопределенные*.

Следует отметить, что в том случае, когда допустимо говорить о вероятности исходов, пусть даже ничего не известно о вероятностных характеристиках данных, можно воспользоваться субъективными вероятностями, в определении которых поможет теория полезности [13] и свести задачу выбора при неопределенности к задаче (8.2).

Примерами нетривиальных задач выбора решений при определенности, потребовавших развития новых разделов математики, являются задачи линейного программирования, решаемые, например, симплекс-методом, и более сложные задачи – задачи нелинейного программирования, решаемые методами динамического программирования (метод Беллмана), или сводимые к последовательности задач линейного программирования с помощью линеариза-

ции (например, с помощью коэффициентов чувствительности – МПЛ).

Сущность задач выбора решений при риске или неопределенности можно пояснить на следующем примере. Пусть имеется множество действий или решений $i = 1, 2, \ldots, l$ и множество возможных исходов, однозначно определяющих так называемые состояния природы $j = 1, 2, \ldots, S$. Состояние природы j – это просто j-сочетание исходных данных или некоторых внешних условий, влияющих на решение. Пусть существует функция, характеризующая потери, убытки или *затраты* $f_{ij} = З_{ij}$, которые связаны с действием i при исходе (сочетании условий, состоянии природы) j. В общем случае f_{ij} – функция цели, тогда числа $f_{ij} = З_{ij}$ можно представить в виде матрицы размерностью $l*S$, называемой *платежной матрицей*.

Очевидно, что истинное состояние природы j нам неизвестно. Тогда требуется найти такое действие i, т.е. выбрать такую строку матрицы $\{f_{ij}\}$, которое в некотором смысле явно лучше других.

Если известны такие вероятности $p_1,...,p_S$ состояний природы, при которых $\sum_{j=1}^{S} p_i = 1$, то имеет место задача выбора решений при риске. При этом часто отдается предпочтение действию, которое минимизирует средние затраты $\sum_{j=1}^{S} f_{ij} p_i$. Это простая задача стохастического программирования.

При решении задач в условиях неопределенности удобно использовать метод платежной матрицы, который был кратко изложен ранее, при этом необходимо выполнить действия:

- проанализировать и выбрать *представительное множество сочетаний исходных данных* (состояний природы);
- выбрать или построить критерий (затраты) и построить платежную матрицу; например, оптимизируя (см. задачу (8.1)) при каждом фиксированном j, легко получить значения диагонали матрицы и полный набор u_i (действий i);

• заполнить матрицу, рассчитав значение $f_{ij} = З_{ij}$ для каждого случая, произвести дополнительные расчеты и получить значения средних характеристик $\overline{З}$ и так называемые риски.

После заполнения матрицы и расчета дополнительных характеристик к матрице можно применить принятые в теории игр [14] минимаксные критерии и выбрать наилучший вариант действий u_i. Таков, вкратце, алгоритм метода платежной матрицы. Прежде чем обсудить применяемые минимаксные критерии, сделаем небольшое отступление.

Выбор был бы очевиден, если бы существовала такая строка k, при которой для каждого $j = 1, 2, \ldots, S$ было бы справедливо неравенство $f_{kj} \le f_{ij}$. В том случае, когда такой строки нет, говорят об оптимальности по Парето: действие *i оптимально по Парето*, если не существует такого $k \ne i$, при котором $f_{kj} \le f_{ij}$.

Введем *принцип недостаточного основания.* Этот принцип впервые был сформулирован Якобом Бернулли. Он состоит в том, что если нет основания считать одно из состояний j более вероятным, чем любое другое, то их следует считать равновероятными и сводить задачу к выбору решений при риске.

Однако имеются возражения и против этого критерия, например этот критерий, как и минимаксы, основан на предположении о полном незнании истинного состояния природы, но на практике исследователь, как правило, имеет некоторое представление (некоторую информацию) о нем. Можно ли в этом случае на состояниях природы задать некоторое априорное распределение вероятностей, отличное от равномерного и отражающее субъективное представление исследователя о сути исследуемых процессов, т.е. задать субъективные вероятности? Отметим, что это было бы очень разумно [13].

Из сказанного видно, насколько разнообразными могут быть подходы к выбору решений в условиях неопределенности и очевидно невозможно преложить какой-либо универсальный, единый для всех задач подход. Все зависит, в первую очередь, от природы задачи, а также опыта и степени осведомленности исследователя. Например, если речь идет о планировании урожайности сельхозпродукции и о погодных условиях, то вряд ли здесь оправданы ми-

нимаксные критерии, но если речь идет о вооружении или защите от предполагаемого противника, злоумышленика или диверсанта, то разумно исходить из худших случаев (наиболее консервативных решений), и преимущество минимаксных критерии тут очевидно.

Значения $З_{ij}$, записанные в *i*-й строке платежной матрицы, представляют собой неоднозначную оценку соответствующего варианта решения (при детерминированных исходных условиях имелся бы только один столбец и оценка каждого варианта была бы однозначной). Если бы вероятности отдельных сочетаний информации были бы известны, что соответствует вероятностно определенной исходной информации, то для каждого варианта можно было бы найти математическое ожидание оценочной функции $З_{ij}$ и достаточно уверенно выбрать вариант, наилучший «в среднем». Однако для условий неопределенности такая возможность отсутствует. При использовании минимаксных критериев выбора вводятся некоторые «характерные» оценки вариантов и применяются соответствующие минимаксные критерии.

Характерные оценки:

1) максимальные затраты для варианта $З_i^{\max} = \max\limits_j З_{ij}$ (наихудшее, что может дать выбор данного варианта);

2) минимальные затраты $З_i^{\min} = \min\limits_j З_{ij}$ (очевидно, что это наиболее оптимистическая оценка);

3) среднеарифметические затраты $\overline{З} = \dfrac{1}{S}\sum\limits_{j=1}^{S} З_{ij}$ (эта оценка имеет формальное сходство с математическим ожиданием и совпадает с ним в случае равновероятных исходных условий);

4) риск R_{ij} и максимальный риск $R_i^{\max}$ $\left(R_{ij} = З_{ij} - З_j^{\min},\ \text{где}\ З_j^{\min} = \min\limits_i З_{ij},\ \text{и}\ R_i^{\max} = \max\limits_j R_{ij}\right)$.

На рис.12 представлен общий вид платежной матрицы. В соответствии с принятой практикой введены новые обозначения для вектора управлений и вектора исходных данных (8.2) $\vec{u} \equiv \vec{x}$; $\vec{\mathfrak{Z}} \equiv \vec{y}$.

x/y	Платежная матрица					Характерные оценки			
	y_1	…	y_j	…	y_S	$\mathfrak{Z}_i^{\max}$	$\mathfrak{Z}_i^{\min}$	$\overline{\mathfrak{Z}}_i$	$R_i^{\max}$
x_1	$\mathfrak{Z}_{11}$	…	$\mathfrak{Z}_{1j}$	…	$\mathfrak{Z}_{1S}$	$\mathfrak{Z}_1^{\max}$	$\mathfrak{Z}_1^{\min}$	$\overline{\mathfrak{Z}}_1$	$R_1^{\max}$
x_2	$\mathfrak{Z}_{21}$	…	$\mathfrak{Z}_{2j}$	…	$\mathfrak{Z}_{2S}$	$\mathfrak{Z}_2^{\max}$	$\mathfrak{Z}_2^{\min}$	$\overline{\mathfrak{Z}}_2$	$R_2^{\max}$
…	…	…	…	…	…	…	…	…	…
x_i	$\mathfrak{Z}_{i1}$	…	$\mathfrak{Z}_{ij}$	…	$\mathfrak{Z}_{iS}$	$\mathfrak{Z}_i^{\max}$	$\mathfrak{Z}_i^{\min}$	$\overline{\mathfrak{Z}}_i$	$R_i^{\max}$
…	…	…	…	…	…	…	…	…	…
x_M	$\mathfrak{Z}_{M1}$	…	$\mathfrak{Z}_{Mj}$	…	$\mathfrak{Z}_{MS}$	$\mathfrak{Z}_M^{\max}$	$\mathfrak{Z}_M^{\min}$	$\overline{\mathfrak{Z}}_M$	$R_M^{\max}$
$\mathfrak{Z}_M^{\min}$	$\mathfrak{Z}_1^{\min}$	…	$\mathfrak{Z}_j^{\min}$	…	$\mathfrak{Z}_S^{\min}$				

Рис. 12. Платежная матрица (матрица вариантов)

Обычно при анализе платежной матрицы используются следующие минимаксные критерии: 1) Вальда; 2) Лапласа; 3) Сэвиджа; 4) Гурвица.

Критерий Вальда (минимаксные затраты или максиминной полезности). По этому критерию рекомендуется выбирать вариант, для которого

$$\min_i \mathfrak{Z}_i^{\max} = \min_i \max_j \mathfrak{Z}_{ij}.$$

Это критерий пессимизма или крайнего консерватизма. По этому критерию выбирают действие, предполагая наиболее неблагоприятное стечение обстоятельств. Он гарантирует, что наши затраты не будут больше некоторой величины при любых возможных

условиях. В этом его достоинство. С другой стороны, ориентация на самую неблагоприятную обстановку является крайне осторожным (пессимистическим, или консервативным) решением. Как правило, можно ожидать некоторого уменьшения затрат, если действовать смелее. Наиболее обосновано применение этого критерия в конфликтных ситуациях, когда каждая сторона стремится предпринять наихудшее для противника. Именно к таким ситуациям, очевидно, можно отнести ряд задач оценки эффективности СФЗ ЯОО.

Критерий Лапласа (минимума среднеарифметических затрат). Этот критерий указывает вариант, для которого

$$\min_i \overline{З}_i = \min_i \frac{1}{S} \sum_{j=1}^{S} З_{ij} .$$

Он соответствует принципу «недостаточного основания», т.е. предположению, что у нас нет оснований выделять то или иное сочетание информации, поэтому нужно поступать так, как будто они равновероятны. В этом его главный недостаток – предположение о равновероятности всех сочетаний исходных данных, отобранных для рассмотрения, лишь очень редко может считаться обоснованным. Вместе с тем такая средняя оценка затрат, бесспорно, представляет интерес.

Критерий Сэвиджа (минимаксного риска). Он основан на оценке $R_i^{\max}$:

$$\min_i R_i^{\max} = \min_i \max_j R_{ij}.$$

Это консервативный критерий, часто совпадающий с критерием Вальда. Как и в критерии Вальда, здесь используется минимаксный принцип, в связи с чем критерий Сэвиджа также может считаться консервативным. Однако, как показал опыт, рекомендации по этому критерию не всегда совпадают с действиями, наилучшими по критерию Вальда. Оперируя с относительной величиной затрат, получаем несколько иную оценку ситуации, что может и обычно

приводит к более «смелым» рекомендациям относительно выбора наилучшего варианта.

Критерий Гурвица («пессимизма–оптимизма»). По этому критерию минимизируется линейная комбинация максимальных и минимальных затрат:

$$\min_i \left[\alpha З_i^{\max} + (1-\alpha) З_i^{\min}\right],$$

где α – показатель «пессимизма – оптимизма» $(0 \le \alpha \le 1)$.

При $\alpha = 1$ критерий Гурвица превращается в критерий Вальда, а при $\alpha = 0$ – в критерий «крайнего оптимизма» (миниминный), выбор по которому предполагает наилучшее стечение обстоятельств, что явно неразумно. При $0 \le \alpha \le 1$ получается нечто среднее, и в этом привлекательность критерия Гурвица. Очевидный его недостаток в том, что параметр α должен выбирать сам исследователь, поэтому он не может объективно выявить наилучший вариант и снять неопределенность выбора. Интуитивно представляется, что значения α следует принимать в пределах от 0,5 до 1, притом тем ближе к единице, чем более серьезны возможные последствия от незнания предстоящих условий.

Аналогично критерию Гурвица можно сконструировать и другие обобщенные критерии, в которых могли бы использоваться все характерные оценки вариантов.

В заключение следует отметить, что описанный подход представляется достаточно универсальным и может быть полезен для решения многих задач. Его стержень – составление и анализ платежной матрицы задачи, которая дает упорядоченную количественную характеристику ситуации. Вместе с тем применительно к каждой конкретной задаче требуется творческая интерпретация отдельных этапов решения. Многое здесь зависит от знания особенностей задачи, глубины проникновения в ее суть, искусства и изобретательности исследователя.

Глава 9
ВЕРОЯТНОСТНЫЙ ПОХОД ПРИ ОЦЕНКЕ НАДЕЖНОСТИ ПЕРСОНАЛА

В гл. 3 надежность была рассмотрена как один из важнейших критериев безопасной и эффективной работы системы или устройства. Возникают вопросы – насколько важна надежность персонала? Возможно ли использовать формализованные подходы для оценки надежности персонала? Выбор именно данного аспекта связан с тем, что надежность оперативного персонала наряду с надежностью техники является одним из важнейших свойств, влияющих на безопасность ядерных объектов. В работе [17], например, предлагается вероятностный подход для таких оценок.

В атомной отрасли, как и во многих других отраслях, процент аварий по вине персонала достаточно велик. Примерно половина аварийных ситуаций на АС, в том числе и самых серьезных, прямо или косвенно связана с ошибками оперативного персонала. По разным оценкам по вине оператора произошло от 15 до 40% всех аварий и от 20 до 80% всех нарушений в работе. С другой стороны, не все ошибки, допускаемые персоналом, приводят к критическим последствиям, да и сами последствия ошибок существенно зависят от режима работы. Так, только 70% ошибок человека на японских АС повлияли на изменение мощности. При этом 54% из них приводили к остановке реактора, 15% - к снижению мощности. Как правило, в этих случаях результатом ошибок становятся экономические потери, которые несет станция и эксплуатирующая организация. Известны и многочисленные случаи, когда операторы спасали ситуацию – принято считать, что оперативный персонал предупреждает до 70% возможных инцидентов на ядерных объектах [18]. Однако хорошо известны и другие ошибки, приведшие к серьезным авариям на АС (США – Davis Besse (1985 г.), Crystal River-III (1991 г.), Salem-I (1994 г.) и даже к катастрофическим последствиям (Three Mile Island-II в США (1979 г.) и на Чернобыльской АЭС в СССР (1986 г.)).

В последнее время особенно отмечается, что последствия ошибочных действий персонала могут проявиться не сразу. По данным EDF (Electricite de France) в более чем 600 инцидентах, происшед-

ших по вине персонала, немедленное наступление последствий ошибок наблюдалось лишь в половине случаев; другая половина инцидентов произошла с задержкой относительно момента совершения ошибки. Примерно в половине из 83% случаев на АС Германии, когда последствия ошибок проявились с задержкой, величина этой задержки составляет от 15 мин да нескольких часов, в трети случаев – превышает 8 часов. Принято [19], рассматривая латентный период последствий ошибок, выделять три фазы движения от ошибки к аварии:

- фаза накопления, в течение которой персоналом допускаются незначительные отклонения от норм ведения процесса (как правило, на этой стадии ошибки и нарушения внешне никак не проявляются);
- фаза инициации аварии, когда происходит событие (как правило, редкое и неожиданное), для которого ранее совершенные ошибки становятся значимыми и опасными;
- фаза «взрыва», когда авария становится необратимой и развивается настолько стремительно, что у оператора не остается ни времени, ни средств для ответных действий.

Прежде чем рассмотреть причины ненадежной работы персонала, возможные пути повышения надежности и место понятия «надежность персонала», следует определиться с понятийным аппаратом. Для этого потребуется ответить на следующие вопросы.

- Что следует понимать под надежностью человека?
- Каковы причины ненадежной работы оперативного персонала?
- Каким должен быть надежный оператор?

Этой проблематике посвящено достаточно много работ российских и зарубежных ученых. Так, можно выделить работы В.Д. Небылицына, А.Ф. Дьякова и др. [20, 21], где приводятся различные определения понятия «надежность персонала», «надежность человека», «надежность оператора» и т.п. Не вступая в полемику с указанными авторами, мы будем ориентироваться на определения, данные в Концепции системы обеспечения профессиональной надежности персонала ФГУП концерна «РОСЭНЕРГОАТОМ» [22]:

1. Надежность человеческого фактора (НЧФ) – совокупность профессиональных знаний, мотивационных, волевых, интеллектуальных и других качеств личности, обеспечивающих точное, без-

ошибочное, адекватное восприятие ситуаций, своевременное и успешное выполнение регламентированных функций в различных режимах работ.

2. Надежность – вероятность того, что задача или работа будет успешно выполнена персоналом при любом требуемом уровне работы системы в течение требуемого промежутка времени (если имеется ограничение во времени).

3. Надежный работник – успешные работник, обладающий психологической готовностью, при которой обеспечение безопасности является приоритетной целью и внутренней потребностью.

Из описания наиболее известных в мире аварий и инцидентов на АС следует, что 56% ошибок было совершено операторами при работе блока на различных постоянных уровнях мощности; 35% – в переходных режимах (пуск-остановка, испытания); 9% – в стояночных режимах [23]. Подобное соотношение является типичным для большинства стран, те же причины называются и в работе [24]: сложность задачи, организация рабочего места, организация работы, процедуры (содержание, форма, несоблюдение), личные качества (профессиональная подготовка, тренированность). Подобные же причины ошибочных действий персонала были и на советских АЭС [25]. К их числу относятся:

- неудовлетворительная подготовка или недостаточная квалификация персонала;
- неудовлетворительные условия работы (микроклимат, шум, освещение и др.), недостатки компоновки рабочих мест;
- неудовлетворительное техническое оснащение и организация рабочих мест (отмечается также, что весьма значимой причиной являются неблагоприятные психологические качества человека).

Можно сделать вывод, что кроме профессиональных знаний и умений, уровня управления в широком значении этого понятия существенное значение для обеспечения надежности оперативного персонала имеют потребностно-мотивационные факторы – безответственность, небрежность, низкая мотивированность в труде – и социально-психологические факторы – неоптимальный режим труда и отдыха, морально-психологический климат, социально-политическая ситуация.

В атомной отрасли накоплены большие массивы экспериментальных данных, отражающих зависимость вероятности ошибки

оператора от различных факторов как технических и эргономических, так и социально-психологических. В качестве примера в табл. 5 и табл. 6 приведены результаты различных исследований, отражающих подобные зависимости[26].

Если детально проанализировать характеристики рабочего места оператора, можно достаточно точно определить конкретные факторы, влияющие на надежность персонала. Например, можно достаточно точно сказать, какое оборудование используется оператором, каково психологическое состояние конкретного оператора и т.п.

В подавляющем большинстве случаев на основе обширных статистических данных, накопленных в атомной отрасли, можно оценить вероятность влияния стохастических факторов, например отказ оборудования. Таким образом, мы имеем возможность определения суммарной вероятности совершения ошибки для каждого рабочего места, а точнее для каждого оператора (если учитывать и социально-психологические факторы):

$$P_{\Sigma} = \sum_{i=0}^{N} R_i P_i \quad , \qquad (9.1)$$

где N – число факторов, оказывающих влияние на надежность персонала; R_i – вероятность возникновения i-го фактора; P_i – вероятность возникновения ошибки при проявлении i-го фактора.

Таблица 5

Принятие решения

Операция	Вероятность ошибки	
	При нормальных условиях	При аномальных условиях
Диагностирование исходного события	–	0,020
Диагностирование ситуации (процесса)	0,140	0,029
Диагностика работоспособности оборудования	0,053	–
Планирование действий	0,049	0,067
Проверка логического условия ИЛИ	0,0040	0,0077

Таблица 6

Когнитивные операции

Операция	Фактор и его значения	Вероятность ошибки
Кратковременное запоминание на:	Вид информации – буквы	
0,5 с		0,1
1,0 с		0,18
1,5 с		0,28
Проверка логического условия:	–	
И		0,0040
ИЛИ		0,0034
Простые арифметические расчеты	–	0,01
Выстраивание объектов в очередь на обслуживание	Подготовленность оператора:	
	высокая	0,001
	средняя	0,052
	низкая	0,093
Обнаружение выпадающих за пределы ряда результатов	–	0,05
Обнаружение, что прибор, с которого считывается информация, поврежден (при отсутствии сигнализации об этом)	–	0,1
Обнаружение сигнала и принятие решения	–	0,048
Прием информации, ее оценка и принятие решения о работоспособности контролируемых частей системы	Число воспринимаемых признаков 1–2, задержка во времени их появления:	
	10–12 с	0,055
	3–5 и 10–12 с	0,047
	5–6 и 15–40 с	0,385
Обобщенная операция «Принятие решения»	Число логических условий:	
	1–2	0,005
	3–4	0,05
	5 и более	0,1

Следует учитывать, что возможны исключающие друг друга исходы, то есть возможны различные суммы исходных событий (факторов). Тогда для дальнейшего анализа используется P_{Σ}, имеющее максимальное значение.

Очевидно, что оптимальной будет ситуация, когда P_{Σ}=0. Однако, учитывая человеческие возможности, можно с уверенностью утверждать о нереальности данной ситуации при отсутствии полной автоматизации (в данном случае мы не рассматриваем возможные отказы оборудования).

Тогда появляется необходимость введения некоторой наиболее «желательной», критериальной суммарной вероятности $P_{\Sigma 0}$, значение которой будет определяться объективными возможностями системы управления.

В случае $P_{\Sigma} > P_{\Sigma 0}$ возникает потребность в управляющих воздействиях с целью снижения P_{Σ}. Например, изменение системы индикации на щите управления (улучшение эргономики) или направление сотрудника на повышение квалификации, которое может включать и психореабилитационные процедуры, в том случае, если выявлено, что определяющим в значении P_{Σ} являются такие причины, как стресс.

С другой стороны, задачу по снижению P_{Σ} придется решать в условиях ограничений:

- технических (например, на современном этапе технолгии невозможно изменить технические факторы, приводящие к ошибкам оператора;
- организационных (например, отсутствует необходимое количество дублеров, способных заменить персонал, направленный на обучение);
- материально-финансовых(например, отсутствуют финансы на организацию обучения или направление сотрудников на обучение в специализированные центры).

Исходя из вышеизложенного, указанная задача может быть сформулирована следующим образом. Целью управленческих воздействий является

$$P_{\Sigma} \rightarrow P_{\Sigma 0} \quad \text{при} \quad S_j < S_{kpj}, \tag{9.2}$$

где S_j – j-е ограничение на принятие решения; S_{kpj} – допустимое значение ограничения j

Однако, очевидно, что часть факторов может проявиться через определенный период времени, что требует последующего мони-

торинга влияния конкретных факторов на вероятность появления ошибок персонала. Соответственно будут скорректированы и значения P_{Σ} и P_i. Для ядерного объекта такой мониторинг не является принципиально новым. Вместе с тем применение вероятностного подхода может быть использовано также для оценки приверженности культуре безопасности в более широком смысле, чем надежность работы персонала.

Приложение

ОСНОВНЫЕ ПОНЯТИЯ И ОСОБЕННОСТИ ОЦЕНКИ БЕЗОПАСНОСТИ ДЛЯ ЯЭУ

Общие положения безопасности ЯЭУ

1. Крупномасштабное использование ядерных реакторов в электроэнергетике, теплофикации, на морском транспорте выдвинули проблему безопасности на первый план.

2. Специфика проблемы безопасности применительно к ЯЭУ заключается в том, что ЯЭУ являются сложными техническими объектами с высоким уровнем потенциальной опасности.

3. Подготовка специалистов в области проектирования и эксплуатации ЯЭУ невозможна без усвоения ими современных требований, способов обеспечения и методов анализа безопасности ядерных реакторов.

Современный подход к обеспечению безопасности наиболее четко сформулирован МАГАТЭ в «Основных принципах безопасности АС». В этом документе рассматриваются цели и принципы, осуществление которых позволяет достичь высокого уровня безопасности АС. При этом **цели** определяют, что должно быть достигнуто, а **принципы** – как должны быть реализованы эти цели.

К целям безопасности относятся:

- защита персонала АС, населения и окружающей среды от радиационной опасности;
- обеспечение при нормальной эксплуатации и авариях непревышение доз облучения на станциях и выбросов радиоактивных веществ за пределы станций на разумно достижимом низком уровне (принцип ALARA);
- предотвращение аварий и ослабление последствий проектных и запроектных аварий, контроль развития и последствий аварий.

Принципы и критерии безопасности

Технические системы большой сложности и большой мощности, каковыми являются АС, создают определенную степень риска возникновения аварии, опасной для человека и окружающей среды. Цена даже единичной аварии резко возрастает. Исходя из того, что

вероятность тяжелых аварий на ЯЭУ, по-видимому, никогда не может быть уменьшена до нуля, должны быть приняты меры, гарантирующие, что последствия любой радиационноопасной аварии будут ограничены.

Основной задачей обеспечения безопасности АС является защита населения, эксплуатационного персонала и окружающей среды от неприемлемого уровня радиационного воздействия, достигаемая как техническими средствами, так и организационными мерами.

Безопасность ЯЭУ в основном обеспечивается реализацией следующих мер и принципов:

- построением многоэшелонированной защиты от выхода в помещение АС и за ее пределы потенциально опасных радиоактивных веществ, содержащихся в ядерном топливе (топливо, оболочка, первый контур, страховочный корпус, герметичные помещения, защитная оболочка);
- высоким качеством и обоснованностью проекта реакторной установки и систем, важных для безопасности;
- высоким качеством изготовления и монтажа оборудования и систем реакторной установки;
- применением надежных средств предотвращения и подавления аварийных процессов, оснащением АС системами безопасности, предназначенными для предупреждения аварий и ограничения их последствий, самозащищенности;
- квалифицированной эксплуатацией АС и строгим соблюдением регламента, обеспечением в целом принципа «культуры безопасности»;
- принятием мер по устойчивости к внешним воздействиям и ситуациям, связанным с человеческим фактором и др.

Основное требование концепции безопасности – исключение катастрофических повреждений АС – реализуется созданием последовательных уровней безопасности (так называемая «защита в глубину»).

Задача первого уровня безопасности – предотвращение аварий и инцидентов, поддержание условий эксплуатации АС в пределах, исключающих возникновение аварий.

Задача второго уровня безопасности – защита от проектных аварий, перевод реакторной установки в безопасное состояние и предотвращение развития аварии.

Задача третьего уровня безопасности – защита от маловероятных аварий, ограничение последствий гипотетических аварий.

Решение задач первого уровня обеспечивается гарантиями качества, отработанностью конструкции ЯЭУ, надежностью систем, квалификацией персонала. Решение задач второго уровня обеспечивается наличием систем безопасности, а для решения задач третьего уровня применяется резервирование, физическое разделение, независимость каналов и систем безопасности, т.е. наличием внутренне присущих свойств безопасности.

Барьеры безопасности

При проектировании ЯЭУ одним из основных принципов безопасности является *принцип защиты в глубину*, в соответствии с которым для предотвращения и ограничения неблагоприятных последствий отказов оборудования и ошибок персонала АС предусматривается несколько уровней защиты. Важнейшим требованием принципа защиты в глубину является организация физических барьеров безопасности. На пути распространения радиоактивности (осколков деления) при их потенциально возможном выходе из топливной композиции в окружающую среду в современных реакторах имеется, как правило, три барьера, которые, учитывая их функции и значения, можно считать барьерами безопасности.

Первый барьер безопасности образует топливная композиция и оболочки твэлов. В случае нарушения этого барьера и попадания радиоактивных продуктов деления в теплоноситель, их дальнейшему распространению препятствуют системы первого контура, трубопроводы и корпусные конструкции первого контура (второй барьер безопасности). И, наконец, при протечках первого контура радиоактивные продукты деления задерживаются либо системой герметичных помещений, либо защитной оболочкой (третий барьер).

Безопасность в аварийных ситуациях

Мировой опыт эксплуатации ЯЭУ показывает, что проблема безопасности – проблема потенциально возможных маловероятных аварий по причинам отказа технических систем, ошибок персонала и внешних воздействий. Как известно, в ЯЭУ мощностью 1000 МВт (эл.) накапливаются продукты деления, суммарная радиоак-

тивность которых может достигать величины $3 \cdot 10^{20}$ Бк. Попадание накопленных радиоактивных веществ в окружающую среду имеет чрезвычайно серьезные последствия. Большая часть радиоактивных веществ находится в топливной композиции твэлов. Их выход возможен при сильном повреждении оболочки твэлов и расплавлении топлива.

Перегрев топлива происходит лишь в том случае, если интенсивность тепловыделений в твэлах превысит интенсивность теплоотвода. Такой тепловой дисбаланс в активной зоне реактора может возникнуть в двух ситуациях.

1. Авария с потерей теплоносителя 1-го контура из-за его разгерметизации или разрушения. При этом нарушается баланс между генерацией тепла и теплоотводом даже в случае прекращения цепной реакции деления при сбросе АЗ, так как остаточное тепловыделение значительно (~7% от номинальной мощности на начальном этапе аварии), а теплосъем существенно ухудшен или практически отсутствует до тех пор, пока в активную зону не будет подан теплоноситель из системы аварийного охлаждения. Это одна из наиболее тяжелых аварий, когда разрушается второй барьер безопасности (барьер системы первого контура), а первый барьер – оболочка твэлов – оказывается в тяжелых условиях работы. В этих условиях не исключено и частичное расплавление активной зоны. Кроме того активный теплоноситель попадает в помещение реакторной установки и, повышая в них давление, создает угрозу теплового и механического разрушения еще одного барьера – защитной оболочки или герметических помещений. В результате создается угроза повреждения всех трех барьеров безопасности.

2. Аварийные переходные процессы. Среди них можно выделить *процессы с ростом реактивности*, когда интенсивность тепловыделения в активной зоне увеличивается по сравнению с интенсивностью отвода тепла от нее, и *процессы с нарушением теплоотвода*, когда интенсивность последнего снижается по сравнению с интенсивностью тепловыделения в активной зоне.

Тяжелые реактивностные аварии могут инициировать одну из наиболее тяжелых ситуаций – аварию с разрушением активной зоны и одновременным разрушением всех барьеров безопасности. При аварийных переходных процессах происходят значительные отклонения основных рабочих параметров реактора от нормальных значений. Многие аварийные ситуации такого рода устраняются

системой управления, которая возвращает реактор в нормальное эксплуатационное состояние. Но некоторые могут оказаться недосягаемыми для системы управления, и тогда требуется остановка реактора системой аварийной защиты во избежание повреждения твэлов или системы первого контура – двух барьеров на пути распространения продуктов деления.

Считается, что наиболее надежно можно защитить реактор, используя внутренне присущие ему свойства безопасности и пассивные средства, т.е. с помощью свойства самозащищенности, обусловленного физико-техническими характеристиками реактора и его основных систем. Поиск решений, направленных на максимально возможную самозащищенность реакторной установки, обусловлен стремлением снизить отрицательное влияние на безопасность человеческого фактора, что особенно важно при увеличении масштабов ядерной энергетики и расширении географии ее применения. Самозащищенность реакторной установки способствует упрощению структуры и объемов активных средств защиты, неизбежно связанных с усложнением оборудования и соответствующим снижением его надежности.

Важным элементом философии обеспечения безопасности ядерных реакторов является принцип множественности барьеров и эшелонированностью защиты. В соответствии с этой философией при любом исходном событии должно оставаться не менее двух барьеров, предохраняющих окружающую среду от аварийного выброса радиоактивных веществ из активной зоны реактора. Поэтому принципиально важно, чтобы была обеспечена функциональная независимость каждого из барьеров в случае аварии.

Системы безопасности. Принцип единичного отказа

Обеспечение безопасности при возникновении аварийных режимов (аварий) осуществляется введенными в состав АС специальными системами, предназначенными для предупреждения аварий и ограничении их последствий. Системы безопасности «контролируют» аварию, выполняют следующие основные функции:

- остановку цепного ядерного процесса;
- отвод остаточного тепловыделения;
- ограничение распространения радиоактивных продуктов.

Системы безопасности подразделяются на защитные, локализующие, управляющие и обеспечивающие. Нормальное состояние систем безопасности – режим ожидания аварии, а основное требование к ним – гарантированное срабатывание и обеспечение при работе проектных характеристик.

С учетом конечного уровня надежности любых технических систем принципиальное значение имеет всесторонний анализ меры и способов резервирования, а также проверка работоспособности элементов, позволяющих снизить вероятность отказов системы. Ко всем системам безопасности необходимо применить так называемый «принцип единичного отказа». В соответствии с этим принципом при анализе безопасности АС одновременно с исходным событием постулируется единичный, независимый от исходного события отказ в системах безопасности, срабатывающих при данном исходном событии. Кратность резервирования должна быть такой, при которой, несмотря на единичный отказ в системах безопасности, функция безопасности была бы выполнена. Сам единичный отказ постулируется в любом узле системы безопасности, но одновременно только один.

Выбор принципа единичного отказа в качестве руководящего принципа для назначения кратности резервирования системы безопасности обусловлен тем, что отказы представляют собой случайные события, возникновение которых характеризуется, вообще говоря, чрезвычайно малой вероятностью. Вероятность возникновения одновременно двух и более таких независимых отказов характеризуется произведением вероятностей каждого из них. Принимается, что значение его настолько мало, что таким событием можно пренебречь.

Принято различать *активный* и *пассивный* принципы действия систем безопасности:

- активный принцип действия системы или устройства – такой, при котором для выполнения заданной функции необходимо обеспечить некоторые условия – подать команду, обеспечить энергией, рабочей средой (системы и устройства, для которых характерен активный принцип действия, называются активными);
- пассивный принцип действия системы или устройства – такой, при котором для выполнения заданной функции не требуется работа других систем и устройств (пассивные системы функционируют

под влиянием воздействий, непосредственно возникающих вследствие исходного события).

Если единичный отказ какого-либо одного элемента приводит к отказу других элементов, то все отказы являются зависимыми и рассматриваются как один отказ.

Отказы по общей причине – отказы нескольких важных для безопасности систем, возникающих вследствие одного из внутренних или внешних воздействий, отказа устройства или ошибки человека.

Общей причиной отказов может быть только то, что является общим для ряда систем или устройств безопасности:

место расположения;

внешние и внутренние условия;

источники снабжения;

технология изготовления;

материалы и др.

Поскольку отказы по общей причине не являются единичными, от них нельзя защищаться только методами резервирования.

Принципы построения систем безопасности

Для удовлетворения принципа единичного отказа и уменьшения вероятности выхода из строя важных для безопасности систем по общей причине следует использовать четыре принципа:

резервирование – применение избыточного количества систем или компонентов для обеспечения избыточной способности выполнения ответственной функции;

независимость – функционирование одной системы не должно зависеть от работы другой;

разделение – физическое отделение систем, выполняющих одну и ту же функцию, барьером или разнесение их на определенное расстояние для уменьшения вероятности одновременного отказа по общей причине;

различие (разнообразие, разнотипность) – защита систем и компонентов, выполняющих одну задачу, от однотипного отказа путем выполнения их различными по конструкции, принципу работы, технологии изготовления.

Методы анализа безопасности

Детерминистский подход основан на концепции проектных аварий и принципа единичного отказа. При этом считают, что каждая система безопасности должна выполнить заданные функции при любом из учитываемых проектом исходном событии, требующем её работы, с учетом одного (независимо от исходного события) отказа какого-либо ее элемента. Проектные исходные события, а также безопасные пределы, на соблюдение которых направлены защитные мероприятия, устанавливают исходя из накопленного опыта и инженерной ситуации.

Детерминистский подход подразумевает анализ последовательности этапов аварийного процесса от исходного события, через все возможные стадии деформации и разрушения до конечного установившегося состояния, при этом не используются количественные вероятностные данные для описания событий или сочетания событий.

Вероятностный подход находит в настоящее время все более широкое применение. Согласно ему при анализе безопасности рассматриваются всевозможные аварии, а также любое количество одновременных отказов.

Применяя метод «дерева событий» (см. гл. 4), можно довести результат анализа безопасности ЯЭУ до числового значения. Основа вероятностного подхода – системный анализ мыслимых сценариев аварий, пути развития аварийных процессов с учетом наложения отказов систем. При этом важным элементом является количественный анализ надежности оборудования и систем, важных для безопасности.

Сравнительный анализ технических решений и вероятностные оценки позволяют сделать обоснованный выбор между различными конкурирующими техническими решениями, а также исследовать чувствительность результатов к изменениям параметров.

Одним из наиболее важных результатов ВОБ является выделение сценариев аварий, которые дают наибольший вклад в последствия. Знание преобладающих последовательностей событий в авариях позволяет выделить важнейшие системы и их компоненты, что весьма полезно для совершенствования проектов. И, наконец, именно методы ВОБ могут позволить обосновать границу прием-

лемого риска и соответствие этому критерию конкретного проекта ЯЭУ.

Ограничения в использовании вероятностных методов связаны с недостаточностью данных для проведения соответствующего анализа, а также знаний о потенциальной опасности отказов, имеющих общие причины, и о поведении эксплуатационного персонала.

Поведение людей – источник неопределенности в ВОБ, поскольку люди могут считать правильными различные действия, и ошибки могут совершаться как при выполнении действий, так и при бездеятельности.

Риск

Ядерные энергетические установки, являясь источником радиоактивных продуктов, также представляют определенный риск для их персонала, населения и окружающей среды. Этот риск связан не только с эксплуатацией АЭС, но и с остальными звеньями ядерного топливного цикла. Риск определяется как мера, учитывающая вероятности аварий и их радиационные последствия (см. гл. 1). Оценка риска использует методы ВОБ, принимает во внимание и самые маловероятные (гипотетические) аварии со сценарием, полагающим наложение любого мыслимого количества технических отказов и ошибок с тяжелыми последствиями. Риск от эксплуатации АЭС считается приемлемым, если он заметно не превышает риска от других способов получения энергии.

В ядерной энергетике, как и в любой технологической деятельности человека, сопряженной с опасностью для человека, для количественной оценки возможного вредного воздействия АЭС и других предприятий на окружающую среду от тех или иных аварийных событий используют понятие риска (см. гл. 1).

Риск и ущерб от тяжелых аварий могут носить социальный, экономико-экологический и медико-биологический характер (см. гл. 4).

Медико-биологический риск в основном соотносится с индивидуальной и коллективной дозами радиоактивного воздействия при авариях с выбросом радиоактивных веществ за пределы ЯЭУ и превышением допустимого уровня облучения. В качестве меры определения ущерба здоровью можно использовать такой параметр,

как математическое ожидание сокращения предстоящей жизни в результате рассматриваемой аварии.

Основным средством снижения медико-биологического риска, выводящего его из ряда главных факторов, является строгое соблюдение «требований к размещению к АЭС», позволяющее эвакуировать население при возникновении угрожающих аварийных ситуаций.

Перечисленные риски зависят от возможной частоты аварийных событий, масштабов самих аварий, места расположения ЯЭУ, плотности населения в прилегающих районах и др.

Разнохарактерность рисков вызывает определенные трудности в определении единого приведенного риска.

Разработано к настоящему времени несколько методов оценки риска, среди которых наибольшее признание получили следующие.

1. Феноменологический метод, основанный на определении возможности или невозможности протекания аварийных процессов из анализа необходимых и достаточных условий, связанных с реализацией тех или иных законов природы. Этот метод наиболее прост при его применении, но дает надежные результаты, если защитные средства ЯЭУ построены на использовании законов природы вдали от границ резкого изменения состояния веществ. Иными словами, если условия протекания процессов в реакторной установке позволяют с достаточным запасом определять состояние ее компонентов.

Феноменологический метод хорош при определении сравнительного потенциала безопасности ЯЭУ различных типов, но мало подходит для анализа разветвленных аварийных процессов, развитие которых определяется надежностью тех или иных компонентов ЯЭУ или ее средств защиты.

2. Детерминистский метод подразумевает анализ последовательности этапов аварийного процесса от исходного процесса через предлагаемые стадии отказов, деформации и разрушения компонентов до конечного установившегося состояния системы. Ход аварийного процесса предсказывается методами математического моделирования, имитируется сложными расчетными методами. Детерминистский подход широко применяется благодаря присущей ему наглядности и наибольшей психологической приемлемости: он позволяет выявить основные факторы, влияющие на ход процесса.

Более того, *такой подход в совокупности с принципом единичного отказа является сейчас основным* в определении уровня безопасности конкретных ядерных энергоблоков в рамках нормативных документов, хотя и обладает некоторыми существенными недостатками. Существует реальная возможность упустить из вида ряд важных цепочек развития аварийных процессов: зачастую не удается найти адекватную математическую модель тем сложным аварийным процессам, которые могут развиваться при аварии. Ощущается острая необходимость в создании и постоянном усовершенствовании математических моделей аварий, а также в проведении дорогостоящих и сложных в реализации экспериментов для тестирования расчетных программ.

3. Вероятностный метод – метод, в соответствии с которым исследование риска содержит как оценку вероятности возникновения аварии, так и расчет относительных вероятностей того или иного пути развития процессов. Здесь анализируются разветвленные цепочки событий и отказов оборудования, выбирается адекватный математический аппарат и оценивается полная вероятность аварий. Расчет последствий аварийных процессов проводится с помощью математических моделей, значительно упрощенных по сравнению с детерминистскими расчетными схемами.

Основные ограничения вероятностного анализа безопасности связаны с недостатком сведений по функциям распределения параметров, а также статистических данных по отказам оборудования. При анализе тяжелых аварий упрощенные расчетные схемы и модели процессов также ограничивают доверительность получаемых оценок риска. И все же этот метод признается теперь одним из основных и наиболее подходит как действенный инструмент проектирования ЯЭУ ближайшего будущего, для которых отказы оборудования – один из основных источников тяжелых аварий.

Вероятностный анализ безопасности насчитывает четыре уровня рассмотрения аварийных процессов:

- нулевой уровень, изучающий деревья аварийных событий и отказов оборудования ЯЭУ;
- первый, рассматривающий начальное развитие тяжелых аварий вплоть до событий, ведущих к разрушению реактора;
- второй, отслеживающий процесс разрушения активной зоны реактора и последующие процессы внутри защитной оболочки энергоблока;

• третий, занимающийся исследованием процессов выброса радиоактивных материалов за пределы ЯЭУ и её возможного повреждения.

Допустимо и эффективно использование сочетаний перечисленных методов анализа риска: детерминистско-феноменологическое (анализ аварий в предположении отказа крупных групп оборудования), вероятностно-детерминистское, включающее последовательное и по возможности детальное рассмотрение различных цепочек развития аварийных процессов с отбрасыванием тех из них, вероятность которых в конкретных условиях протекания аварии признается пренебрежимо малой. При этом может быть рекомендован консервативный способ оценки вероятности отказов оборудования или защитных систем: если какое-либо аварийное событие носит вероятностный характер, но доверительная оценка его вероятности отсутствует, целесообразно считать такое событие происшедшим.

Ядерная и радиационная безопасность

Под **радиационной безопасностью** понимается совокупность условий, при которых достигается ограничение или практическое исключение вредного воздействия ионизирующих излучений на настоящее и будущие поколения людей и радиоактивного загрязнения окружающей среды, обусловленных эксплуатацией радиационно-опасных объектов и других источников ионизирующих излучений. Совокупность условий составляют принципы, нормы, правила безопасности, а также качество радиационноопасных объектов и других источников ионизирующего излучения, соблюдение, выполнение и наличие которых определяются существующим уровнем научно-технических, экономических и социальных факторов.

Под **ядерной безопасностью** понимается сохранение защищенности человека и среды его обитания от неуправляемых реакций деления на установках и изделиях, использующих делящиеся материалы, и физическая защита от несанкционированного использования этих материалов. Нарушения и аварии на установках или изделиях, использующих ядерные материалы, включая возникновение неуправляемой ядерной реакции, имеют в основном радиационные последствия. Исключение составляет взрыв ядерного боеприпаса или самодельного ядерного устройства, при котором дополнительно возникают взрывная волна и световое излучение. Поэтому часто

используют главным образом термин «радиационная безопасность».

Под системой мер обеспечения радиационной безопасности понимаются:

- процедуры и устройства для удержания доз облучения людей и рисков возникновения неблагоприятных воздействий ниже установленных пределов и на таких низких уровнях, которые реально достижимы;
- средства достижения защиты людей от воздействия ионизирующего излучения и обеспечения их безопасности;
- процедуры и устройства для предотвращения аварий в случае, если они возникают.

Основные принципы и критерии ядерной и радиационной безопасности

- Непревышение допустимых пределов индивидуальных доз облучения персонала и населения от всех видов источников ионизирующего излучения – **принцип нормирования**.
- Запрещение всех видов деятельности по использованию источников ионизирующего излучения (ИИИ), при которых полученная для человека и общества польза не превышает риск возможного вреда, причиненного дополнительным к естественному радиационному фону облучением – **принцип обоснования**.
- Поддержание на возможно низком и достижимом уровне с учетом экономических и социальных факторов индивидуальных доз облучения и числа облучаемых лиц при использовании любого ИИИ – **принцип оптимизации**.

Безопасность ядерно- и радиационноопасных объектов должна обеспечиваться во всех режимах эксплуатации, в том числе и при нарушениях и авариях. Для каждого из возможных режимов предусматриваются соответствующие технические и организационные меры. При проектировании, нормальной эксплуатации ядерных установок и других объектов ограничение радиационного облучения персонала и населения достигается путем:

- выбора площадки для размещения объекта и установления границ санитарно-защитной зоны;
- ограничения радиоактивных выбросов и сбросов с предприятий, использующих ядерные установки и радиоактивные источники;

• сведения к минимуму образования радиоактивных отходов;

• установления предельнодопустимых уровней индивидуального облучения;

• установления контрольных уровней облучения;

• ограничения коллективной дозы облучения.

В проектах ядерно- и радиационноопасных объектов должны быть предусмотрены системы безопасности и другие меры так, чтобы последствия проектных аварий по величине выбросов и сбросов радиоактивных веществ в окружающую среду не приводили к дозам облучения населения, требующим принятия обязательных мер по его защите. В случае тяжелых (запроектных) аварий и аварийного радиоактивного загрязнения окружающей среды, требующего противорадиационных мер, должны быть приняты заранее разработанные практические способы сведения к минимуму доз облучения и количества облученных лиц, радиоактивного загрязнения окружающей среды, экономических и социальных потерь. Система критериев безопасности для человека и среды его обитания, которая удовлетворяла бы вышеизложенным принципам, может основываться на концепции приемлемого риска, предлагаемой Международной комиссией по радиологической защите.

Согласно статье 13 Федерального закона РФ «О радиационной безопасности населения», оценка радиационной безопасности осуществляется по следующим основным показателям:

• характеристика радиоактивного загрязнения окружающей среды;

• анализ обеспечения мероприятий по радиационной безопасности и выполнение норм, правил и гигиенических нормативов в области радиационной безопасности;

• вероятность радиационных аварий и их масштаб;

• степень готовности к эффективной ликвидации радиационных аварий и их последствий;

• анализ доз облучения, получаемых отдельными группами населения от всех источников ионизирующего излучения;

• число лиц, подвергшихся облучению выше установленных пределов доз облучения.

Нормами радиационной безопасности НРБ-99 установлены основные дозовые пределы облучения категорий персонала и населения при нормальной эксплуатации.

СПИСОК ЛИТЕРАТУРЫ

1. Бахметьев А.М., Самойлов О.Б, Усынин Г.Б. Методы оценки и обеспечения безопасности ЯЭУ. М.: Энергоатомиздат, 1988.

2. Шевелев Я.В., Клименко А.В. Эффективная экономика ядерного топливно-энергетического комплекса. М.: РГТУ, 1996.

3. Клемин А.И. Надежность ядерных энергетических установок. М.: Энергоатомиздат, 1987.

4. Гераскин Н.И., Петрова Е.В. Теория вероятностей и прикладная математическая статистика в задачах физической защиты ядерно-опасных объектов; учета и контроля ядерных материалов. М.: МИФИ, 2001.

5. Вероятностный анализ безопасности. М.: ЯО РФ, 1992.

6. Королев А.В., Румянцев А.Н., Шмарин А.А., Сискинд Б. Вероятностный анализ эффективности усовершенствований систем физической защиты, контроля и учета ЯМ. ГНЦ ФЭИ. Обнинск, 2000.

7. Бенджамин-Альварадо Дж., Бек М., Хрипунов И., Джонс С. В поисках общей основы: к критериям оценки систем УиК ЯМ. ГНЦ ФЭИ. Обнинск, 2000.

8. Методика проектирования систем физической защиты (СФЗ). SNL, 1997.

9. Основы оценки уязвимости объектов. УМЦУК ЯМ. ГНЦ ФЭИ. Обнинск, 1998.

10. Измайлов А.В. Методы проектирования и анализа эффективности систем физической защиты ядерных материалов и установок: Уч. пособие. М.: МИФИ, 2002.

11. Архангельский В.А., Горбатенко В.М., Злобин А.М. и др. Методика оценки эффективности физических инвентаризаций. РФЯЦ-ВНИИЭФ. Материалы Международной конференции по учету, контролю и физ. защите ЯМ. Обнинск, 1997.

12. Моисеев Н.Н., Иванилов Ю.П., Столяров Е.М. Методы оптимизации. М.: Наука, 1978.

13. Райфа Г. Анализ решений. М.: Наука, 1977.

14. Оуэн Г. Теория игр. М.: Мир, 1971.

15. Вентцель Е.С. Теория вероятностей. М.: Высш. шк., 1998.

16. Ермольев Ю.М. Методы стохастического программирования. М.: Наука, 1976.

17. Селезнев Ю.Н. Системный подход к повышению квалификации персонала атомного энергопромышленного комплекса России.– Обнинск: ФГОУ «ЦИПК», 2007.

18. Третьяков В.П. Психология безопасности эксплуатации АЭС. М.: Энергоатомиздат; 1993

19. Чачко С.А. Предотвращение ошибок операторов на АЭС. М.: Энергоатомиздат, 1992.

20. Небылицын В.Д. Надежность работы оператора в сложной системе управления // Хрестоматия по инженерной психологии: Учебное пособие / Под ред. Б.А. Душкова. М.: Высшая школа, 1991. – С. 238–248.

21. Дьяков А.Ф. Надежная работа персонала в энергетике. М.: МЭИ, 1991.

22. Концепция системы обеспечения профессиональной надежности персонала ФГУП концерна «РОСЭНЕРГОАТОМ» / Утв. Генеральным директором концерна «РОСЭНЕРГОАТОМ» 10.05.2006.

23. Аварии и инциденты на атомных станциях / Под общ. ред. С.П. Соловьева. Обнинск: ИАТЭ, 1992.

24. May R.S. Knowledge-based modeling of operatorresponse for severe-accident analysis / R.S. May, A. Singh, S.P. Karla // Transactions of ANS, 1991. – Vol. 64. – P. 173-174.

25. Абрамова В.Н. Инженерная психология на АЭС. Обнинск: ИАТЭ, 1990.

26. Деревянкин А.А. Исследование, разработка и применение методов оценки надежности персонала при проведении вероятностного анализа безопасности атомных станций): Дис. канд. техн. наук. – М., 1991.

Николай Иванович Гераскин

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

Учебное пособие

Редактор Н.Н. Антонова
Компьютерная верстка Г.А. Бобровой

Подписано в печать 25.11.2008 Формат 60x84 1/16
Печ.л. 6,0 Уч.-изд.л. 6,0 Тираж 150 экз. Изд. № 4/44
Заказ № 2-2412

Московский инженерно-физический институт
(государственный университет).
115409 Москва, Каширское шоссе, 31

Типография издательства «Тровант»
г. Троицк Московской области