ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
Государственное образовательное учреждение высшего профессионального образования
«ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Б.П. Степанов, А.В. Годовых

ОСНОВЫ ПРОЕКТИРОВАНИЯ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ ОБЪЕКТОВ

Издательство
Томского политехнического университета
2009

УДК 621.039.58(076.5)
ББК 31.46я73
С12

Степанов Б.П.

С12 Основы проектирования систем физической защиты ядерных объектов: учебное пособие / Б.П. Степанов, А.В. Годовых; Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2009. – 118 с.

В пособии рассмотрены теоретические и практические вопросы проектирования, так же подробно изложены вопросы системного анализа эффективности, безопасности и надежности систем физической защиты ядерных материалов и установок.

Пособие разработано в рамках реализации Инновационной образовательной программы ТПУ по направлению «Атомная энергетика, ядерный топливный цикл, безопасное обращение с радиактивными отходами и отработанным ядерным топливом, обеспечение безопасности и противодействия терроризму» и предназначено для студентов, специализирующихся в области учета, контроля ядерных материалов и физической защиты ядерных объектов.

УДК 621.039.58(076.5)
ББК 31.46я73

Рецензент

Кандидат технических наук
ведущий инженер СХК
А.И. Соловьев

Главный инженер Реакторного завода СХК
Е.А. Комаров

СОДЕРЖАНИЕ

1. МЕТОДЫ ПРОЕКТИРОВАНИЯ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ МАТЕРИАЛОВ И УСТАНОВОК

1.1. Цели и задачи курса. Анализ и синтез СФЗ как сложной системы

В курсе «Основы проектирования систем физической защиты ядерных объектов» приведены краткие сведения о системах физической защиты (СФЗ) ядерных материалов (ЯМ) и ядерных установок (ЯУ) [1]. Из материалов данного курса можно составить представление о назначении, структуре, составе и функциях подсистем, входящих в СФЗ (рис. 1.1). Освещен также вопрос о нормативно-правовом обеспечении проблематики физической защиты (ФЗ) ЯМ и ЯУ. Введены основные термины и определения в области ФЗ [2].

Все это дает представление о СФЗ как о сложных человеко-машинных системах, в которых присутствует конфликт интересов сторон (нарушитель – система защиты). Кроме того, следует отметить, что задача физической защиты решается в условиях неопределенности, так как имеется лишь общее представление о целях вероятного нарушителя, стратегии и тактике их реализации.

Весьма актуальным является вопрос о том, как же построить такую систему, «портрет» которой мы нарисовали. При этом необходимо не только иметь представление о составных частях СФЗ, но и учитывать также их взаимосвязи, взаимодействие во времени. Поясним это на простом примере.

Средства обнаружения дают информацию о нарушении (преодолении периметра объекта, проносе ядерного материала через КПП и т. п.), физические барьеры препятствуют нарушителю, силы реагирования, получив указанную выше информацию, выполняют конечную задачу по защите объекта.

Все звенья этой цепи должны быть хорошо сбалансированы. То есть все три основные подсистемы должны функционировать во времени так согласованно, чтобы силы реагирования успели воспрепятствовать нарушителю в его акции (диверсия, хищение ЯМ).

Процесс создания СФЗ будем называть проектированием (в широком смысле слова), так как объектами проектирования являются не только технические системы, строительные конструкции, но и организационные структуры, и алгоритмы их функционирования.

Под анализом понимается определение свойств системы (характеристик и т. п.) при ее заданных структуре и составе.

Под синтезом понимается определение структуры и состава при заданных требованиях, предъявляемых к системе (по характеристикам, функциям и т. п.). В процессе синтеза необходимо решать, как правило многократно, задачу анализа.

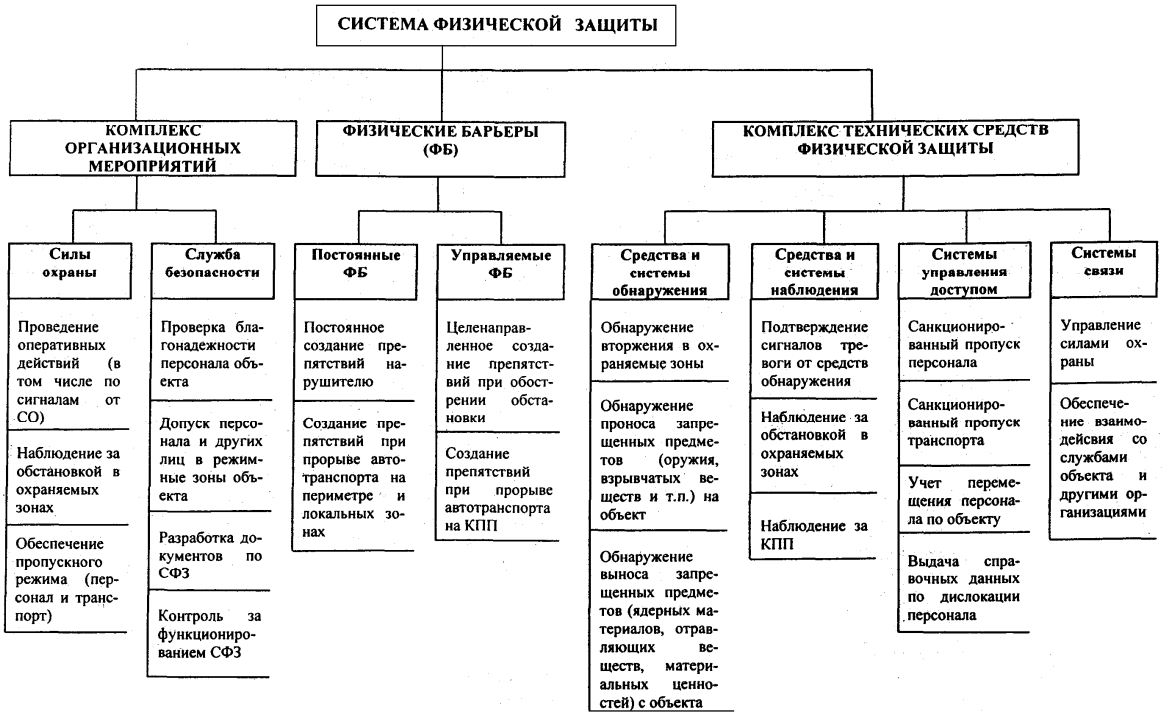


Рис. 1.1. Структура и функции системы физической защиты ядерного объекта

Кроме умения достоверно с заданной точностью определять характеристики СФЗ, необходимо иметь критерии, в соответствии с которыми производится синтез системы. В общем случае задача синтеза решается с помощью методов многокритериальной (векторной) оптимизации. Наиболее распространенным является двумерный случай: синтез сложной системы по критерию «эффективность – стоимость». Как будет показано ниже, эффективность СФЗ можно характеризовать вероятностью защиты ядерно-опасного объекта при заданной модели потенциальное нарушителя. В качестве стоимостного показателя могут выступать капитальные затраты на создание СФЗ и ее отдельных элементов, эксплуатационные затраты, в том числе трудозатраты сил реагирования и технического персонала.

Таким образом, в курсе «Основы проектирования систем физической защиты ядерных объектов» будут представлены основные принципы и процедуры проектирования СФЗ как сложной системы и методы оценки частных показателей качества СФЗ (эффективность, надежность,

стоимость и др.), используемые при проектировании. Кроме того, по сравнению с курсом «Введение в системы учета, контроля и физической защиты ядерных материалов» рассмотрим такие вопросы, как классификация ядерно-опасных объектов (ЯОО), формализация угроз и моделей нарушителей, стадии и этапы создания СФЗ (предпроектная стадия, собственно проектирование, ввод в действие). Особое внимание уделено этапу концептуального проектирования, на котором определяется «облик» системы и ее основные характеристики.

1.2. Стадии и этапы создания и совершенствования систем физической защиты

Чем же отличается процесс создания СФЗ от аналогичного процесса применительно к другим техническим и организационно-техническим системам? Прежде всего, как это было отмечено выше. СФЗ – человеко-машинная система. Далее, ее функционирование основано на конфликте сторон. И, наконец, она работает в условиях неопределенности.

Все это делает процесс создания СФЗ специфичным. Резко возрастает роль ранних (аналитических) стадий и этапов, на которых проводится анализ и принимаются концептуальные решения по структуре, составу и функциям СФЗ в целом и отдельных ее составных частей.

Стадии и этапы полного цикла создания СФЗ представлены на рис. 1.2, к которому необходимо дать некоторые комментарии.

Рис. 1.2. Стадии и этапы создания (совершенствования) СФЗ

Работа начинается с изучения ЯОО в целом (геополитическое расположение, характер производства, архитектурные особенности, климатические и природные условия и т. п.).

Предпроектная стадия начинается с анализа уязвимости ЯОО с целью определения так называемых «жизненно важных центров» (ЖВЦ) ЯОО.

В качестве примеров таких ЖВЦ можно привести: места хранения ЯМ, элементы системы, важные для безопасности ЯУ и т. п. В дальнейшем будем называть их предметами физической защиты (ПФЗ).

Затем производится категорирование ПФЗ, мест их нахождения (помещений и зданий ЯОО) и ЯОО в целом. В качестве критериев для категорирования выступают категория ЯМ и возможные последствия несанкционированных действий (ПНСД).

Концептуальное проектирование СФЗ направлено на синтез («крупными мазками») структуры и состава СФЗ и оценку основных характеристик выбранного ее варианта (вариантов). На этапе обоснования инвестиций большее внимание уделяют экономическим аспектам, схемам реализации предложенных выше концептуальных решений. После указанных этапов появляются исходные данные для составления обоснованного технического задания на СФЗ.

На стадии проектирования разрабатывается технико-экономическое обоснование (проект) СФЗ и чертежи, по которым в дальнейшем строители и монтажники будут реализовывать комплекс инженерных и технических средств физической защиты (КТСФЗ).

Стадия оборудования и ввода СФЗ в действие включает следующие основные этапы:

- закупка необходимого оборудования (комплектация в соответствии с ранее выпущенным проектом);
- проведение строительных и монтажно-наладочных работ;
- подготовка персонала СФЗ;
- испытания (различных видов) и приемка СФЗ.

Все сказанное относится и к процессу совершенствования СФЗ, когда работа начинается не «с нуля».

Следует отметить, что на всех стадиях создания и совершенствования СФЗ должна проводиться оценка эффективности СФЗ и других ее характеристик, чтобы иметь «индикаторы» правильности принимаемых на всех стадиях организационных и инженерно-технических решений.

После ввода СФЗ ответственность за ее эффективное функционирование возлагается на ЯОО в лице его руководителя.

1.3. Общие принципы построения СФЗ. Нормативное обеспечение процесса создания СФЗ

В основу создания сложных систем закладываются общие принципы, такие как надежность функционирования, унификация элементов, а также некоторые принципы, отражающие специфику именно данного

класса систем. Указанные ранее особенности СФЗ накладывают свой отпечаток на набор этих специфических принципов, основными из которых являются:

- адекватность СФЗ принятому перечню потенциальных угроз и моделям вероятных нарушителей;
- зональный принцип, эшелонирование рубежей защиты, усиление защитных мер от периферии к предметам физической защиты;
- своевременное противодействие принятым угрозам;
- равнопрочность защиты ПФЗ с учетом их ценности (привлекательности), возможных последствий несанкционированных действий и вероятности реализации нарушителем тех или иных сценариев;
- гибкость функционирования СФЗ в различных условиях;
- постоянный контроль за функционированием СФЗ, соблюдением принятых на объекте процедур.

Некоторые из указанных принципов требуют комментариев.

Принцип адекватности СФЗ угрозам связан с тем, что, если система будет рассчитана на более слабую потенциальную угрозу, то защита не будет обеспечена. Если же СФЗ будет избыточна (на всякий случай), то это чревато излишними капитальными и эксплуатационными затратами.

Зональный принцип позволяет не только создать эшелонированную систему защиты, но и фиксировать попытки преодоления нарушителем отдельных рубежей (границ зон), прогнозировать его траектории и цели, а также иметь полную (с точностью до зоны) информацию о месте нахождения персонала ЯОО.

Принцип своевременности противодействия связан с тем, что необходимо при любых рассматриваемых сценариях обеспечить выполнение соотношения

$$T_н \geq T_{ср},$$

где $T_н$ – время, необходимое нарушителю для выполнения своей акции, а $T_{ср}$ – время, необходимое силам реагирования на пресечение указанной акции при действиях по сигналам тревоги от технических средств.

Принцип равнопрочности комментариев не требует, все ясно из приведенного выше определения.

Гибкость функционирования обеспечивает адаптацию СФЗ к возможным изменениям самого ЯОО (например, местоположения ПФЗ и т. п.) или условий функционирования (сезоны, погодные условия).

И, наконец, постоянный контроль необходим для того, чтобы фиксировать любые отклонения от заданного порядка на объекте, например, контроль за правильностью выполнения процедур персоналом СФЗ.

В связи с большими объемами информации, циркулирующей в СФЗ, без автоматизации процесса контроля в современных СФЗ ЯОО не обойтись.

Вопрос о нормативном обеспечении (своего рода «законодательство») в области СФЗ был рассмотрен в предыдущих курсах. Однако там основное внимание уделялось общей структуре правовых и нормативных документов (НД) в области физической защиты ядерных материалов и установок. Однако не менее важно, как обеспечена эта тематика на отраслевом уровне и на уровне ЯОО. В данной главе мы основное внимание уделим нормативным документам, касающимся процесса создания (совершенствования) СФЗ.

Кроме упомянутых ранее основных документов федерального уровня, относящихся непосредственно к физической защите [3, 4], имеется ряд общих нормативных документов, регламентирующих строительство любых объектов в Российской Федерации. Это НД под общим названием «Строительные нормы и правила» (СНиП), определяющие стадию проектирования [5].

К сожалению, на этом уровне практически нет документов, регламентирующих работы на предпроектной стадии.

Имеется ряд документов отраслевого уровня, содержащих порядок проведения работ и методическое обеспечение этой стадии [6–10]. Это очень важно, так как результаты работ, проводимых на предпроектной стадии, в значительной степени зависят от специфики проектируемой системы.

Следует также отметить, что стадия ввода СФЗ в действие также должна быть обеспечена НД отраслевого и объектового уровня.

В заключение следует еще раз отметить, что правовые и нормативные документы упорядочивают требования и вообще всю деятельность в области ФЗ. При их отсутствии может возникнуть хаос, возрастает влияние человеческого фактора (в негативном плане) и произвола в действиях персонала СФЗ. Поэтому нормативная база является одним из ключевых звеньев во всем процессе создания, совершенствования и применения СФЗ [11].

1.4. Концептуальное проектирование СФЗ. Процедура и комментарии

С учетом специфики СФЗ как человеко-машинных систем, работающих в условиях неопределенности (нарушитель нам точно не известен, мы прогнозируем его действия), возрастает роль предпроектной стадии (рис. 1.2).

В принципе предпроектная стадия на конкретном ЯОО должна завершаться составлением обоснованного технического задания на СФЗ в

целом. Поэтому с целью обоснования предлагаемых организационных и инженерно-технических решений вводится отдельный этап – разработка концептуального проекта, на котором выполняются следующие основные работы:

- разработка перечня угроз для ЯОО;
- определение жизненно важных центров (ЖВЦ) ЯОО и их категорирование;
- разработка моделей потенциальных нарушителей;
- оценка эффективности существующей СФЗ;
- разработка вариантов создания (совершенствования) СФЗ;
- оценка основных характеристик (эффективность-стоимость, надежность и т. п.) указанных вариантов;
- выбор оптимального варианта по критерию «эффективность-стоимость»;
- разработка предложений (плана) реализации выбранного варианта с учетом ограничений практического характера (ресурсы и т. п.).

Процедура концептуального проектирования СФЗ представлена на рис. 1.3.

Необходимо дать комментарии к указанной процедуре.

На начальном этапе дается характеристика объекта в целом (тип, характер производства, геополитическое положение, природные и климатические условия). Отсюда вытекает перечень потенциальных угроз. Например, если объект АЭС, то наиболее вероятна террористическая акция, если это хранилище ЯМ (уран, плутоний и др.), то более вероятна акция хищения ЯМ и, как следствие, нарушение режима нераспространения.

Отсюда вытекает перечень потенциальных угроз. Например, если объект АЭС, то наиболее вероятна террористическая акция, если это хранилище ЯМ (уран, плутоний и др.), то более вероятна акция хищения ЯМ и, как следствие, нарушение режима нераспространения.

После этого формируется рабочая экспертная группа из представителей ЯОО и других организаций, которая проводит анализ уязвимости объекта. В процессе этой работы выявляются уязвимые места (УМ) ЯОО и вероятные последствия несанкционированных действий (ПНСД) в отношении УМ. Тут «первую скрипку» играют эксперты – технологи. Подробно этот вопрос рассмотрен в п. 5.

Затем проводится категорирование УМ, чтобы определить приоритеты в последующих мероприятиях по усилению ФЗ ЯОО.

По каждому УМ или, как ранее названо, ЖВЦ, формируются модели нарушителей (МН). Подробно этот вопрос рассмотрен в п. 6.

После этого для действующих ЯОО проводится оценка эффективности той СФЗ, которая уже функционирует на объекте.

Рис. 1.3. Процедура концептуального проектирования СФЗ

Затем начинается собственно концептуальное проектирование, основанное на синтезе СФЗ по критерию «эффективность-стоимость».

В итоге надо выбрать и обосновать структуру СФЗ в целом и ее подсистем.

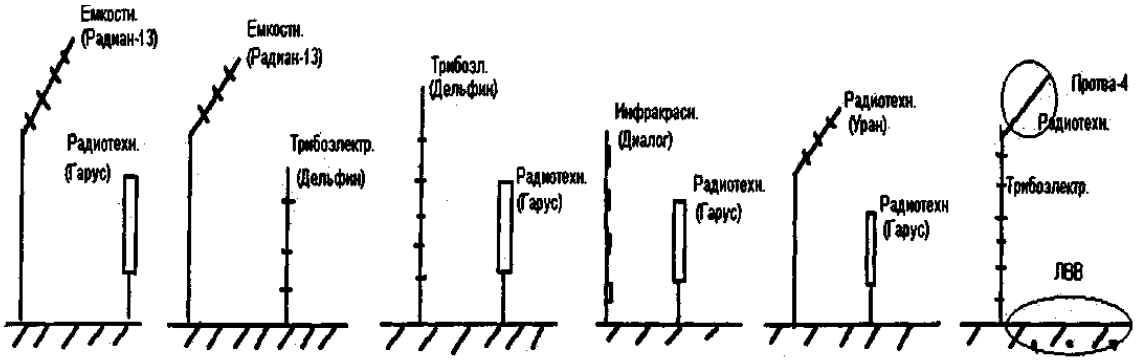


Рис. 1.4. Типовые варианты оснащения периметра средствами обнаружения

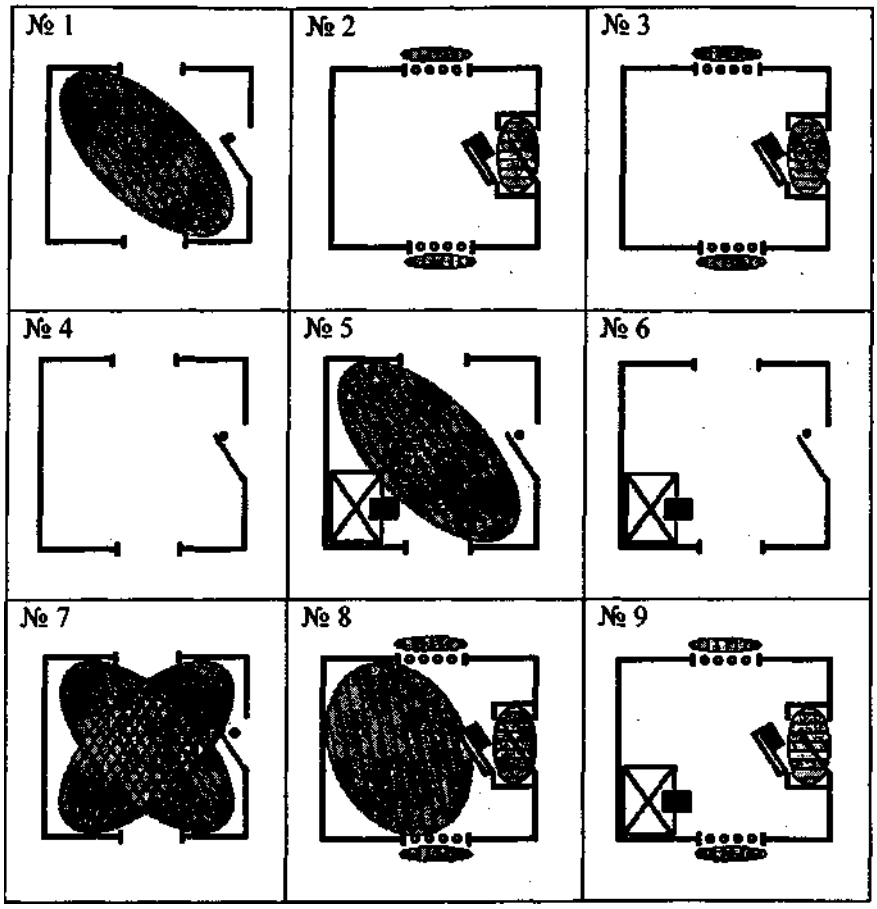
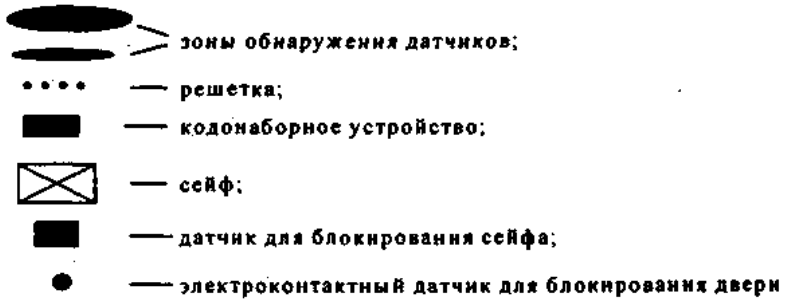


Рис. 1.5. Типовые варианты оснащения помещений средствами обнаружения:



В частности, нужно выбрать структуру и состав комплекса технических средств физической защиты (КТСФЗ), который включает в себя:

- средства обнаружения;
- средства оценки ситуации (наблюдения);
- средства управления доступом;
- средства связи и др.

При этом возможны различные сочетания технических средств, и каждый вариант обеспечивает тот или иной уровень эффективности СФЗ в целом с учетом специфики проектируемой СФЗ.

На рис. 1.4 и 1.5 показаны примеры типовых вариантов оснащения периметров объектов и помещений средствами обнаружения.

1.5. Анализ уязвимости ЯОО

В соответствии с требованиями нормативных документов [4, 7] на стационарных ЯОО должен проводиться анализ уязвимости объекта, который включает в себя, прежде всего определение внешних и внутренних угроз объекту и тех уязвимых мест, физическая защита которых должна обеспечиваться.

Результаты анализа уязвимости ЯОО используются в качестве исходных данных для проектирования СФЗ ЯОО.

Основными этапами проведения анализа уязвимости являются:

- создание рабочей группы экспертов для проведения анализа;
- разработка плана (программы) проведения анализа;
- сбор исходных данных об уязвимых местах ЯОО и предметах физической защиты;
- определение угроз и моделей нарушителя;
- оформление результатов анализа.

В соответствии с «Правилами ФЗ …» анализ уязвимости проводит администрация ЯОО с привлечением (при необходимости) специализированных организаций (силовых структур, профилирующих научно-исследовательских и проектных организаций по профилю данного ЯОО и т. п.).

Определение уязвимых мест ЯУ – это процесс выявления элементов ЯУ, которые могут быть предметами посягательства нарушителя, и мест их расположения.

Уязвимыми местами ЯОО с точки зрения хищения ЯМ являются места их хранения и использования внутри охраняемых зон.

Следует отметить, что уязвимые места по ЯМ являются более очевидными – это места нахождения ЯМ. Выявление уязвимых мест ЯУ требует проведения специальной аналитической работы. Например, ответы на вопрос, вызовет ли тяжелые радиационные последствия вывод из строя

(разрушение) того или иного элемента ЯУ (насоса, емкости, трубопровода, кабеля системы управления и т. п.), не всегда очевидны и требуют проведения достаточно серьезных исследований, моделирования ЯУ.

Выявление уязвимых мест ЯУ может производиться на основе использования логических схем и математического аппарата теории графов.

Логическая схема является эффективным средством определения уязвимых мест при рассмотрении потенциальных угроз хищения ЯМ или диверсии на ЯУ.

Рассмотрим пример, в котором опасным последствием (событием) является утечка радиоактивности в результате диверсии в отношении некоторого элемента оборудования [8].

В процессе анализа обычно строится дерево повреждений при диверсии (ДПД) рис. 1.6.

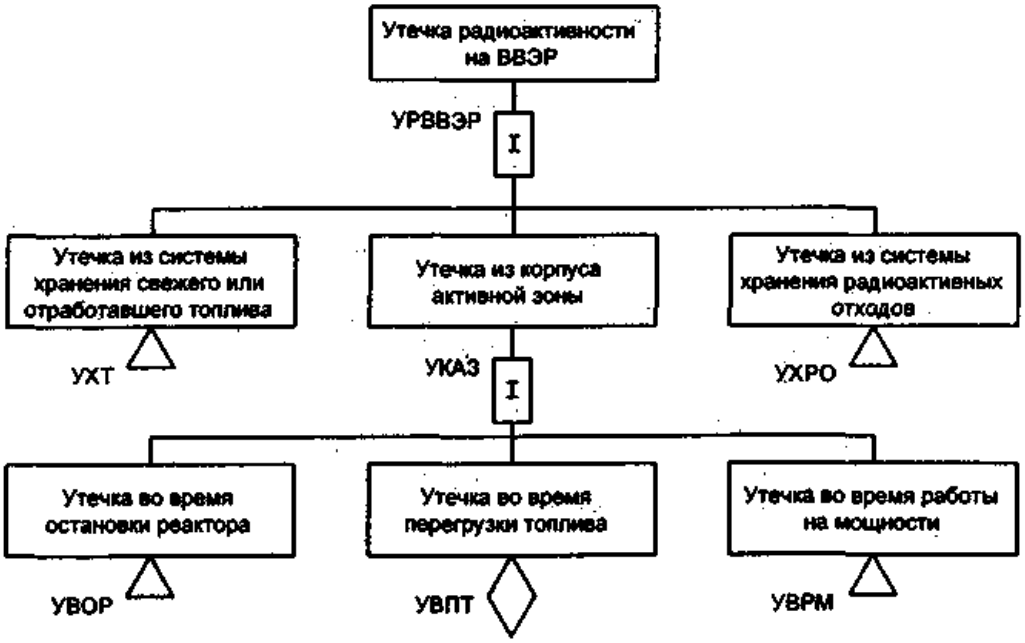


Рис. 1.6. Верхняя часть ДПД для реактора типа ВВЭР

Из рис. 1.6 видно, что конечное событие «Утечка радиоактивности» раскрывается в промежуточные события первого уровня, второго уровня и т. д., пока мы не дойдем до исходных событий. На рис. 1.7 показан пример раскрытия события с 3 по;6 уровни.

Следующим шагом в определении охраняемой зоны является определение местонахождения элемента ЯУ, повреждение которого может вызвать заданное событие. Для этого надо дерево (рис. 1.8) событий преобразовать в дерево местонахождений.

Допустим, что местонахождения М1…М5 соответствуют исходным событиям С1…С10.

Исходные события С1…С5 могут произойти в местонахождении Ml, С6 – в М2, С7 и С8 – в М3, С9 – в М5, СЮ – в М4. Анализ схемы показывает, что для совершения конечного события (верхнего на схеме) является достаточным совершение любой группы событий из следующих шести:

1) С3;
2) С4;
3) С5;
4) С1 и С2;
5) С6 и С7;
6) С8, С9 и С10.

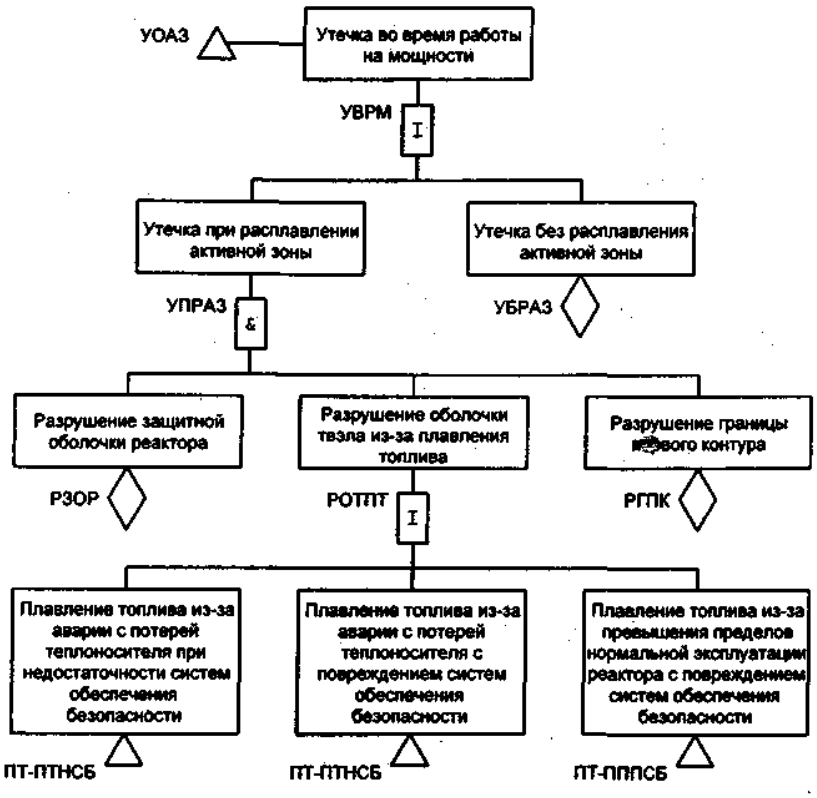


Рис. 1.7. Раскрытие события с 3 по 6 уровни

Для преобразования схемы событий в схему местонахождений необходимо определить, какие местонахождения соответствуют данным событиям. Например, группа событий под номером 6 (С8, С9 и С10) соответствует местонахождениям М3, М4 и М5. Таким образом, местонахождениями, соответствующими полученным шести группам событий, являются:

1) С3 – Ml;
2) С4 – Ml;
3) С5 – Ml;

4) C1 и C2 – Ml;
5) C6 и C7 – M2 и M3;
6) C8, C9 и C10 – M3, M4 и M5.

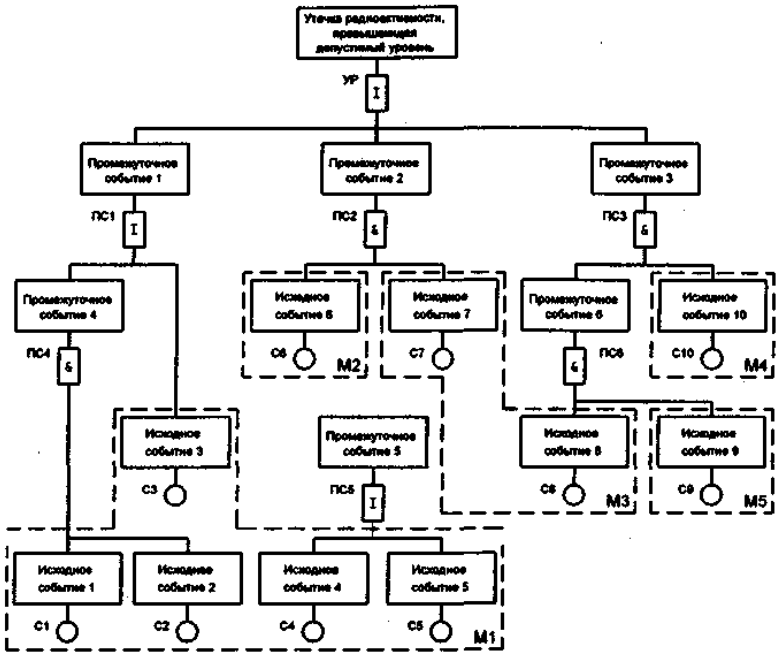


Рис. 1.8. Пример дерева событий

Это означает, что акты диверсии, способные привести к указанному конечному событию, могут быть совершены или в местонахождении Ml, или в M2 и M3 (одновременно), или в M3, M4 и M5.

Теперь строится дерево местонахождений. Следующим шагом является определение минимальных групп местонахождений (минимальных критических групп), защита которых предотвратит совершение указанного конечного события (опасного последствия). Одной из таких групп является, например, комбинация Ml и M3. Особенность этой группы состоит в том, что она имеет общие члены со всеми ранее выявленными группами местонахождений, относительно которых может быть инициировано совершение конечного события, т. е. с группами:
1) M1;
2) M2 и M3;
3) M3, M4 и M5.

Анализ показывает, что утечки радиоактивности не произойдёт, если будет исключён доступ нарушителя в любую из следующих трёх групп местонахождений:
1) M1 и M3;
2) Ml, M2 и M4;
3) M1, M2 и M5.

Эти группы называются группами защиты.

При выборе конкретной группы для принятия мер по ее физической защите необходимо учитывать стоимость и влияние этих мер на работу ЯУ.

Аналогичные, хотя и более простые примеры, можно привести и для случая хищения ЯМ.

1.6. Формализация моделей нарушителей

Одним из основополагающих моментов в процессе создания СФЗ является определение и анализ потенциальных угроз и моделей вероятных нарушителей – «проводников» этих угроз.

Нарушители бывают внешние и внутренние.

Внешние нарушители, в свою очередь разделяются на силовую группу и одиночных нарушителей.

К внутренним нарушителям можно отнести:

- вспомогательных работников ЯОО (дворники, сантехники и др.), имеющих ограниченный допуск в охраняемые зоны;
- основной персонал ЯОО, допущенный в охраняемые зоны и к ПФЗ;
- персонал охраны и службы безопасности.

Нарушители каждого типа имеют свои сильные и слабые стороны. Например, нарушители из числа основного персонала ЯОО не имеют оружия, не могут адекватно противостоять силам охраны, но допущены к предметам физической защиты, имеют высокую осведомленность. В качестве другого примера потенциальных нарушителей можно привести силы охраны, которые, хотя и имеют ограниченный санкционированный доступ в охраняемые зоны (например, в помещения), но вооружены и могут противостоять силам реагирования при обострении обстановки.

Как же формировать модель нарушителя в процессе работ на предпроектной стадии, в частности, при концептуальном проектировании?

На практике заполняется приведенная ниже специальная анкета «Модель нарушителя и задачи охраны» по каждому помещению**,** принадлежащему внутренней или особо важной зонам: Анкета заполняется на объекте экспертной группой, в состав которой входят представители ЯОО (служба безопасности, технологи, строители и т. п.), войсковых формирований, охраняющих ЯОО, специализированной организации (аналитики), под методическим руководством которых и проводится данная работа.

При заполнении анкеты надо руководствоваться следующими методическими рекомендациями.

Методические рекомендации по заполнению формы-анкеты «Модель нарушителя и задачи охраны»

Модель нарушителя для ЯОО предлагается формировать путем заполнения специально разработанной формы-анкеты (рис. 1.9).

Модель нарушителя и задач охраны

Примечание		19	
Условия эксплуатации (температура, влажность, агрессивная среда, радиоактивность и т. д.)		18	
Время движения сил охраны до подобъекта, с		17	
Возможный ущерб		16	
Место задержания нарушителя: 1 – до акции; 2 – на месте акции; 3 – после акции в здании; 4 – после акции на территории		15	
Продолжительность акции, с		14	
Место, куда необходимо проникнуть нарушителю для совершения акции: 1 – в здание; 2 – в помещение; 3 – в сейф; 4 – прочее (указать)		13	
Характер ожидаемой акции		12	
Исходное положение нарушителя: 1 – вне территории объекта; 2 – на территории объекта; 3 – внутри здания		11	
Характеристика канала проникновения		10	
Ранги каналов проникновения	Вентиляционная система	9	
	Межэтажные перекрытия	8	
	Стены	7	
	Окна	6	
	Двери	5	
Ранг (категория) подобъекта охраны		4	
Номер помещения		3	
Этаж		2	
Здание		1	

Рис. 1.9. Пример формы-анкеты

Примечание. Кроме того, при разработке модели нарушителя указанные данные необходимо дополнить информацией описательного характера (развернутой характеристикой целей и задач нарушителя, его возможностей и т. п.).

В некоторых графах указываются соответствующие коды, которые приведены в шапке таблицы. Если вопрос для данного подобъекта не имеет смысла, то в соответствующей графе ставится прочерк (например, если сооружение не имеет окон, то в графе 6 нужно поставить прочерк).

Ниже приведены комментарии к содержанию отдельных граф формы-анкеты.

Графа 1 – наименование объекта охраны (номер здания, его назначение).

Графа 2 – этаж, на котором находится подобъект охраны.

Графа 3 – номер охраняемого помещения.

Графа 4 – ранг (категория) подобъекта охраны, который отражает его важность. Присваивается по 10-бальной шкале, т. е. самым важным подобъектам присваивается ранг 10, другим подобъектам (в соответствии с их важностью) методом экспертных оценок присваиваются ранги в диапазоне от 1 до 9. Этот ранг понадобится для определения приоритетов и при оценке эффективности СФЗ.

Графы 5–9 – ранги возможных путей (каналов) проникновения нарушителя в помещения и сооружения. Ранги присваиваются по 10-бальной шкале, наиболее вероятному каналу проникновения присваивается ранг 10, далее соответствующие ранги присваиваются по мере убывания вероятности проникновения через данный канал. Для каналов, проникновение через которые маловероятно, устанавливается ранг 0. Эти ранги понадобятся при оценке эффективности СФЗ и при проектировании КТСФЗ.

Графа 10 – характеристики каналов проникновения. Указываются такие параметры как материал, из которого изготовлены двери, решетки, размеры окон, толщина дверей и т. д.

Графа 11 – вероятное исходное положение нарушителя, откуда он может начать свои действия (до срабатывания средств обнаружения периметра, здания, помещения соответственно).

Например, в случае, если исключено легальное появление нарушителя на территории или невозможно преодоление им периметра без выдачи сигнала срабатывания, указывается, что исходным положением нарушителя является «вне территории». При наличии нескольких вариантов исходного положения нарушителя в графе 11 указывается наиболее «опасное» по отношению к охраняемому подобъекту исходное положение.

Графа 12 – характер ожидаемой акции, которую может совершить нарушитель.

Графа 13 – место, куда необходимо проникнуть нарушителю для совершения акции (связано с характером ожидаемой акции, см. графу 12).

Графа 14 – продолжительность акции. Указывается вероятное время собственно акции нарушителя (без учета времени преодоления инженерных препятствий: решеток, дверей, сейфов и т. п.) в секундах. Это время определяется на основе экспертных оценок специалистов соответствующих служб предприятия.

Графа 15 – место, где допускается задержание нарушителя после (в процессе) совершения им акции, т. е. где еще не поздно пресечь акцию.

Графа 16 – указываются возможные последствия, к которым может привести осуществление указанной в графе 12 акции.

Графа 17 – время движения сил охраны от места дислокации до соответствующего подобъекта.

Графа 18 – условия эксплуатации, влияющие на работоспособность ТСФЗ (температура, влажность, агрессивная или взрывоопасная среда, наличие радиоактивности, источники электромагнитных помех и т. п.).

Графа 19 – указываются дополнительные сведения, которые не относятся к предыдущим графам, но представляют интерес для разработчиков системы физической защиты. Например, возможное наличие у нарушителя ключей от охраняемых помещений и сейфов, установленные на настоящий момент технические средства охраны и т. д.

Результаты заполнения формы-анкеты будут использованы в процессе оценки эффективности СФЗ и при выборе конкретных организационных и проектно-технических решений.

1.7. Оценка эффективности СФЗ

Для объективной оценки приспособленности любой системы к выполнению возложенных на нее задач необходимо иметь метод оценки эффективности данной системы. Такие методы могут быть качественными, но лучше, если в их основу положены количественные показатели, позволяющие сравнивать различные варианты системы.

Эффективность как свойство конкретного класса систем зависит от их специфики. В частности, применительно к СФЗ можно дать следующее определение.

Эффективность СФЗ представляет собой свойство системы, заключающееся в способности СФЗ противостоять действиям нарушителя в отношении ядерных материалов (ЯМ), ядерных установок (ЯУ), других уязвимых мест (УМ) ЯОО и предметов физической защиты (ПФЗ) с учетом определенных в процессе анализа уязвимости ЯОО угроз и моделей нарушителя. Обеспечение необходимого уровня эффективности СФЗ должно предусматривать комплекс работ по контролю и ана-

лизу выполнения СФЗ возложенных на нее задач по обеспечению физической защиты и определению путей повышения эффективности СФЗ или поддержания ее на требуемом уровне.

Для унификации подходов к оценке эффективности в Минатоме разработан соответствующий нормативный документ [8].

Для определения эффективности СФЗ необходимо оценить способности СФЗ пресечь несанкционированные действия нарушителя. Под термином пресечение понимается своевременный выход сил охраны на рубежи (к месту) нейтрализации нарушителя.

Задачами оценки эффективности являются:

- выявление элементов СФЗ, преодолевая которые, нарушитель имеет наибольшую вероятность совершения Диверсий или хищения ЯМ;
- рассмотрение и выявление наиболее вероятных сценариев действий нарушителя для совершения диверсий или хищения ЯМ;
- выявление уязвимых мест действующих СФЗ, формально отвечающих требованиям, установленным в нормативных документах;
- анализ причин появления уязвимых мест в СФЗ;
- оценка вероятности пресечения тех или иных действий нарушителя силами охраны, действующими по сигналу тревоги при внешней и внутренней угрозе;
- выбор оптимальных проектных решений на этапе создания и модернизации СФЗ;
- подготовка предложений администрации ЯОО и силам охраны ЯОО по совершенствованию СФЗ и ее отдельных структурных элементов.

Проведение оценки эффективности СФЗ обязательно на этапе проектирования СФЗ, при ее создании или совершенствовании. Количественный показатель эффективности может быть использован в процессе проектирования СФЗ для сравнения конкурирующих вариантов СФЗ, в том числе для обоснования целесообразности проведения модернизации СФЗ. При этом сравниваются показатели эффективности существующей СФЗ и предлагаемого варианта СФЗ.

Для действующей СФЗ оценка эффективности проводится в полном объеме при отсутствии на ЯОО результатов ранее проведенной оценки эффективности СФЗ с привлечением специализированной организации, а также в следующих случаях:

- при планируемых изменениях на объекте в СФЗ ЯОО;
- по результатам проведения анализа уязвимости ЯОО;
- при выявлении новых уязвимых мест в результате государственного надзора, ведомственного и внутриобъектового контроля безопасности ЯОО.

В указанных случаях может проводиться как оценка эффективности СФЗ в полном объеме, так и уточнение результатов оценки эффективности, проведенной при проектировании СФЗ.

Основанием для проведения оценки эффективности при планируемых изменениях на объекте ив СФЗ, ЯОО являются:

- изменение структуры объекта и дислокации УМ и ПФЗ ЯОО;
- изменение вида или способа охраны;
- изменение численности подразделений охраны;
- передислокация мест расположения сил охраны;
- другие причины**,** связанные с изменением времени реагирования охраны на сигналы тревоги;
- изменение структуры и состава комплекса технически; средств физической защиты (КТСФЗ).

Основанием для проведения оценки эффективности по результатам проведения анализа уязвимости действующего ЯОО, а также государственного надзора, ведомственного и внутриобъектового контроля безопасности ЯОО являются:

- уточнение модели нарушителя;
- уточнение и выявление новых УМ и ПФЗ, в отношении которых могут быть совершены несанкционированные действия;
- выявление новых угроз для ЯОО и способов их осуществления;
- изменение технологических процессов на ЯОО;
- выявление элементов СФЗ, которые не отвечают предъявляемым к ним требованиям;
- выявление элементов СФЗ, преодолевая которые нарушитель имеет благоприятные возможности для совершения диверсий или хищения ЯМ или других ПФЗ;
- другие причины, повышающие уязвимость ЯМ, ЯУ и других ПФЗ.

Как отмечалось выше, в качестве основного критерия оценки эффективности СФЗ принимается способность СФЗ пресечь несанкционированные действия нарушителя. Эффективность СФЗ оценивается количественными показателями, отражающими вероятность пресечения несанкционированных действий нарушителя силами охраны, действующими по сигналу тревоги.

Показатели эффективности зависят от определенных в процессе анализа уязвимости ЯОО угроз, моделей нарушителя и уязвимых мест. Для оценки эффективности СФЗ применяют:

- дифференциальный показатель эффективности, учитывающий вероятность пресечения акции нарушителя против одной цели (УМ, ПФЗ);
- интегральный показатель**,** представляющий собой усредненный с учетом важности целей показатель эффективности СФЗ по ЯОО в целом.

При оценке эффективности учитываются:

- вероятности обнаружения нарушителя техническими средствами физической защиты (ТСФЗ);
- время задержки нарушителя физическими барьерами (ФБ);
- времена движения сил охраны и нарушителя на ЯОО;
- взаимное расположение технических средств (возможность определения направления движения нарушителей);
- наличие систем и средств оптико-электронного наблюдения;
- наличие средств идентификации вторжения (контрольно-следовая полоса, пломбы);
- тактика действий сил охраны;
- оснащение нарушителя (транспортные средства, инструменты, оружие и др.).

Оценка эффективности основана на событийно-временном анализе развития конфликтной ситуации в системе «охрана – нарушитель» при внешней и внутренней угрозах.

Цели нарушителя рассматриваются только в стационарном состоянии.

Оценка эффективности СФЗ проводится для двух типов акций нарушителя:

- хищение ЯМ и других ПФЗ;
- диверсия против ЯМ, ЯУ или пункта хранения ЯМ.

Работы обычно проводятся в два этапа. На первом этапе, на основе инженерных расчетов, проводится предварительная оценка эффективности СФЗ. На втором этапе, с помощью специализированного программного обеспечения, проводится окончательная оценка эффективности СФЗ.

Работа проводится в следующей последовательности:

- формирование рабочей группы и организация совещания специалистов по оценке эффективности СФЗ ЯОО;
- сбор исходных данных для проведения оценки эффективности СФЗ ЯОО;
- разработка формализованного описания ЯОО;
- оценка эффективности СФЗ ЯОО при внешней угрозе;
- оценка эффективности СФЗ ЯОО при внутренней угрозе;
- оформление и анализ результатов оценки эффективности СФЗ ЯОО.

Оценка эффективности СФЗ проводится отдельно для внешних и внутренних угроз.

Эффективность СФЗ при внешней угрозе проводится для всех УМ ЯОО и ПФЗ с учетом моделей нарушителя, разработанных при проведении анализа уязвимости ЯОО и уточненных на этапах сбора ИД и составления формализованного описания объекта.

При расчетах показателя эффективности предполагается, что внешний нарушитель при преодолении каждого из рубежей СФЗ может выбрать один из двух вариантов действий:

- вариант 1 – внешний нарушитель преодолевает рубеж ФЗ, по возможности, скрытно. Такой вариант характеризуется низким значением вероятности обнаружения и значительным временем преодоления ФБ;
- вариант 2 – внешний нарушитель преодолевает рубеж ФЗ, по возможности, быстро, в том числе, используя специальные силовые инструменты и взрывчатые вещества для разрушения ФБ. Такой вариант характеризуется высоким значением вероятности обнаружения и малым временем преодоления ФБ.

Оценка эффективности СФЗ при внешней угрозе должна проводиться для обоих вариантов действий нарушителя.

Интегральный показатель эффективности СФЗ ЯОО при внешней угрозе ($P_{внеш}$) оценивается исходя из выражения:

$$P_{внеш} = \sum_{j=1}^{J} \beta_j \bullet P_{внеш\,j}, \qquad (1.1)$$

где j – число целей нарушителя на ЯОО (УМ ЯОО, ПФЗ); β_j – весовой коэффициент, отражающий важность (категорию) j-й цели; $P_{внеш\,j}$ – дифференциальный показатель эффективности СФЗ, вероятность предотвращения акции внешнего нарушителя против j-й цели.

Весовой коэффициент β_j определяется следующим образом:

рабочая группа экспертным путем присваивает каждой цели нарушителя ранг (R_j) от 1 до 10 в зависимости от последствий, которые может повлечь за собой акция нарушителя или категории, присвоенной УМ ЯОО, ПФЗ. Больший ранг присваивается более важной цели;

β рассчитывается по формуле:

$$\beta_j = R_j / \sum_{j=1}^{J} R_j. \qquad (1.2)$$

Дифференциальный показатель эффективности СФЗ оценивается исходя из выражения:

$$P_{внеш\,j} = 1 - \prod_{k=1}^{K} (1 - P_{внеш\,jk}), \qquad (1.3)$$

где k – общее количество отдельных тактических групп сил охраны (периметровая тревожная группа и др.), участвующих в развитии кон-

фликтной ситуации при проникновении нарушителя на ЯОО; $P_{внеш\,jk}$ – вероятность пресечения k-й тактической группой сил охраны акции внешнего нарушителя против j-й цели.

При рассмотрении нескольких сценариев действии нарушителя против j-й цели, дифференциальный показатель эффективности СФЗ этого УМ ЯОО, ПФЗ принимается равным минимальному значению по всем рассмотренным сценариям.

Сценарий действий нарушителя, соответствующий минимальному значению вероятности предотвращения акции против j-й цели, принимается в качестве критического.

Вероятность предотвращения k-й тактической группой сил охраны акции внешнего нарушителя против j-й цели в общем случае является функцией:

$$P_{внеш\,jk} = f(P_{o\,jl}, P_{зах\,jkl})(l = 1,\ldots,L), \tag{1.4}$$

где l – общее количество рубежей СФЗ, которые необходимо преодолеть внешнему нарушителю для проникновения к j-й цели; $P_{o\,jl}$ – вероятность обнаружения нарушителя, действующего против j-й цели на l-м рубеже СФЗ; $P_{зах\,jkl}$ – вероятность захвата k-й тактической группой сил охраны, действующей по сигналам начиная с l-го рубежа СФЗ, нарушителя, совершающего акцию против j-й цели.

Вероятности обнаружения принимаются равными значениям тактико-технических характеристик для соответствующих ТСФЗ, указанным в технической документации.

Численные значения вероятностей $P_{внеш\,jk}$ оцениваются согласно выражениям, приведенным в справочном приложении к нормативному документу [8].

Вероятности захвата нарушителя определяются с учетом выполнения условия:

$$\Delta T = T_o - T_н < 0 \tag{1.5}$$

для соответствующей оперативной ситуации. Здесь ΔT – резерв времени сил охраны; T_o и $T_н$ – времена действий охраны и нарушителя (с момента поступления сигнала тревоги) соответственно. Вероятности захвата оцениваются согласно выражению:

$$P(\Delta T = T_o - T_н < 0) = F(-x), \tag{1.6}$$

где $F(-x)$ – функция распределения стандартной нормальной случайной величины; x – математическое ожидание приведенного резерва времени сил охраны, определяемое из выражения:

$$x = \frac{M[T_o] - M[T_н]}{\sqrt{D[T_o] - D[T_н]}}, \tag{1.7}$$

где $M[T]$ и $D[T]$ – соответственно математическое ожидание и дисперсия времен сил охраны и нарушителя.

Значения времен нарушителя и охраны складываются из составляющих, относящихся к различным этапам их действий (для нарушителя – время преодоления ФБ периметра, локальных зон, зданий, помещений т. п.; для сил охраны – время сборов, время движения, время осмотра участка периметра и т. п.). Расчет математических ожиданий и дисперсий времен действий нарушителя и охраны производится исходя из соотношения для суммы независимых случайных величин, согласно которому при $T = \sum_{i=1}^{I} M[t_i]$ имеем:

$$D[T] = \sum_{i=1}^{I} D[t_i], \tag{1.6}$$

где t_i, $i = 1,\ldots,I$ – отдельные случайные величины; $M[t_i]$ и $D[t_i]$ – математические ожидания и дисперсии величин t_i.

Оценка эффективности СФЗ при внутренней угрозе проводится для всех УМ ЯОО и ПФЗ с учетом полномочий различных групп персонала объекта. Под группой персонала понимается группа сотрудников ЯОО, имеющих одинаковые полномочия доступа.

Оценка эффективности должна проводиться для каждой группы персонала отдельно.

При расчетах показателя эффективности предполагается, что внутренний нарушитель при преодолении каждого из рубежей СФЗ может выбрать один из двух вариантов действий.

- Вариант 1 – внутренний нарушитель преодолевает рубеж ФЗ, используя свои служебные полномочия, по путям санкционированного прохода. При этом, для уменьшения вероятности пресечения акции, внутренний нарушитель может пытаться выбросить/забросить запрещенные к проносу предметы из/в зону ФЗ, используя каналы, не доступные для проникновения человека (трубопроводы, окна верхних этажей, между прутьев решетки и пр.).;

- Вариант 2 – внутренний нарушитель преодолевает рубеж ФЗ «силовым» способом, используя несанкционированный канал проникновения, аналогично внешнему нарушителю. Предполагается, что последующие рубежи ФЗ нарушитель преодолевает также «силовым» способом.

Оценка эффективности СФЗ при внутренней угрозе проводится в предположении, что сценарий действий нарушителя состоит из двух частей – проход с использованием своих полномочий до какой-либо зоны ФЗ и затем – «силовой» прорыв. В частном случае, второй этап действий нарушителя может отсутствовать.

При оценке рассматриваются различные наборы инструментов и материалов, которые нарушитель может проносить на объект и использовать при прорыве к цели и совершении акции.

При оценке учитывается возможность использования для совершения несанкционированных действий инструментов и материалов, находящихся на ЯОО в силу производственной или иной необходимости.

Интегральный показатель эффективности СФЗ ЯОО при внутренней угрозе ($P_{внут}$) для каждой из целей оценивается исходя из выражения:

$$P_{внут} = \sum_{i=1}^{I} \gamma_i \bullet P_{внут\ i}, \qquad (1.7)$$

где i – число групп персонала, выделенных на объекте, применительно к рассматриваемой цели; γ_i – весовой коэффициент, равный отношению числа лиц, относящихся к i-й группе к общему числу сотрудников ЯОО; $P_{внут\ i}$ – дифференциальный показатель эффективности СФЗ ЯОО при внутренней угрозе – вероятность предотвращения акции нарушителем из числа i-й труппы допуска против рассматриваемой цели.

Дифференциальный показатель эффективности СФЗ ЯОО оценивается, исходя из выражения:

$$P_{внут\ j} = 1 - (\prod_{l=1}^{L}(1 - P_{внут\ il})) \bullet (1 - P_{il}), \quad (1.8)$$

где l – количество рубежей ФЗ, преодолеваемых нарушителем с использованием своих служебных полномочий; $P_{внут\ il}$ – вероятность задержания нарушителя, проносящего запрещенные предметы или объект хищения, на контрольно-пропускном пункте (КПП) 7-го рубежа ФЗ; P_{il} – вероятность захвата нарушителя, действующего «силовым» способом из секции, находящейся за l-м рубежом ФЗ.

При рассмотрении нескольких сценариев действий внутреннего нарушителя против j-й цели, дифференциальный показатель эффек-

тивности СФЗ этого УМ ЯОО, ПФЗ принимается равным минимальному значению по всем рассмотренным сценариям.

Вероятность задержания нарушителя на КПП, проносящего запрещенные предметы и материалы, в общем случае определяется из выражения:

$$P^*_{внут} = 1 - (1 - P^*_{досм} \cdot P_{досм}) \cdot (1 - P^*_{мет} \cdot P_{мет}) \cdot (1 - P^*_{ВВ} \cdot P_{ВВ}) \cdot (1 - P^*_{ям} \cdot P_{ям}), \quad (1.9)$$

где $P^*_{досм}$ – вероятность проведения личного досмотра; $P_{досм}$ – вероятность обнаружения запрещенных предметов при досмотре; $P^*_{мет}$ – вероятность проведения досмотра с применением металлообнаружителя; $P_{мет}$ – вероятность обнаружения металлических предметов при помощи металлообнаружителя; $P^*_{ВВ}$ – вероятность проведения досмотра с применением детектора взрывчатых веществ (ВВ); $P_{ВВ}$ – вероятность обнаружения ВВ при помощи детектора ВВ; $P^*_{ЯМ}$ – вероятность проведения досмотра с применением детектора ЯМ; $P_{ЯМ}$ – вероятность обнаружения ЯМ при помощи детектора.

Примечание**:** если у нарушителя отсутствует тот или иной, запрещенный к проносу материал или предмет, то вероятность обнаружения для соответствующего детектора принимается равной «0».

Вероятности захвата внутреннего нарушителя действующего «силовым» способом (P_{li}), определяются аналогично вероятностям захвата внешнего нарушителя. При этом не учитываются рубежи ФЗ, пройденные внутренним нарушителем легальным способом (считается, что нарушитель дошел до секции, находящейся за l-*м* рубежом ФЗ, необнаруженным).

1.8. Оценка других показателей качества СФЗ

Показатель эффективности СФЗ является основным показателем качества, характеризующим применение СФЗ по назначению. Однако на практике любая Система определяется и другими показателями. Например, немаловажным фактором являются затраты на создание и эксплуатацию системы; Важны также и другие свойства системы (надежность, помехоустойчивость и др.).

Чтобы оценить СФЗ на наличие каждого из этих свойств, необходимо:

- выбрать количественный показатель, характеризующий данное свойство;
- разработать методику его оценки;
- иметь необходимые исходные данные.

Например, количественным показателем затрат является стоимость необходимого оборудования СФЗ и работ по оснащению ЯОО техническими средствами физической защиты. Методика получения стоимостных показателей достаточно проста и традиционна – это сметные расчеты. Размерность данного показателя (рубль или USD) также понятна.

Надежность КТСФЗ, как и любой другой технической системы, характеризуется показателями безотказности (среднее время наработки на отказ и др.), ремонтопригодности (среднее время восстановления и др.) и т. п.

Помехоустойчивость обычно характеризуется таким показателем, как среднее время наработки на ложное срабатывание технических средств.

Можно предложить использовать показатели, характеризующие такие «тонкие» свойства системы, как скорость развертывания сигнализационных средств (для мобильных технических средств), маскируемость и др.

Имеются соответствующие методики, которые позволяют получить количественную оценку указанных показателей, а также соответствующие базы исходных данных.

1.9. Компьютерные программы для оценки эффективности СФЗ

Ранее были освещены методы оценки эффективности СФЗ.

Следует отметить, что работа по сбору необходимых ИД, подготовке к расчетам и непосредственно оценке эффективности СФЗ требует проведения значительного количества рутинных действий и вычислений. При этом в процессе разработки концептуального проекта оценка эффективности проводится неоднократно, по мере выбора оптимальных (целесообразных) решений. Эти и ряд других факторов неизменно приводят к мысли о необходимости автоматизации процедуры оценки эффективности СФЗ и, как следствие, к разработке специализированных компьютерных программ. Техническая революция в области создания и применения персональных компьютеров сделала эту задачу актуальной и выполнимой.

В России широко известны американские специализированные компьютерные программы, предназначенные для оценки эффективности СФЗ, такие как:

- EASY, SAVI – программы MS DOS для оценки эффективности СФЗ при «внешней» угрозе [12];
- ET – программа MS DOS для оценки эффективности при «внутренней» угрозе;
- ASSESS – WINDOWS – программа для оценки эффективности СФЗ при «внешней» и «внутренней» угрозах, при сговоре «внешнего»

и «внутреннего» нарушителей, расчета вероятности нейтрализации вооруженного противника [13].

Наибольшее распространение в России получила программа ASSESS, переданная российским ЯОО в рамках международного сотрудничества. Эта программа имеет ряд существенных преимуществ, по сравнению с более ранними американскими специализированными компьютерными программами.

Однако в ходе применения программы ASSESS российскими ЯОО и с приобретением практического опыта работ, был выявлен ряд недостатков этой программы, ограничивающих возможности ее применения на российских ЯОО. Например, в программе ASSESS заложена жесткая тактика действий сил реагирования, не всегда соответствующая российской специфике. Кроме того, в составе программы ASSESS отсутствует база данных по реальным тактико-техническим характеристикам ТСФЗ и ФБ, относящихся к чувствительной информации.

В России также ведутся работы по созданию отечественных специализированных компьютерных программ оценки эффективности СФЗ, позволяющих максимально полно учитывать российскую специфику. Можно отметить следующие компьютерные программы, разработанные ГУП СНПО «Элерон»:

- АЛЬФА – программа MS DOS для оценки эффективности СФЗ при «внешней» угрозе на объектах с жестко заданной структурой рубежей СФЗ;
- ВЕГА-2 – WINDOWS-программа для оценки эффективности СФЗ как при «внешней», так и при «внутренней» угрозах, позволяющая производить расчеты на основе аналитического метода и имитационного моделирования [14].

Особенно следует отметить программный комплекс (ПК) ВЕГА-2, который дает возможность более гибко описывать тактики действий сил охраны и вероятного нарушителя, учитывает целеуказующую функцию средств обнаружения, существенную для объектов с разветвленным деревом целей нарушителя, позволяет оценить вклад применения охранного телевидения на различных рубежах ФЗ и др. ПК ВЕГА-2 постоянно совершенствуется и модернизируется с учетом практического опыта его применения на конкретных ЯОО.

Остановимся более подробно на компьютерных программах ASSESS и ВЕГА-2.

Эти программы объединяет общий подход к их построению. Программы являются модульными, при этом рабочие модули программ объединяются специальными оболочками-менеджерами в программные комплексы.

Американская программа ASSESS содержит следующие основные модули для оценки эффективности системы ФЗ:

1. Facility (объект) – для описания объекта;
2. Outsider (внешний нарушитель) – при внешней угрозе;
3. Insider (внутренний нарушитель) – при внутренней угрозе;
4. Collusion (сговор) – при сговоре внешнего и внутреннего нарушителей;
5. Neutralization (нейтрализация) – для оценки результатов боестолкновения сил реагирования (охраны) и нарушителя.

Как уже отмечалось ранее, программа ASSESS является WINDOWS-приложением и работа с ней производится с помощью стандартных приемов, используемых для работы в WINDOWS. В связи с этим, при дальнейшем изложении материала вопросы запуска программ, сохранения, загрузки, копирования и удаления файлов не рассматриваются.

Для инициализации работы программы ASSESS необходимо запустить файл Assess.exe, активизирующий работу менеджера.

Работа с программой начинается с создания файла описания объекта с помощью запуска программы Facility.

Объект физической защиты описывается так называемыми схемами последовательности действий нарушителя (СПДН), представляющими собой графическое описание объекта, включающее в себя:

- зоны защиты – какие-либо части территории объекта, например, не охраняемая (внешняя) территория, охраняемая территория, охраняемое здание, помещение, место дислокации цели нарушителя;
- элементы защиты – основные элементы, составляющие систему физической защиты, например, ограждение, стена здания, дверь, окно, контрольно-пропускной пункт и др.
- слои защиты – совокупности элементов защиты, разделяющие зоны защиты объекта;

Каждый элемент защиты описывается двумя основными характеристиками:

- продолжительность задержки действий нарушителя;
- вероятность обнаружения нарушителя. Последовательности элементов защиты, преодолевая которые,
- нарушитель может проникнуть к цели, называются маршрутом движения нарушителя.

Интерфейс программы Facility позволяет пользователю в удобном и наглядном виде создавать графическое описание объекта защиты. При этом один файл описания соответствует одной цели нарушителя. Если на объекте имеется несколько различных целей,

расположенных в разных зонах защиты, необходимо для каждой из них создавать свой файл описания.

Программа Facility позволяет одновременно описывать объект защиты в двух состояниях: рабочее и нерабочее время. Эти состояния объекта могут отличаться между собой. Например, транспортный контрольно-пропускной пункт в нерабочее время может быть закрыт и работать только как участок охраняемого периметра.

Для ввода характеристик элементов защиты в программу ASSESS включены базы данных по вероятностям (обнаружения нарушителя и временам задержки его действий. При этом данные вводятся для различных способов преодоления элемента физической защиты, например:

- без оборудования;
- с ручными инструментами;
- с инструментами с приводом (специальные инструменты);
- с помощью взрывчатых веществ;
- с помощью автотранспорта (там, где это возможно).

Каждый элемент защиты может включать в себя до трех различных элементов обнаружения и физических барьеров, – имеющих различные характеристики. Кроме того, при описании элемента защиты определяется наличие или отсутствие на нем специальных средств обнаружения запрещённых к проносу материалов и предметов, наличие или отсутствие часовых сил охраны, вводятся их характеристики.

Программа позволяет указывать, какие зоны защиты могут преодолеваться нарушителем на автотранспорте, а какие – нет.

Перед проведением оценки необходимо определить модель нарушителя, для которой будет выполнена оценка. Для этого необходимо задать угрозу, определить стратегию нарушителя, методы его действий.

В результате оценки программа определит так называемый критический маршрут нарушителя, т. е. маршрут на котором эффективность системы физической защиты минимальна, и выделит его на экране красным светом. В текстовой части окна отобразится информация о численном значении показателя эффективности, резерве времени сил реагирования.

Программа позволяет проводить оценку эффективности по десяти различным наихудшим, с точки зрения задач охраны, маршрутам нарушителя, и для десяти различных времен реагирования сил охраны в заданном интервале времени.

Перед проведением оценки эффективности СФЗ при внутренней угрозе необходимо определить список внутренних нарушителей, лиц имеющих допуск в различные охраняемые зоны объекта, а также определить их полномочия. Перечень полномочий определяет, в какие зоны

охраны допущен внутренний нарушитель, каким процедурам досмотра он подвергается при проходе и т. д.

В результате проводимой оценки эффективности программа рассчитывает вероятности обнаружения системой физической защиты каждого типа внутренних нарушителей как на пути движения к цели, так и на пути ухода с объекта.

Программа Neutralization не имеет жесткой «привязки» к модулю описания объекта и запускается из программы-менеджера выбором соответствующего приложения в меню.

Программа Neutralization позволяет оценивать вероятность победы сил охраны при боестолкновении с нарушителем.

Перед проведением непосредственных расчетов задаются численность сил охраны (реагирования) и нарушителя, временные интервалы, в течение которых к силам охраны может прибыть подкрепление. Кроме того, для каждого бойца задаются такие основные характеристики, как:

- вид оружия;
- расстояние между противоборствующими сторонами;
- уровни защиты при ведении огня и перезарядке оружия и др. Кроме значения вероятности нейтрализации нарушителя модуль позволяет оценить ожидаемое время боя, количество выживших и погибших с обеих сторонка также исследовать чувствительность рассчитанного значения вероятности нейтрализации к изменению характеристик нарушителей и сил охраны.

Российская компьютерная программ ВЕГА-2 разработана как программный комплекс, объединяющий в себе ряд программ-модулей, таких как:

1. Модуль описания объекта.
2. Расчетный модуль.
3. Модуль формирования отчета.
4. Автоматизированные базы данных по средствам обнаружения, физическим барьерам, моделям нарушителей.

Программа ВЕГА-2 является WINDOWS-приложением.

Работа с программой начинается с запуска модуля описания объекта. В результате работы с модулем разрабатывается формализованное описание объекта с точки зрения его физической защиты, включающее в себя:

- зоны защиты – какие-либо части территории объекта, например, не охраняемая (внешняя) территория, защищенная внутренняя и особо важная зоны;
- секции – элементы формализованного описания ЯОО, представляющие локализованные части объекта, отделенные от других частей

рубежами ФЗ. Секциями описываются территория ЯОО, локальные зоны, помещения (группы помещений и т. д.);

- цели нарушителя – элементы формализованного описания ЯОО, представляющие уязвимые места объекта или предметы физической защиты;
- переходы – элементы формализованного описания ЯОО, представляющие вероятные каналы проникновения нарушителя, например, дверь, окно, стена и др.;

Каждый переход является элементом вероятного маршрута движения нарушителя и описывается двумя основными характеристиками: временем преодоления и вероятностью обнаружения нарушителя. Для удобства описания переходов в составе программы ВЕГА-2 разработаны специальные шаблоны описания типовых переходов, позволяющие пользователю в удобном и наглядном виде вводить необходимые для расчетов исходные данные.

К модулю описания объекта подключены автоматизированные справочники по средствам обнаружения и временам преодоления физических барьеров, а также специализированные расчетные процедуры для оценки времен разрушения для отдельных типов физических барьеров.

В отличие от программы ASSESS файл описания объекта программы ВЕГА-2 описывает все цели нарушителя, находящиеся на объекте.

После завершения описания объекта хотя бы одной цели можно приступать к проведению оценки эффективности СФЗ. Для этого необходимо выбрать опцию «расчетный модуль».

Расчетный модуль объединяет в себе расчетные процедуры, как для внешней, так и для внутренней угрозы. При внешней угрозе имеется возможность проведения расчетов для диверсионной акции и акции хищения ядерных материалов. При этом возможно провести оценку аналитическим методом или с помощью имитационного моделирования.

Для проведения оценки эффективности при внешней угрозе необходимо инициализировать расчетный модуль, задав модель вероятного нарушителя. Для этого в модуль встроена автоматизированная база данных моделей нарушителя.

Программный модуль позволяет проводить оценку эффективности СФЗ для:

- конкретной цели нарушителя;
- группы целей, относящихся к одной категории важности;
- объекта в целом.

Результатом оценки эффективности является вероятность пресечения действий нарушителя силами реагирования, рассчитанная для

наихудшей, с точки зрения охраны, ситуации. При этом расчетный модуль отражает критический маршрут нарушителя, которому соответствует оценка.

Основным отличием программы ВЕГА-2 от программы ASSESS является то, что при оценке эффективности при внутренней угрозе предполагается, что внутренний нарушитель может перейти к силовым действиям для проникновения в зону охраны, секцию или к цели, если он не имеет права легального доступа к ним. При этом учитывается наличие или отсутствие на контрольно-пропускных пунктах специальных средств обнаружения, запрещенных к проносу материалов и предметов (оружие, ядерные материалы, взрывчатые вещества), а также наличие или отсутствие этих материалов и предметов у нарушителя. Таким образом, программа оценки эффективности при внутренней угрозе оценивает:

- вероятность обнаружения внутреннего нарушителя при попытке вноса им в разрешенную зону или секцию запрещенных материалов и предметов, используя каналы легального прохода;
- вероятность пресечения силовых действий внутреннего нарушителя, в зависимости от его оснащения;
- итоговый показатель эффективности при внутренней угрозе для каждого типа нарушителя с учетом комбинации скрытных и силовых действий, в зависимости от его оснащения.

Модуль формирования отчетов автоматически формирует отчет о результатах оценки эффективности при внешней и внутренней угрозах для выбранной цели нарушителя. При необходимости отчет может быть распечатан.

1.10. Список литературы

1. Глебов В.Б., Измайлов А.В., Румянцев А.Н. Введение в системы учета, контроля и физической защиты ядерных материалов. – М.: МИФИ, 2001.
2. Терминологический словарь по учету, контролю и физической защите ядерных материалов. – М.: ЦНИИатоминформ, 2000.
3. Закон Российской Федерации об использовании атомной энергии. Принят 21 октября 1995.
4. Правила физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов. Утверждены постановлением Правительства РФ от 7 марта 1997 г. № 264.
5. Инструкция о порядке разработки, согласования, утверждения и составе проектной документации на строительство предприятий, зданий и сооружений. СНиП 11-01-95, Минстрой России. – М., 1995.

6. Системы физической защиты ЯМ и У. Инструкция по организации проектирования. Минатом РФ. РД95 10544-99.
7. Системы физической защиты ЯОО. Общие требования (проект), Минатом РФ, 2001.
8. Системы физической защиты ЯОО. Методические рекомендации по анализу уязвимости ЯОО (проект). Минатом РФ, 2001.
9. Системы физической защиты ЯОО. Методические рекомендации по оценке эффективности. Минатом РФ (проект), 2001.
10. Системы физической защиты ЯОО. Требования к проектным решениям. Минатом РФ (проект), 2001.
11. Измайлов А.В., Гран Т., Григгс Дж. и др. Разработка нормативных документов для Минатома России по физической защите ЯМ и У в рамках Программы MPC&A // Труды 42-й Ежегодной конференции Института по обращению с ядерными материалами (INMM). – г. Индиан Уэллс, США, 2001.
12. Описание компьютерной программы SAVI. SandiaNL, США, 1990.
13. Описание компьютерной программы ASSESS. Материалы тренинг-курса по обучению пользованию программой. LLNL, США, 1995.
14. Описание компьютерной программы «Вега-2», ГУП СНПО «Элерон», Минатом России, 1999.
15. Подиновский В.В. Оптимизация систем по последовательно применяемым критериям. – М.: Радио и связь, 1985.

2. КРИТЕРИИ БЕЗОПАСНОСТИ, ОЦЕНКА ЭФФЕКТИВНОСТИ И РИСКА ПРИ ПРОЕКТИРОВАНИИ СФЗ ЯДЕРНЫХ МАТЕРИАЛОВ И УСТАНОВОК

2.1. Задачи обоснования надежности, безопасности и оценки эффективности в СФЗ

Данная глава посвящена вопросам системного анализа эффективности, безопасности и надежности систем физической защиты и ядерно-опасных объектов (установок). Задача оценки эффективности трактуется как оптимизационная задача с ограничениями.

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 не тривиальность 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 создание 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 познакомиться 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 познакомиться 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.* Что 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.

2.2. 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 не превышение 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 последствиями. Для каждого вида деятельности риск специфичен, так же как и меры по его уменьшению. Особенностью объектов ядерной энергетики (ЯЭ) является существования 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:

$$R_i = p_i S_i, \tag{2.1}$$

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:

$$\vec{R} = \sum_{i=1}^{N} R_i = \sum_{i=1}^{N} p_i \vec{S_i}, \tag{2.1}$$

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 $R^{доп}$?

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

$$R \le R^{доп}. \qquad (2.3)$$

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 осознано или не осознано 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 относится 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.

2.3. 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. Так как оценка риска в виде (2.2) и решение задачи (2.3) 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 (2.3) 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), предложенном *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 качестве 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: общество

всегда располагает ограниченным потенциалом средств. Что 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. 2.1 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.

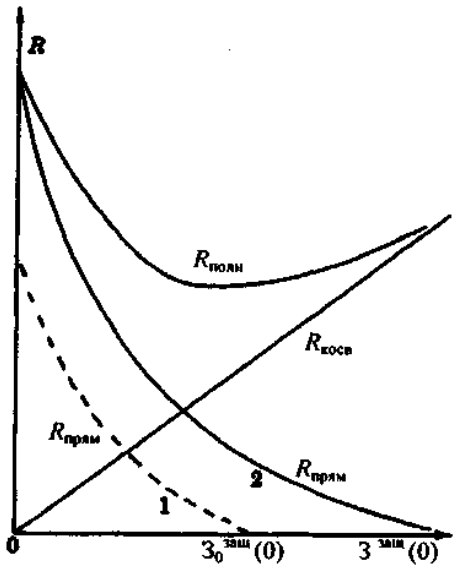


Рис. 2.1. Зависимость риска от затрат на защиту

Поскольку совершенно безопасных технологий нет вообще, следует учесть, что помимо прямого риска (кривые 1 и 2 на рис. 2.1) 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:

$$R = R_{прям} + R_{косв}.$$

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 этот случай 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. 2.1).

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 приведенный

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.

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. $Э(0)$ = const и $З^{осн}(0)$ = 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. 2.2).

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

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

где $Э^{защ}(0) = У(0)_{R_{НАЧ}} + У(0)_{R_{ДОСТИГНУТОЕ}}$; $R_{НАЧ}$ и $R_{ДОСТИГНУТОЕ}$ – риски до и после принятия данной меры защиты.

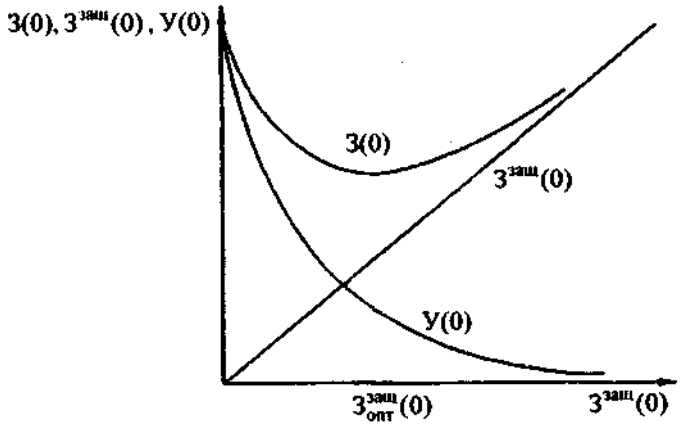


Рис. 2.2. Зависимость обобщенных приведенных затрат от затрат на защиту

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

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, вовлекаемым 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. 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. 2.3 изображены *1* – кривые постоянного уровня жизни, поэтому они идут не горизонтально, а наклонно; *2* – кривая экономических 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.

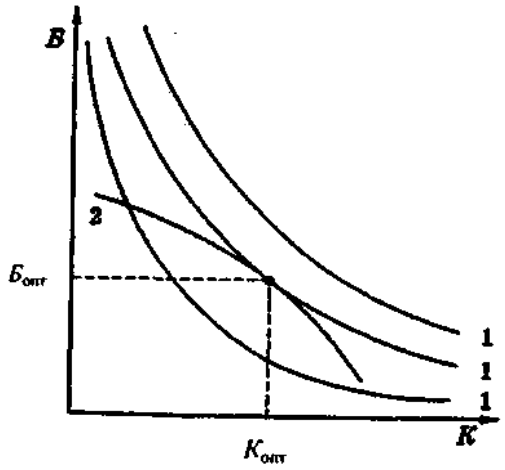


Рис. 2.3. Безопасность и качество жизни

Есть возможность получить и субъективную цену риска. Наибольшую информацию тут могут дать результаты статистических исследо-

ваний 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.

2.4. Основные понятия и методы теории надежности

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 обладает 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. Иногда 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.

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:
$f(x_1, x_2, ..., x_i, ..., x_n)$ или n – мерного вектора $\{x_i\}$, 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 Θ:

$$R(t) = 1 - F(T);\ \ \lambda(t) = \frac{f(t)}{1 - F(t)}, \tag{3.1}$$

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

$$\overline{\Theta} = \int_0^\infty t \cdot f(t)dt = \int_0^\infty R(t)dt.$$

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

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

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 0, т. е. среднее число отказов за время работы элемента.

Метод дискретных Марковских процессов наиболее эффективен, когда число элементов, включенных в структурную схему, относительно 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 плановопредупредительных 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.

2.5. 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. 2.4, легко выделить семь КГЭ, образующих полный набор для рассматриваемого отказа ЯЭУ.

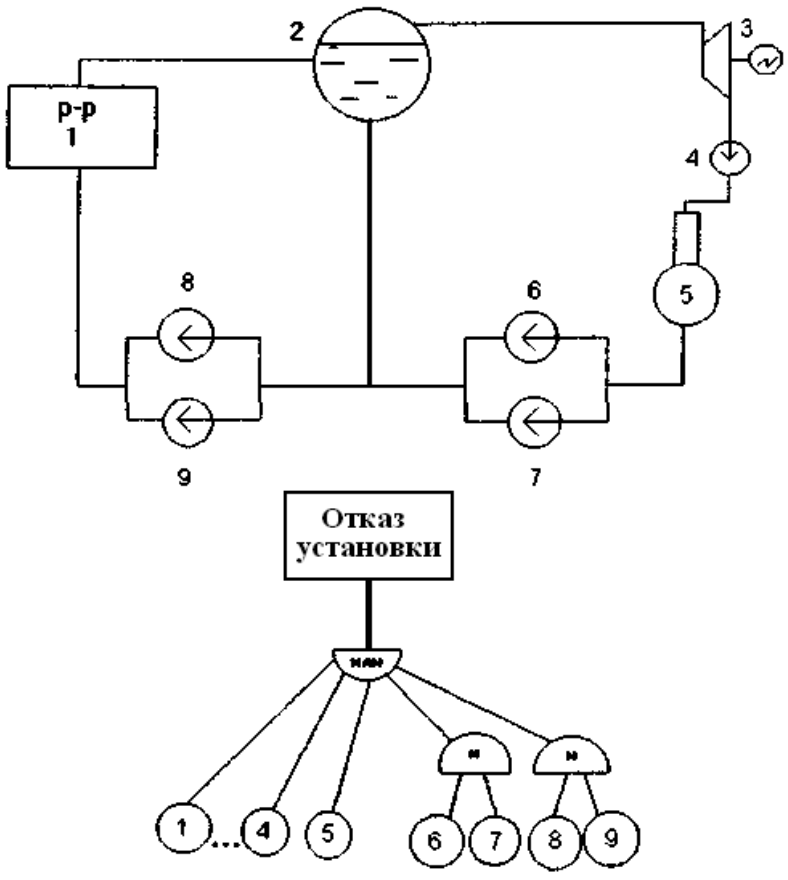


Рис. 2.4. Пример построения дерева отказов для ЯЭУ. Элементы установки: 1 – реактор; 2 – сепаратор; 3 – турбоагрегат; 4 – конденсатный насос; 5 – деаэратор; 6–9 – питательные насосы (основные и резервные)

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. 2.5).

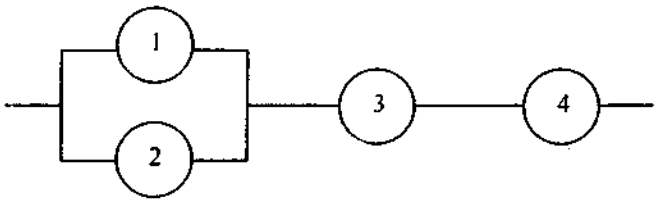


Рис. 2.5. Параллельное и последовательное включение элементов

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 «И» для последовательного способа включения, обозначающие соответственно сумму событий, и операторы «ИЛИ», обозначающие, соответственно, произведение событий отказов рассматриваемых элементов.

Для простых деревьев отказов (содержащих относительно малое количество элементов и логических операторов) выбор минимального 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.

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

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	$2\cdot10^{-1}$ $4\cdot10^{-2}$
Разрыв корпуса реактора	$\le10^{-6}$
Падение самолёта	$\le10^{-6}$
Максимальное расчётное землетрясение	10^{-4}
Пожар	10^{-1}

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 / 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

$$R(t)=\prod_i R_i(t),$$

а в случае экспоненциального закона получим

$$\lambda(t)=\sum_i \lambda_i(t). \qquad (4.3)$$

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

$$F(t)=\prod_i F_i(t) \text{ или } R(t)=1-\prod_i (1-R_i(t)). \qquad (4.4)$$

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 $F(t) = 1 - \exp(-\lambda t)$. 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:

равнительный анализ технических решений и исследования чувствительности результатов в изменениях 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;
- 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 wiu 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″* 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. 2.6.

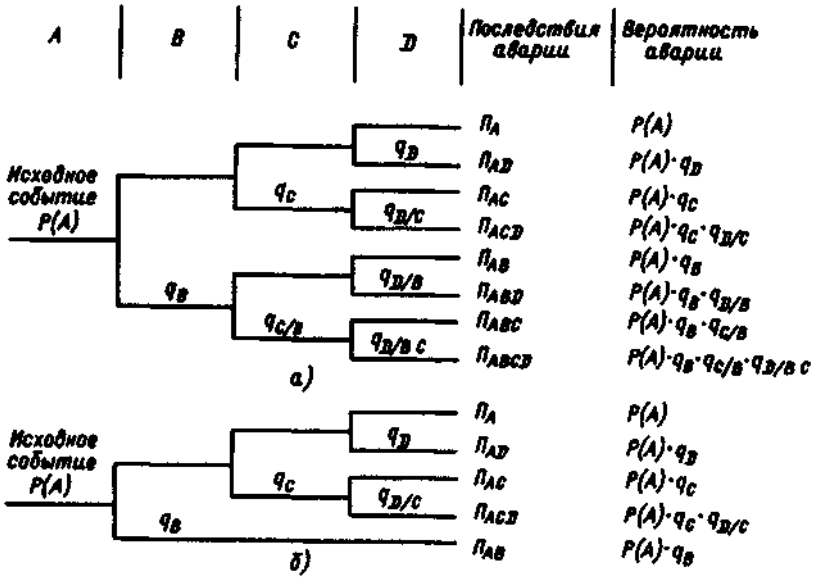


Рис. 2.6. Вид дерева событий

Отметим, что верхние ветви после разветвления соответствуют работоспособному состоянию системы, а нижние – неработоспособному состоянию. На рис. 2.6, *а* – общий случай, а на рис. 2.6, *б* – упрощенное дерево для случая зависимых отказов *(*Исследование по методу ДС является итерационным по своей сути, поскольку предполагает выделение определяющих по последствиям аварийных цепочек и тщательный их повторный анализ.

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.

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 = О, 1, 2, 3, … с вероятностью:

где X – параметр, то говорят, что она распределена по закону Пуассона. Это закон редких событий, вероятность которых p мала, а число n велико и где имеет смысл интенсивности событий на единичном интервале времени.

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

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 независимо от числа ЯОО в доверительном интервале вероятностей не должны происходить значительные аварии (нежелательные события).* Таким образом, потребуем, чтобы ожидаемая величина числа аварий в переделах одной или более дисперсий не выходила за значение, равное единице.

Или, исходя из (4.5), имеем

$$X + к>/x<\backslash, \qquad (4.6)$$

где *к* – множитель перед среднеквадратическим отклонением, *к*=\, 2, 3,…

Очевидно, что, зная оценку для я, легко из (4.6) найдем искомую оценку вероятности/?. 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 310. Тогда при различных *к* получаем табл.

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

$$i>_m * T^{*0,07} \_ \quad (4\_7)$$

$$i>_m * T^{*0,07} \_ \qquad (4.7)$$

Такое 7%-е 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 КИ совместно с Брукхевенской национальной лабораторией (БЫЛ), 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 переменной. 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 *J{X)* случайной величины *X* с энтропийным коэффициентом $\kappa > 1{,}7$ 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 $\backslash X \sim X_0 \backslash / a(X) = 1{,}6 \pm 0{,}05$, 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:

$$*o{,}05 = *o - Кб \bullet o(X);\ X_{095} = X_0 + 1{,}6 \bullet a(X). \qquad (4.8)$$

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 БЫЛ пакет ВЭСС прошел апробацию и был применен для анализа эффективности усовершенствованных систем УиК и ФЗ центрального хранилища РНЦ КИ. Из-за малости статистики отказов мате-матическое ожидание частоты отказов в основном определялось в соответсвиии 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	
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 храниться 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.

2.6. 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 тоже 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 эффективности СФЗ ЯОО должны быть применены более сложные косвенные методы анализа и оценки. Природа защищаемых ядерно-опасных 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 перехвата (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. 2.7) 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. 2.8, 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

P_0 для данной стратегии рассчитывается из P_D преодоления каждого средства защиты

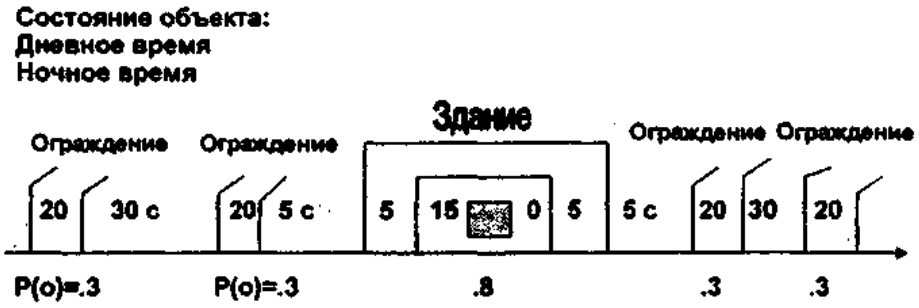


Рис. 2.7. Расчет времени задержки

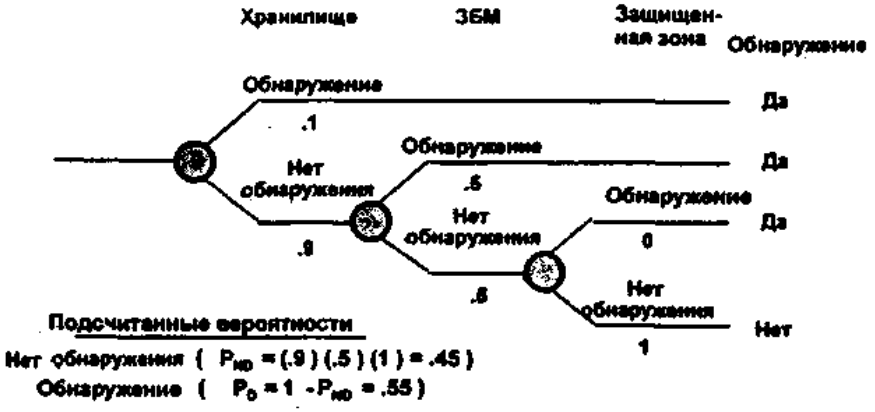


Рис. 2.8. Логическая схема и расчет вероятности обнаружения и перехвата

2. Модель и программа SAVT 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 маршрутов 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. 2.9, 2.10.

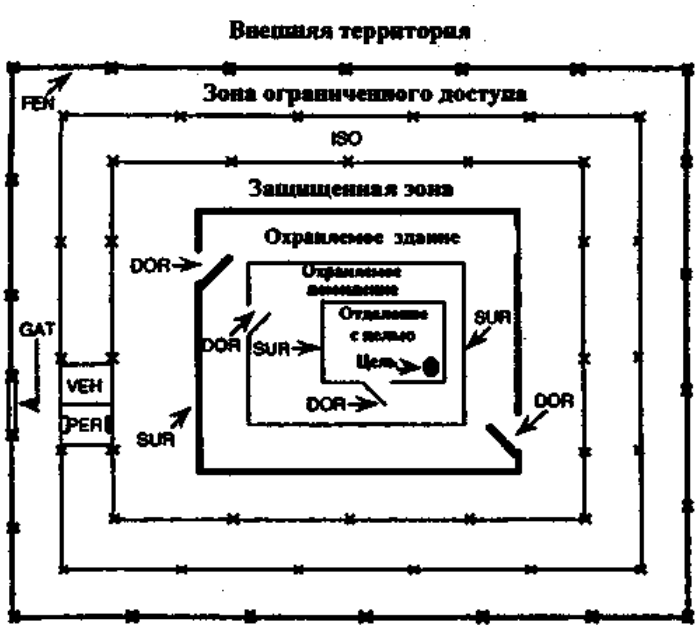


Рис. 2.9. Пример планировки объекта и СФЗ;

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.

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.

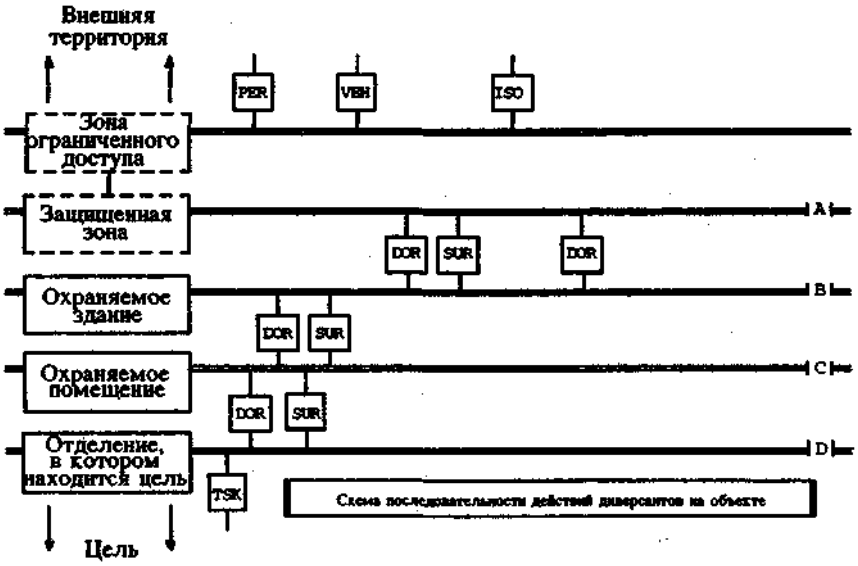


Рис. 2.10. Пример СПДД. построенной с учетом характеристик объекта

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 SAV1. 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].

2.7. 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 формализовать 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.

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 находится 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%-я 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.

Учтем, что количество информации S 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 /),=1/Ми 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 plogp равно нулю лишь при $p = 0$ или $p = 1$, то энтропия опыта принимает минимальное значение 5 = 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 0.5.

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.

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_{cril}, выше которого не допустима эксплуатация хранилища, а также алгоритм определения вероятностей 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_t, характеризующий вероятность нахождения рассматриваемой УЕ в бездефектном состоянии. Значение /?, вводится в момент постановки УЕ на учет и изменяется в соответствии с характером работ в помещениях хранилища, режимом и условиями хранения УЕ.

Значение /?,, 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 />,.

Будем считать, что вероятность *p,(1)* УЕ с номером / находится в момент / в бездефектном состоянии и определяется произведением трех сомножителей, каждый из которых имеет смысл парциальной вероятности независимого события:

$$p,(1) = pГ''(0pГ(0p^(0, (б.з)$$

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

Для описания парциальных вероятностей *pf''*, *pf*''*, *p*™ должны использоваться модельные зависимости, содержащие *феноменологические параметры.* Так, зависимость от времени величины *pf* логично принять в виде

$$pP^{d}(_{t}) = l^{l}\sim^{bt} \text{ при } 0</<0,5//>;$$

$$|0,5;/> 0,5/6 \text{ при}/>0,5//>.$$

В этом соотношении сделано предположение о линейном характере вероятности *pf* 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/Ь* имеет достаточно большое значение. Разумеется, можно выбрать и другой вид модельной зависимости *pf* (/). Можно предложить и ряд зависимостей для двух других парциальных вероятностей входящих в (6.3). Следует только заметить, что вероятность />/*г(/) зависит от времени неявно, через количество рабочих дней, когда хранилище с ЯМ посещал персонал после последней проверки. А вероятность p_{f}^{as} 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,* 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_t 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_{oul} и по ней, наконец, определяются апостериорные вероятности p^* для УЕ, не попавшие в число проверяемых.

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

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

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

$$Sin = -X\{AlogA+D-/>>g[l-Al\ (^{6}\_^{4})$$

$$/=1$$

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

$$S_{in}=-N\{p\backslash ogp+[\backslash -p]\backslash ol\backslash -n. \quad (6.5)$$

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

$W(N,D,n,d) = –(p)^{\{N\_D)}(\backslash -p)^{D\backslash N}]w(N,D,n,ci),$ где $w(N,D,n,d)$ – функция гипергеометрического распределения.

$$(DVN-D\hat{}\ w(N,D,n,d)\hat{}P(X = d) = \hat{}^{d}\hat{}''_{N}\sim^{d} K$$

$$\boldsymbol{y'')}$$

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

$$(N –_{n}\backslash^{N}\text{-}''^{r+d}\ \backslash fNY^{d}\ I$$

$$^{S}\hat{}=-[-jr)\ \text{I»4\^{}A*.rf)logW J}\ W\{N,D,n,d)V \quad (6.6)$$

Вероятность после проверки $p\backslash$ для УЕ, принадлежащих проверяемой подсистеме, но не попавших в число проверяемых, находится согласно следующему алгоритму.

По результатам выборочной проверки присваиваются новые значения *p*\ всем элементам подсистемы и определяется новое значение энтропии S^+ всей системы УЕ. Если значение S^+ меньше допустимого S_0 = *Sent,* то наши знания о системе находятся на приемлемом уровне.

Качественно зависимость информационной энтропии от времени показана на рис. 2.11. За начало отсчета принят произвольный момент времени.

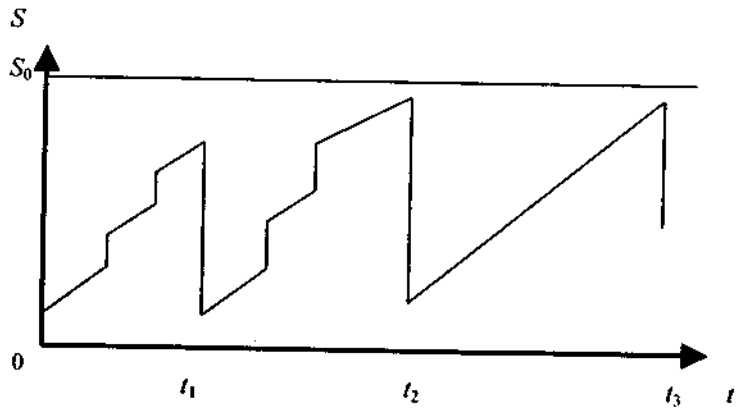


Рис. 2.11. Зависимость информационной энтропии от времени

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*\, /2» *h* на рис. 2.11). Продолжительность между контрольными проверками может быть различной в зависимости от интенсивности работ в хранилище и объема предыдущей выборочной проверки. Третий участок времени ($/_2$ – /з) соответствует отсутствию работ в хранилище, когда изменение энтропии определяется только эффективностью СФЗ.

2.8. Оценка эффективности как оптимизационная задача. Методы оптимизации, применяемые при анализе безопасности и эффективности

Из вышесеазанного 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, направляемых на решение задачи, то фактически приходим к необходимости найти решение *оптимизационной задачи с ограничениями.* Например, зада-

чи (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 управления.

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 *u*, который доставляет наилучшее (минимальное или максимальное) значение критерию оптимальности $F_0(u)$ при выполнении ограничений задачи:

найти такие *ŭ*, при которых: min/b(5),

$$F,(u)<Fr,$$

где /*)^{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:

где *ajj*, *bi*, *Cj* – заданные постоянные величины и *к* <*m.*

Из вида задачи ясно, что целевая функция и ограничения представляют из себя линейные формы относительно неизвестных управлений *х.*

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 $к = 0$ и $/ = n$. Совокупность чисел (управлений) $X = (x_ь x_2,.-,x_n)$, удовлетворяющих ограничением задачи (7.2)-(7.4), называется допустимым решением (или *планом).* Можно показать [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, рассматривае-

мые в данном пособии, – линейные задачи вряд ли возможны вообще. Среди задач нелинейного программирования наиболее 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 *ueU* 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.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 последователь-

ном 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 *Fo(u),* должна быть тем проще, чем уже допустимая область изменения аргумента *и.* 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 получиться, 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 е S_0 и является управляемой. Благодаря осуществлению некоторого управления *U система переходит из начального состояния* 5_0 в конечное состояние Sy_m. 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(JJ)* 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 дг, руб. для каждого /-го мероприятия обеспечит прирост защищенности, определяемый значением нелинейной функции */fa).*

Математическая постановка задачи состоит в определении наибольшего значения функции.

Сформулированная задача является задачей нелинейного программирования. В том случае, когда известно, что /(*;) – выпуклые функции, ее решение можно найти, например, методом множителей Лагранжа. Если же функции /(я,) не являются таковыми, то

известные методы не позволяют определить глобальный максимум 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 *к* мероприятиях *(к* = 1, …, /?).

Решения об объемах капиталовложений, выделяемых для *k-vo* 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 *к-м* шаге определяется выбранным управлением на данном шаге и состоянием системы в *к-1* шаге и не зависит от того, каким образом система пришла в *к*-\ состояние.

Далее будем считать, что если в результате реализации А>го шага обеспечен определенный выигрыш или доход, также зависящий от исходного состояния системы в начале шага *(к*-\ состояние) и от выбранного управления $u_к$ и равный $W_k(X \sim \backslash u_к)$, то общий выигрыш за *n* шагов составляет:

$$F = J\, W_k\{X^{(k}\text{-}^{\{}\backslash u_k). \qquad (7.7)$$

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 *п-м* шаге, затем на двух последних *п-м,* (и-1)-м и т. д. вплоть до первого шага.

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

$$F_n\{X^{<)})^{\wedge}m_{\alpha}x[W_x\{X\backslash u_x) + \ldots + W_i(_{<}X^{(n\_x}\backslash u_n)), \qquad (7.8)$$

$$F_{n\_k}(X^{(k)}) = {}_m ax[W_{k+l}(X^{(k)},u_{k+i}) + \ldots + F_M(X^{\{k+J\})}l$$

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 $к = n - 1$ 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 результате последовательного прохождения всех этапов от конца к началу определяем максимальное значение выигрыша за *п* 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.

2.9. 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: 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 9_y е{Э},у'-й – набор исходных

параметров с известными вероятностными характеристиками, тогда задача запишется в виде:

найти такие и, при которых $\min F_0(M,\S)$,

Тогда, зная вероятностные характеристики реализации того или иного Э, 6 {9} 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 $\&_y$е{9}, 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 измененными допустимыми значениями ограничений и решать ее относительно математического ожидания критерия $F_0(H)$:

найти такие u, при которых $\min M\{F_0(u)\}$,

где *Qj* – рассчитанные запасы на выполнение соответствующих ограничений, которые находятся из вероятностных условий типа:
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 линеаризации (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 / = 1, 2, …, / и множество возможных исходов, однозначно определяющих так называемые состояния природы у' = 1, 2, …, *S.* Состояние природы у – это просто /-сочетание исходных данных или некоторых внешних условий, влияющих на решение. Пусть существует функция, характеризующая потери, убытки или *затраты/у* = 3,у, которые связаны с действием *i* при исходе (сочетании условий, состоянии природы)/ В общем случае */у* – функция цели, тогда числа/у = 3,у можно представить в виде матрицы размерностью *l*S,* называемой *платежной матрицей.*

Очевидно, что истинное состояние природы *j* нам неизвестно. Тогда требуется найти такое действие /', т. е. выбрать такую строку матрицы {/„}, которое в некотором смысле явно лучше других.

Если известны такие вероятности p_t, …, p_s состояний природы, при которых ^*p,*I = 1, то имеет место задача выбора решений при риске. При этом часто отдается предпочтение действию, которое *s* минимизи-

рует средние затраты Это простая задача стохаотического 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/ легко получить значения диагонали матрицы и полный набор *Uj* (действий /);
- заполнить матрицу, рассчитав значение^ = 3,у для каждого случая, произвести дополнительные расчеты и получить значения средних характеристик 3 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 и,. Таков, вкратце, алгоритм метода платежной матрицы. Прежде чем обсудить применяемые минимаксные критерии, сделаем небольшое отступление.

Выбор был бы очевиден, если бы существовала такая строка *к,* при которой для каждого у = 1,2, …, *S* было бы справедливо неравенство f_{kj} *и/у.* В том случае, когда такой строки нет, говорят об оптимальности по Парето: действие /' *оптимально по Парето,* если не существует такого *к* * /, при котором $f_{kj} < fy$.

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 минимаксные 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 критерий тут очевидно.

Значения *Зу,* записанные в /-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 *Зу* 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 *Зу* (наихудшее, что может дать выбор данного варианта);
2) минимальные затраты $З_{i}^{min}$ =min3,у (очевидно, что это наи-

Обычно при анализе платежной матрице 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

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:

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

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:

$$\min[a3_{;}^{max}+(l-a)3,^{min}],$$

где а – показатель «пессимизма – оптимизма» (0 < а < 1).

При а = 1 критерий Гурвица превращается в критерий Вальда, а при а = 0 – в критерий «крайнего оптимизма» (миниминный), выбор по которому предполагает наилучшее стечение обстоятельств, что явно неразумно. При 0 < а S 1 получается нечто среднее, и в этом привлекательность критерия Гурвица. Очевидный его недостаток в том, что параметр **а** должен выбирать сам исследователь, поэтому он не может объективно выявить наилучший вариант и снять неопределенность выбора. Интуитивно представляется, что значения а 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. Мно-

гое здесь зависит от знания особенностей задачи, глубины проникновения в ее суть, искусства и изобретательности исследователя.

2.10. 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, не превышение доз облучения на станциях и выбросов радиоактивных веществ за пределы станции 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 на может быть уменьшена до нуля, должны быть приняты меры, гарантирующие, что последствия любой радиационно-опасной 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 радиоактивность которых может достигать величины 310^{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 тепло-отвода. 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 А3, 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 теплоот-вода,* 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 радиоак-

тивных 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 обеспе-

чить 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 приемлемого 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 ана-

лиза 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 мо^ дели 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, с изучения деревьев 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.

2.11. 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.

ПРИЛОЖЕНИЕ

Положение об общих требованиях к системам физической защиты ядерно-опасных объектов Минатома России

(выдержки)

1. Общие положения

1.1. Настоящее «Положение об общих требованиях к системам физической защиты ядерно-опасных объектов Минатома России» (далее – Общие требования) является отраслевым нормативным документом, определяющим порядок организации работ по физической защите ЯМ, ЯУ и ПХ ЯМ (далее для краткости – физическая защита) в Минатоме России и общие функциональные требования к СФЗ, их структурным компонентам и элементам.

1.2. Общие требования разработаны в соответствии с:

- Федеральным законом «Об использовании атомной энергии» [1], а также другими федеральными законами, регламентирующими вопросы безопасности и охраны объектов, защиты информации, сертификации продукции и услуг [2–5];
- «Правилами физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов» [6], утвержденными постановлением Правительства Российской Федерации от 07.03.97 № 264;
- Положением о Министерстве Российской Федерации по атомной энергии [7], утвержденным постановлением Правительства Российской Федерации от 05.04.97 № 392,

с учетом международных обязательств, вытекающих из Конвенции о физической защите ядерного материала, а также другими нормативными правовыми актами в области физической защиты.

1.3. Настоящий документ устанавливает:

- порядок организации и обеспечения работ по физической защите на отраслевом уровне;
- перечень направлений нормотворческой деятельности по физической защите отраслевого уровня;
- состав основных нормативных документов по физической защите объектового уровня;
- цели, задачи и принципы построения СФЗ;
- критерии и порядок категорирования ЯОО и предметов физической защиты;

- порядок проведения анализа уязвимости ЯОО;
- структуру СФЗ;
- функциональные требования к структурным компонентам и элементам ИТСФЗ;
- общие требования к оснащению охраняемых зон ИТСФЗ;
- требования к созданию и совершенствованию СФЗ;
- требования к планированию и организации функционирования СФЗ;
- требования к организации эксплуатации ИТСФЗ;
- требования к обеспечению физической защиты при транспортировке ЯМ;
- требования к организации и проведению учений по проверке и отработке взаимодействия в рамках СФЗ;
- требования к персоналу СФЗ, его обучению и повышению квалификации.

1.4. Настоящий документ конкретизирует требования и положения «Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов» [6] (далее – Правила) применительно к организации работ по физической защите в Минатоме России, к СФЗ ЯОО, их структурным компонентам и элементам.

1.5. Требования к СФЗ конкретных ЯОО, их структурным компонентам и элементам определяются на основании Общих требований с учетом результатов анализа уязвимости ЯОО, категории и особенностей функционирования конкретных ЯОО, оценки эффективности СФЗ и предъявляются при создании, функционировании и совершенствовании СФЗ.

Требования к количественным характеристикам ИТСФЗ предъявляются в нормативной документации по стандартизации федерального или отраслевого уровня.

1.6. Общие требования предназначены для использования администрацией и персоналом службы безопасности ЯОО, в том числе ведомственной охраны, а также других организаций отрасли, осуществляющих деятельность в области физической защиты при:

- организации работ по физической защите;
- создании и совершенствовании СФЗ;
- обеспечении функционирования СФЗ;
- осуществлении контроля соответствия СФЗ установленным требованиям.

1.7. Требования настоящего документа распространяются на СФЗ ЯОО Минатома России, а также на обеспечение физической защиты ЯМ и изделий на их основе при транспортировке.

Общие требования не распространяются на обеспечение физической защиты транспортных ядерных установок, выполняющих свои основные функции в процессе передвижения.

1.8. На основании требований и положений настоящего документа разрабатывается новая или уточняется действующая нормативная документация по физической защите отраслевого и объектового уровней.

1.9. Ответственность за обеспечение физической защиты ЯОО несет его руководитель [6].

2. Функции Минатома России по организации и обеспечению физической защиты

2.1. В соответствии с Положением о Минатоме России [7] одной из основных его задач как федерального органа исполнительной власти, осуществляющего государственное управление использованием атомной энергии, является обеспечение физической защиты на предприятиях и в организациях ядерного комплекса.

В целях решения задач физической защиты Минатом России выполняет следующие основные функции:

- обеспечивает в пределах своей компетенции выполнение международных обязательств, вытекающих из Конвенции о физической защите ядерного материала;
- организует и координирует работу по физической защите на предприятиях и в организациях ядерного комплекса;
- организует совместно с другими федеральными органами исполнительной власти транспортировку ЯМ и обеспечивает их физическую защиту;
- разрабатывает федеральные и отраслевые нормативные правовые акты по вопросам обеспечения физической защиты;
- принимает решение о признании подведомственных ядерноопасных объектов пригодными эксплуатировать ЯУ или ПХ ЯМ и осуществлять собственными силами или с привлечением других организаций деятельность по проектированию, сооружению, эксплуатации и выводу из эксплуатации ЯУ или ПХ ЯМ, а также деятельность по обращению с ЯМ;
- разрабатывает отраслевые и межотраслевые научно-технические программы, обеспечивает разработку федеральных целевых программ в области атомной науки и техники, в которых, в том числе, предусматриваются вопросы обеспечения физической защиты;
- осуществляет за счет централизованных средств финансирование научно-исследовательских и опытно-конструкторских работ,

выполняемых в целях повышения безопасности функционирования ЯОО, в том числе, обеспечения их физической защиты;

- организует и проводит работы по сертификации технических средств, используемых в СФЗ;
- участвует в установленном порядке в выдаче лицензий на осуществление видов деятельности в области использования атомной энергии;
- осуществляет контроль за организацией и состоянием физической защиты на подведомственных ЯОО.

В составе центрального аппарата Минатома России функционируют структурные подразделения, участвующие в обеспечении физической защиты как на отраслевом уровне в целом, так и на подведомственных ЯОО.

К ним относятся:

- Департамент защиты информации, ядерных материалов и объектов;
- Отдел ведомственной охраны;
- Департамент отраслевой экономики и планирования;
- Департамент сооружения атомных объектов;
- Транспортное управление;
- департаменты, которым подчиняются ЯОО.

Непосредственно в организации и обеспечении физической защиты принимают участие эксплуатирующие организации и ядерно-опасные объекты.

2.2. Департамент защиты информации, ядерных материалов и объектов является основным структурным подразделением Минатома России, осуществляющим координацию и организационно-методическое руководство работами по физической защите [8].

В этой части Департамент защиты информации, ядерных материалов и объектов:

- организует разработку и утверждение в установленном порядке нормативных и методических документов по вопросам обеспечения физической защиты;
- обеспечивает взаимодействие с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации и организациями по вопросам обеспечения физической защиты;
- организует и координирует научно-исследовательские и опытно-конструкторские работы, выполняемые предприятиями и организациями отрасли по вопросам обеспечения физической защиты;

- организует совместно с Транспортным управлением и другими федеральными органами исполнительной власти транспортировку ЯМ и специальных грузов и их охрану при транспортировке;
- участвует в организации работ по сертификации технических средств физической защиты (ТСФЗ) и приеме в эксплуатацию СФЗ, применяемых на ЯОО Минатома России;
- участвует в организации, координации и контроле международного научно-технического сотрудничества в области физической защиты;
- организует и осуществляет ведомственный контроль за обеспечением физической защиты.

Указанные функции Департамент защиты информации, ядерных материалов и объектов выполняет во взаимодействии с Управлением ведомственной охраны, Департаментом отраслевой экономики и планирования, Департаментом сооружения атомных объектов, Транспортным управлением, департаментами, которым подчиняются ЯОО, и эксплуатирующими организациями, а также с Департаментом международных и внешнеэкономических связей (в части организации, координации и контроля международного научно-технического сотрудничества).

Управление ведомственной охраны осуществляет организационно-методическое руководство ведомственной охраной, контроль за деятельностью подразделений ведомственной охраны по защите охраняемых объектов от противоправных посягательств [9].

Департамент отраслевой экономики и планирования осуществляет организационно-методическое руководство и координацию работ по формированию и реализации федеральных целевых программ, предусмотренных к финансированию за счет федерального бюджета, а также проводит работу по формированию и использованию централизованных средств и внебюджетных фондов на финансирование научно-исследовательских и опытно-конструкторских работ, в том числе, выполняемых в целях повышения безопасности функционирования ядерно-опасных производств и объектов, а также их физической защиты [10].

Департаменты по подчиненности ядерно-опасных объектов и эксплуатирующие организации организуют и обеспечивают осуществление физической защиты на подведомственных ЯОО.

2.3. Источниками финансирования работ по физической защите ядерно-опасных объектов могут быть:

- средства федерального бюджета;
- централизованные средства внебюджетных фондов;
- собственные средства ЯОО;

- средства, получаемые ЯОО в качестве технической помощи за счет международного научно-технического сотрудничества.

Указанные средства могут быть выделены в установленном порядке в рамках федеральных целевых или отраслевых научно-технических программ, капитального строительства (реконструкции) ядерно-опасных производств и объектов, научно-исследовательских, опытно-конструкторских и проектно-изыскательских работ, выполняемых в целях повышения безопасности функционирования ядерно-опасных производств и объектов и повышения эффективности СФЗ.

2.4. Деятельность по созданию и совершенствованию на ЯОО систем физической защиты может являться как составной частью федеральных целевых программ в области использования атомной энергии, так и основным содержанием отраслевых программ [11] по совершенствованию физической защиты, нацеленных на выполнение следующих основных задач:

- поэтапное совершенствование СФЗ ЯОО;
- проведение научных исследований, разработку и производство ТСФЗ;
- разработку и совершенствование нормативных правовых актов и нормативных документов по стандартизации (государственных и отраслевых стандартов, руководящих документов, методик испытаний) по физической защите;
- подготовку, переподготовку и повышение квалификации специалистов в области физической защиты.

Государственным заказчиком федеральных и отраслевых программ является Минатом России [11].

2.5. В целях организации работы по созданию и совершенствованию СФЗ на ядерно-опасных объектах отрасли, выработки единой технической политики в этой области и определения приоритетных направлений научно-исследовательских и опытно-конструкторских работ по созданию новых образцов техники при эффективном использовании финансовых средств при Минатоме России функционирует Экспертный совет по вопросам физической защиты [12]. Деятельность совета определяется положением, утвержденным Министром [13].

2.6. В деятельности по физической защите ядерно-опасных объектов Минатом России взаимодействует с МВД России, ФСБ России, Госатомнадзором России, УГН ЯРБ Минобороны России, другими федеральными органами исполнительной власти [6].

На уровне министерств и ведомств Минатом России:

- согласовывает федеральные, межведомственные и ведомственные нормативные правовые акты по физической защите, затра-

гивающие вопросы, находящиеся в компетенции соответствующих министерств и ведомств;

- согласовывает планы совместных действий и учений по проверке состояния физической защиты ЯОО;
- информирует заинтересованные стороны о планах проведения ведомственного контроля за обеспечением физической защиты ЯОО [14].

Порядок взаимодействия определяется законодательством Российской Федерации и взаимно согласованными нормативными правовыми актами.

На уровне администрации ЯОО вопросы взаимодействия с воинскими частями (подразделениями) внутренних войск МВД России, осуществляющими охрану ЯОО (подразделениями охраны), а также с другими заинтересованными органами управления федеральных органов исполнительной власти (территориальными органами внутренних дел, ФСБ России, межрегиональными территориальными округами Госатомнадзора России, УГН ЯРБ Минобороны России, профессиональными аварийно-спасательными формированиями Министерства Российской Федерации по чрезвычайным ситуациям (МЧС России) на всех этапах создания, функционирования и совершенствования СФЗ в штатном режиме и при чрезвычайных ситуациях на ЯОО определяются «Положением о взаимодействии в системах физической защиты ядерно-опасных объектов» [15].

2.7. В соответствии с федеральным законодательством и Правилами технические средства систем физической защиты подлежат обязательной сертификации в рамках Системы сертификации оборудования, изделий и технологий для ядерных установок, радиационных источников и пунктов хранения [16] (далее – Система сертификации ОИТ).

Цели, принципы, организационная структура и основные правила Системы сертификации ОИТ, порядок взаимодействия между участниками Системы и другими заинтересованными юридическими и физическими лицами, деятельность которых связана с разработкой, изготовлением, испытаниями, использованием и сертификацией ОИТ, включая сертификацию систем качества и производств ОИТ, установлены в основополагающих документах Системы.

В состав утвержденной в Системе номенклатуры продукции, подлежащей обязательной сертификации [17], входят технические средства физической защиты.

Технические и программные средства систем физической защиты, участвующие в обработке информации, составляющей государственную и служебную тайну, подлежат в установленном порядке обязательной сертификации по требованиям безопасности информации.

Созданные и реконструированные СФЗ подлежат обязательной проверке на соответствие требованиям государственных и отраслевых нормативных документов, в том числе аттестации по требованиям безопасности информации и приемке в эксплуатацию в установленном порядке межведомственной комиссией.

2.8. Физическая защита осуществляется в соответствии с требованиями федеральных и отраслевых нормативных правовых актов, разрабатываемых в рамках отраслевых программ и планов работ, а также в рамках международного научно-технического сотрудничества в этой области под организационно-методическим руководством Департамента защиты информации, ядерных материалов и объектов.

Отраслевые нормативные правовые акты разрабатываются в целях конкретизации Правил и иных нормативных правовых актов федерального уровня, настоящего документа и определяют:

- общие угрозы ядерно-опасным объектам;
- общую модель внешнего и внутреннего нарушителей;
- порядок и методику проведения анализа уязвимости ЯОО;
- критерии и порядок категорирования ЯОО и предметов физической защиты (ПФЗ);
- требования к организации разрешительной системы допуска и доступа к ЯМ, ЯУ и ПХ ЯМ, к информации о функционировании СФЗ;
- требования к организации охраны ЯОО, пропускного и внутриобъектового режима;
- порядок создания и совершенствования СФЗ;
- требования к составным частям СФЗ;
- требования к физической защите при транспортировке ЯМ;
- порядок и методику оценки эффективности СФЗ;
- порядок взаимодействия администрации ЯОО с подразделениями охраны, а также с другими заинтересованными органами управления федеральных органов исполнительной власти;
- основные функции, права и обязанности должностных лиц по обеспечению физической защиты;
- требования и рекомендации по управлению в СФЗ;
- порядок функционирования отраслевой системы радиосвязи в интересах физической защиты;
- требования и рекомендации по защите информации в СФЗ;
- требования к службе безопасности ЯОО;
- требования к подразделениям ведомственной охраны;
- требования и рекомендации к персоналу СФЗ, его обучению и повышению квалификации;

- порядок проведения ведомственного контроля за обеспечением физической защиты ЯОО;
- порядок и условия проведения конкурсов (тендеров) на оборудование ЯОО системами физической защиты и на поставку технических и инженерных средств физической защиты;
- требования и методические указания по разработке нормативных документов объектового уровня по физической защите.

2.9. В целях предъявления требований к компонентам и элементам СФЗ разрабатываются и вводятся в действие установленным порядком нормативные документы по стандартизации, в соответствии с требованиями которых осуществляются разработка, производство, сертификация и приемка в эксплуатацию технических средств, комплексов и систем физической защиты.

Нормативные документы по стандартизации определяют:

- применяемые термины и определения;
- порядок разработки комплексов технических средств;
- общие технические требования;
- тактико-технические характеристики и функциональные требования к различным типам технических средств, в том числе, подлежащих обязательной сертификации;
- требования к электрической и электромагнитной совместимости;
- формы представления сообщений на устройствах отображения информации;
- методы испытаний различных видов технических средств;
- требования к эксплуатационной документации;
- номенклатуру показателей качества.

Основной перечень нормативных документов, регламентирующих процессы разработки, испытаний и применения технических средств физической защиты, приведен в [18].

2.10. В целях обеспечения ЯОО техническими и инженерными средствами физической защиты в Минатоме России организована разработка и производство этих средств.

Разработка и производство осуществляются предприятиями и организациями отрасли в соответствии с отраслевыми программами и планами работ как на средства федерального бюджета и централизованные средства внебюджетных фондов, так и на собственные средства предприятий.

На ядерно-опасных объектах Минатома России могут использоваться также технические и инженерные средства физической защиты, произведенные (поставленные) другими производителями (поставщиками), в том числе зарубежными. При этом ТСФЗ, предназначенные для

внедрения на ядерно-опасных объектах Минатома России, должны быть сертифицированы и включены в Перечень технических средств физической защиты, разрешенных к применению в системах физической защиты ЯОО Минатома России.

Решение о включении конкретной аппаратуры в указанный перечень принимается Экспертным советом Минатома России по вопросам физической защиты [13].

Порядок формирования и ведения (актуализации) Перечня, а также порядок применения Перечня определяется Правилами формирования и ведения перечня технических средств физической защиты, разрешенных к применению в системах физической защиты ядерно-опасных объектов Минатома России [19].

В целях обеспечения качества и конкурентоспособности работ в области физической защиты и оборудования, предназначенного для использования в составе комплексов технических средств физической защиты ЯОО, в Минатоме России для выявления исполнителя работ (поставщика оборудования), обеспечивающего лучшие условия исполнения договора (контракта), предусмотрено проведение конкурсов (тендеров) на выполнение работ по проектированию, поставке и монтажу технических и инженерных средств физической защиты. Порядок и условия их проведения определяются соответствующим положением.

2.11. Для обеспечения задач физической защиты ядерно-опасные объекты Минатома России пользуются услугами специализированных организаций [6]:

- территориальных органов внутренних дел и ФСБ России, обеспечивающих ЯОО информацией об оперативной обстановке в районах их дислокации [6];
- государственных организаций Минатома России, обеспечивающих научно-методическое руководство работами в области физической защиты [20, 21];
- проектных организаций, выполняющих работы по проектированию (реконструкции) ядерно-опасных объектов и их систем физической защиты;
- строительно-монтажных организаций, выполняющих работы по строительству зданий и инженерных сооружений, монтажу технических средств физической защиты;
- образовательных организаций, осуществляющих подготовку, переподготовку и повышение квалификации специалистов в области физической защиты;
- организаций, специализирующихся в вопросах информационной безопасности.

Все специализированные организации должны иметь лицензии на соответствующий вид деятельности, выдаваемые в установленном порядке уполномоченными федеральными органами исполнительной власти.

2.12. В целях обеспечения физической защиты ядерно-опасных объектов осуществляется международное научно-техническое сотрудничество. Международное научно-техническое сотрудничество осуществляется как в рамках межправительственного соглашения между Минатомом России и Министерством энергетики США в области учета, контроля и физической защиты ядерных материалов [22], так и в рамках соглашений и договоров с другими странами.

В рамках этих соглашений предусмотрено финансирование работ и услуг в следующих направлениях:

- создание и совершенствование СФЗ;
- разработка нормативных и методических документов в области физической защиты;
- поставка технических и инженерных средств для СФЗ;
- монтаж оборудования;
- обучение персонала СФЗ.

В целях координации международного научно-технического сотрудничества в области физической защиты ядерных материалов, в том числе, с учетом необходимости поддержки федеральных и отраслевых программ в этой области, оптимизации использования технической помощи, а также контроля за выполнением принятых решений при Минатоме России функционирует специальная комиссия [22].

3. Цель, задачи и принципы построения СФЗ ЯОО

3.1. Цель СФЗ.

3.1.1. Целью СФЗ является предотвращение несанкционированных действий по отношению к ЯМ, ЯУ и другим предметам физической защиты (ПФЗ) на ЯОО.

Системы физической защиты рассматриваются в рамках настоящих Общих требований в виде совокупности организационных и технических мероприятий, проводимых администрацией ЯОО, его службой безопасности, подразделениями охраны (персоналом СФЗ) с использованием инженерно-технических средств физической защиты.

СФЗ является частью общей системы организационно-технических мер, осуществляемых на ЯОО, в целях обеспечения безопасности ядерной деятельности и сохранности ЯМ.

3.1.2. К ПФЗ относятся:

- ЯМ, в том числе изделия на их основе;

- ЯУ и/или ее уязвимые элементы, выявленные в процессе анализа уязвимости;
- носители секретной информации об ЯОО и ПФЗ, об организации, составе и функционировании СФЗ;
- другие системы, элементы и коммуникации ЯОО, необходимость в предотвращении несанкционированных действий по отношении к которым выявлена в процессе анализа уязвимости ЯОО.

3.1.3. Цель СФЗ достигается путем создания и обеспечения функционирования единой системы мер, направленных на решение задач СФЗ.

3.2. Задачи СФЗ.

3.2.1. СФЗ предназначена для выполнения следующих основных (целевых) задач:

- предупреждение несанкционированных действий;
- своевременное обнаружение несанкционированных действий;
- задержка (замедление) продвижения нарушителя;
- пресечение несанкционированных действий;
- задержание лиц, причастных к подготовке или совершению несанкционированных действий.

3.2.2. Предупреждение несанкционированных действий и обеспечение санкционированного доступа достигается путем:

- информирования местного населения и персонала ЯОО о степени безопасности функционирования ЯОО, эффективности его СФЗ, ответственности за несанкционированные действия по отношению к ЯМ, ЯУ и другим ПФЗ в соответствии с законодательством Российской Федерации;
- организации допуска персонала, командированных лиц и посетителей на ЯОО;
- организации пропускного режима на ЯОО;
- оборудования периметров охраняемых зон инженерно-техническими средствами физической защиты (ИТСФЗ);
- выявления лиц, причастных к подготовке диверсий или хищений ЯМ, а также несанкционированных действий по отношению к другим ПФЗ (совместно с органами ФСБ России и МВД России).

3.2.3. Своевременное обнаружение совершения или попытки совершения диверсии, хищения ЯМ, несанкционированного доступа, проноса (провоза) запрещенных предметов, вывода из строя средств физической защиты достигается путем:

- организации охраны периметров охраняемых зон, КПП и отдельных объектов;

- применения систем охранной сигнализации, технические средства обнаружения которых расположены по периметру охраняемых зон, зданий, сооружений, помещений, а также могут располагаться внутри сооружений, помещений;
- применения систем оптико-электронного наблюдения за периметрами охраняемых зон, контрольно-пропускными пунктами, охраняемыми зданиями, сооружениями, помещениями и подступами к ним;
- досмотра персонала, командированных лиц, посетителей (далее именуются – лица) и их вещей, в том числе с применением средств обнаружения проноса ЯМ, взрывчатых веществ и предметов из металла;
- своевременного выявления умышленного вывода из строя (попыток вывода из строя) ИТСФЗ;
- обеспечения пропускного и внутриобъектового режима на ЯОО;
- монтажа и эксплуатации ИТСФЗ в строгом соответствии с проектной и эксплуатационной документацией;
- контроля состояния и работоспособности ИТСФЗ;
- проведения учебы, разъяснительной работы и профилактики по обнаружению несанкционированных действий и оповещению сил реагирования СФЗ персоналом ЯОО;

3.2.4. Задержка (замедление) продвижения нарушителя к месту совершения диверсии или хищения ЯМ достигается путем:

- установки физических барьеров на возможных маршрутах проникновения нарушителя к местам совершения диверсий или хищения ЯМ, позволяющих задержать нарушителя на время, достаточное для прибытия сил охраны;
- выполнения подразделениями охраны и службы безопасности ЯОО действий по задержке продвижения нарушителей к месту совершения диверсии или хищения ЯМ.

3.2.5. Пресечение несанкционированных действий достигается путем:

- действий подразделений охраны, а также, в случае необходимости, внешних сил реагирования (региональных, федеральных) по предотвращению несанкционированного доступа в охраняемые зоны в соответствии с планом охраны и обороны ЯОО и порядком, установленным в нормативных правовых актах, регламентирующих действия ВВ МВД России и ведомственной охраны;
- нейтрализации нарушителей, проникших в охраняемые зоны, силами охраны, службы безопасности и персонала ЯОО в со-

ответствии с порядком, установленным планом взаимодействия администрации ЯОО, службы безопасности и подразделений охраны в штатных и чрезвычайных ситуациях, а также должностными инструкциями персонала СФЗ и ее дежурных служб;

- установления правила двух (трех) лиц при проведении работ в особо важной зоне, проверке транспортных средств, выезжающих за пределы охраняемых зон, вывозимых контейнеров и емкостей, при вскрытии и сдаче под охрану помещений, а также в других случаях, требующих использования принципа групповой работы для снижения возможности несанкционированных действий;
- применения в установленных законодательством случаях средств нелетального воздействия на нарушителей в целях временного вывода их из строя.

3.2.6. Задержание лиц, причастных к подготовке или совершению диверсии или хищения ЯМ, достигается путем:

- действий подразделений охраны, а также, в случае необходимости, внешних сил реагирования (региональных, федеральных) по задержанию нарушителей при совершении несанкционированного доступа в охраняемые зоны в соответствии с планом охраны и обороны ЯОО и порядком, установленном в нормативных правовых актах, регламентирующих действия ВВ МВД России и ведомственной охраны;
- действий по задержанию нарушителей, проникших в охраняемые зоны, личным составом подразделений охраны и персонала службы безопасности в соответствии с порядком, установленном планом взаимодействия администрации ЯОО, службы безопасности и подразделений охраны ЯОО в штатных и чрезвычайных ситуациях, а также должностными инструкциями персонала СФЗ;
- взаимодействия администрации, службы безопасности и подразделений охраны ЯОО с органами ФСБ России и МВД России в целях задержания нарушителей при подготовке к совершению диверсий, террористических актов (захват ядерных взрывных устройств и ядерных установок с последующей угрозой их подрыва, захват заложников и др.), хищений и несанкционированного доступа на территорию ЯОО и в его охраняемые зоны, а также при проведении оперативно-розыскных мероприятий по возвращению похищенных ЯМ и изделий на их основе.

3.2.7. В дополнение к основным задачам в рамках СФЗ в целях их эффективного решения должны выполняться обеспечивающие задачи по:

- разработке правового и нормативного обеспечения СФЗ;
- анализу уязвимости ЯОО и оценке эффективности СФЗ, подготовке на их основе предложений по совершенствованию СФЗ;
- защите информации в СФЗ;
- обеспечению подготовки персонала СФЗ к решению задач СФЗ;
- эксплуатации инженерно-технических средств.

3.3. Общие принципы построения СФЗ.

3.3.1. Принципы построения СФЗ направлены на достижение ее эффективности. СФЗ должна обеспечивать требуемую эффективность, которая определяется способностью СФЗ противостоять действиям нарушителей в отношении ЯМ, ЯУ и других ПФЗ с учетом перечня угроз и моделей нарушителей для конкретного ЯОО, определенных на этапе проведения анализа уязвимости.

3.3.2. При построении СФЗ необходимо руководствоваться следующими принципами:

- зонального построения;
- равнопрочности;
- обеспечения надежности и живучести;
- адаптивности;
- регулярности контроля функционирования;
- адекватности.

3.3.3. Принцип зонального построения СФЗ.

3.3.3.1. В зависимости от расположенных и эксплуатируемых на территории ЯОО ЯМ, ЯУ и других ПФЗ СФЗ должна предусматривать организацию и создание охраняемых зон, обеспечивающих «эшелонированную» защиту ПФЗ.

3.3.3.2. На ЯОО следует выделять как зоны, в которых размещаются ЯУ и/или хранятся ЯМ и/или проводятся работы с ними (защищенная, внутренняя и особо важная зоны), так и зоны, доступ в которые ограничивается из-за расположения в них жизненно важных для объекта и его систем безопасности элементов, но в которых ЯМ и ЯУ отсутствуют (зоны ограниченного доступа – ЗОД).

3.3.3.3. ПФЗ, в соответствии с присвоенными им категориями, должны размещаться в соответствующих охраняемых зонах. При организации зонирования объекта должно обеспечиваться усиление физической защиты от периферии к центру, то есть к защищаемым ПФЗ. Если в процессе проведения оценки эффективности СФЗ выясняется, что существующих охраняемых зон недостаточно для нейтрализации потенциальных угроз, то могут организовываться дополнительные охраняе-

мые зоны (рубежи) внутри существующих зон или ПФЗ размещаются в других охраняемых зонах.

Требования по категорированию и размещению ПФЗ в соответствующих охраняемых зонах определены в разделе 4 настоящего документа.

3.3.4. Принцип равнопрочности.

3.3.4.1. Должен быть обеспечен требуемый уровень эффективности СФЗ для всех выявленных в процессе анализа уязвимости типов нарушителей, способов совершения несанкционированных действий и маршрутов движения. Равнопрочность СФЗ должна обеспечиваться с точки зрения:

- предотвращения несанкционированного доступа;
- обнаружения попытки совершения несанкционированных действий;
- пресечения несанкционированных действий и задержания нарушителей в различных ситуаций;
- утечки информации.

Требуемый уровень эффективности СФЗ должен уточняться при создании и совершенствовании СФЗ с учетом категории ЯОО и критерия «эффективность-стоимость».

3.3.4.2. Равнопрочность СФЗ должна обеспечиваться по всему периметру охраняемой зоны (для заданного категорированного помещения или группы помещений), включая контролируемые проходы и/или КПП.

3.3.5. Принцип обеспечения надежности и живучести.

3.3.5.1. СФЗ должна быть способна выполнять задачи в штатных и чрезвычайных ситуациях, в том числе в условиях аварийной ситуации на ЯОО в пределах проектной аварии и ликвидации ее последствий.

3.3.5.2. Для обеспечения живучести СФЗ в штатных и чрезвычайных ситуациях в составе комплекса ИТСФЗ следует выделять группу инженерно-технических средств, используемых для физической защиты отдельной охраняемой зоны, а также входящих в ее состав категорированных помещений. Для управления работой указанной группы ИТСФЗ должен организовываться ЛПУ, имеющий все необходимые элементы индикации и связи и обеспечивающий возможность обеспечения физической защиты охраняемой зоны в автономном режиме.

3.3.5.3. Организация эксплуатации инженерно-технических средств должна предусматривать реализацию системы планово-предупредительного технического обслуживания.

3.3.5.4. Должны проводиться отбор и проверка благонадежности персонала ЯОО, обучение, подготовка персонала службы безопасности

ЯОО и личного состава подразделений охраны к действиям в штатных и чрезвычайных ситуациях.

3.3.5.5. Должно быть обеспечено резервирование элементов СФЗ. Резервирование отдельных функций может осуществляться за счет компенсационных мероприятий (с использованием персонала, технических и организационных мер). Для связи и передачи данных должны предусматриваться резервные каналы, в том числе с использованием альтернативных (носимых, световых, звуковых и т. п.) средств передачи информации

3.3.5.6. Нарушение функционирования отдельных элементов СФЗ не должно приводить к нарушениям функционирования СФЗ в целом. Для повышения надежности и живучести СФЗ должны использоваться соответствующие технические решения и организационные меры.

3.3.5.7. СФЗ следует строить на базе унифицированных модулей, обеспечивающих их совместимость при функционировании СФЗ:

- структурную;
- конструктивную;
- логическую;
- информационную;
- электромагнитную и т. д.

3.3.6. Принцип адаптивности.

3.3.6.1. СФЗ должна иметь возможность адаптироваться к изменениям:

- угроз и моделей нарушителей;
- в конфигурации объекта и границ охраняемых зон;
- видов и способов охраны;
- размещения ПФЗ.

3.3.6.2. СФЗ должна иметь возможность образовывать дополнительные рубежи физической защиты.

3.3.6.3. В СФЗ должны сочетаться различные способы постановки/снятия периметров, зданий, сооружений, помещений под охрану как в автоматическом, так и в ручном режимах.

3.3.6.4. СФЗ не должна создавать препятствий функционированию ЯОО и должна адаптироваться к технологическим особенностям работы ЯОО, в том числе в чрезвычайных ситуациях с учетом принятых на нем мер ядерной, радиационной, технологической и пожарной безопасности.

3.3.7. Принцип регулярности контроля функционирования.

3.3.7.1. Контроль за обеспечением физической защиты осуществляется на ведомственном уровне и на уровне ЯОО.

3.3.7.2. С целью определения эффективности СФЗ и отработки вопросов взаимодействия периодически должны проводиться учения, а

также проводиться оценка эффективности СФЗ аналитическим и другими методами. Результаты оценки эффективности должны использоваться для совершенствования СФЗ.

3.3.7.3. Вопросы осуществления ведомственного контроля отражены в разделе 16 настоящего документа и регламентируются Правилами и «Положением о ведомственном контроле за обеспечением физической защиты ядерно-опасного объекта» [14].

3.3.7.4. Уведомление обо всех имевших место случаях несанкционированных действий в отношении ЯМ, ЯУ и ПХ ЯМ должно проводиться в течение часа в порядке, установленном Правилами. Факты возникновения нештатных ситуаций в СФЗ должны сообщаться в Ситуационно-кризисный центр Минатома России [23].

3.3.7.5. Комплекс ТСФЗ должен иметь в своем составе компоненты и встроенные элементы, позволяющие осуществлять постоянный дистанционный контроль состояния и работоспособности ТСФЗ и функционирования СФЗ в целом.

3.3.8. Принцип адекватности.

Принятые на ЯОО организационные и административные меры, технические способы реализации физической защиты должны соответствовать принятым угрозам и моделям нарушителей.

Реализация принципа адекватности обеспечивается путем:

- проведения анализа уязвимости ЯОО;
- категорирования ЯОО, ПФЗ и мест их хранения и использования;
- выбора структуры и состава ИТСФЗ;
- определения способов охраны и обороны ЯОО;
- оценки эффективности СФЗ;
- использования при создании и совершенствовании СФЗ критерия «эффективность-стоимость»;
- возможности применения компенсационных мер.

3.3.9. На основании указанных принципов устанавливаются требования к созданию и организации функционирования СФЗ.

5. Анализ уязвимости ЯОО

5.1. С целью определения конкретных внутренних и внешних угроз, вероятных способов их осуществления, моделей нарушителя, а также выявления уязвимых мест ЯУ, ПХ ЯМ и технологических процессов использования и хранения ЯМ для последующего создания на основании полученных результатов эффективной СФЗ проводится анализ уязвимости ЯОО.

5.2. Анализ уязвимости ЯОО проводится на основе общих угроз ЯОО и общей модели нарушителя, устанавливаемых на отраслевом уровне.

Общие угрозы ЯОО и общая модель нарушителя излагаются в документе отраслевого уровня «Системы физической защиты. Методические рекомендации по проведению анализа уязвимости ядерно-опасных объектов».

Кроме того, на отраслевом уровне устанавливается перечень моделей внешнего и внутреннего нарушителей в зависимости от типа ЯОО, его категории и особенностей технологических процессов использования и хранения ЯМ, вводимых в действие приказами или распоряжениями по Минатому России.

5.3. Разработку указанных выше документов и их доведение до ЯОО в целях использования при проведении анализа уязвимости конкретных ЯОО организует и осуществляет в отрасли Департамент защиты информации, ядерных материалов и объектов.

5.4. Порядок и условия проведения анализа уязвимости ЯОО определяются в документе отраслевого уровня «Системы физической защиты. Методические рекомендации по проведению анализа уязвимости ядерно-опасных объектов» [24].

Анализ уязвимости проводится для всех действующих ЯОО, а также для вновь проектируемых и реконструируемых объектов, которые будут заниматься указанной деятельностью, с периодичностью, определяемой нормативными актами Минатома России.

Учебное издание

СТЕПАНОВ Борис Павлович
ГОДОВЫХ Алексей Валерьевич

ОСНОВЫ ПРОЕКТИРОВАНИЯ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ ОБЪЕКТОВ

Учебное пособие

Издано в авторской редакции

Компьютерная верстка *К.С. Чечельницкая*
Дизайн обложки *О.Ю. Аршинова*

Подписано к печати 08.06.2011. Формат 60x84/16. Бумага «Снегурочка».
Печать XEROX. Усл. печ. л. 6,86. Уч.-изд. л. 6,21.
Заказ 839-11. Тираж 35 экз.

Национальный исследовательский Томский политехнический университет
Система менеджмента качества
Издательства Томского политехнического университета сертифицирована
NATIONAL QUALITY ASSURANCE по стандарту BS EN ISO 9001:2008

ИЗДАТЕЛЬСТВО ТПУ. 634050, г. Томск, пр. Ленина, 30
Тел./факс: 8(3822)56-35-35, www.tpu.ru