Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)
Институт машиностроения и автомобильного транспорта
Кафедра «Автотранспортная и техносферная безопасность»

Методические указания к практическим занятиям
по дисциплине
«Надежность технических систем и техногенный риск»

часть 5

Составитель:
Киндеев Е.А.

Владимир, 2016

Темы практических занятий.

1. Общая структура анализа техногенного риска.
2. Принцип глубокоэшелонированной защиты и его реализация.
3. Пути понижения вероятности отказа.
4. Статистический метод расчета вероятности безошибочного выполнения операции.

Последовательность проведения анализа риска

1. Планирование и организация работ. На этом этапе необходимо:

- указать причины, вызывавшие необходимость проведения анализа риска;
- идентифицировать и описать анализируемую техническую систему;
- подобрать команду исполнителей, привлекаемых для проведения анализа риска;
- установить рабочие источники информации о безопасности системы;
- определить исходные данные для анализа риска;
- проанализировать неопределенности анализа риска;
- определить цели анализа риска и критерии приемлемого риска.

2. Идентификация опасностей. Основная задача – на основе собранной информации об объекте и опыта работы подобных систем выявить все присущие данной технической системе опасности. На этом же этапе проводится предварительная оценка опасностей с целью выбора одного из трех направлений деятельности:

а) в случае незначительности выявленных опасностей прекратить дальнейший анализ;

б) при значительной неопределенности выявленных опасностей провести более детальный анализ риска;

в) выработать рекомендации по уменьшению опасностей.

В первом случае процесс анализа риска может заканчиваться уже на этапе идентификации опасностей.

3. Оценка риска. Из всех идентифицированных опасностей необходимо выбрать опасности с неприемлемым уровнем риска. При этом критерии приемлемого риска и результаты оценки риска могут быть выражены качественно (в виде текстового описания) или количественно (например, в виде количества несчастных случаев или аварий в год).

Оценка риска включает в себя анализ вероятности возникновения опасного события и анализ тяжести последствий этих событий. Однако, когда тяжесть последствий незначительна или событие крайне маловероятно, достаточно оценить один параметр. Для анализа частоты обычно используются:

- исторические данные по соответствующим типам технических систем или видам деятельности;
- статистические данные по аварийности и надежности оборудования;
- логические методы анализа «деревьев событий» или «деревьев отказов»;
- экспертная оценка с учетом мнения специалистов в данной области.

Анализ тяжести последствий включает в себя оценку воздействия на людей, имущество или окружающую среду. Для прогнозирования последствий необходимо понимать сущность происходящих аварийных процессов, действующих поражающих факторов и оценить степень поражения изучаемых объектов воздействия.

В ходе проведения оценки риска следует проанализировать возможную неопределенность результатов, вызванную неточностью информации по надежности оборудования и ошибкам персонала, а также принятыми допущениями в применяемых при расчете моделях аварийного процесса. Анализ неопределенности – это оценка неопределенности результатов оценки риска, вызванной неопределенностью исходных данных и точностью использованных моделей.

Следует подчеркнуть, что часто сложные и дорогостоящие расчеты дают значение риска, точность которого очень невелика.

Качественные (инженерные) методы анализа риска позволяют достигать основных целей анализа риска при использовании меньшего объема информации и затрат труда. Однако количественные методы оценки риска всегда очень полезны, а в некоторых ситуациях – единственно возможны, в частности, для сравнения опасностей различной природы или при экспертизе особо опасных сложных технических систем.

4. Разработка рекомендаций по управлению риском. Существующий риск может быть признан приемлемым, в противном случае необходимо указать меры по уменьшению риска. Меры по

управлению риска могут иметь технический, эксплуатационный или организационный характер.

Следует заметить, что иногда могут происходить события, считавшиеся ранее чрезвычайно маловероятными. Тяжесть последствий таких событий может быть очень велика. Например, катастрофа океанского лайнера «Титаник» или авария на японской атомной электростанции «Фукусима». В обоих случаях произошли природные катаклизмы, ранее никогда не наблюдавшиеся и считавшиеся невероятными. Технические системы попали в условия эксплуатации, при которых их функционирование стало невозможно.

Качественные методы анализа риска

Существуют следующие методы идентификации возможных опасностей:

1. Инженерные методы. На основе собранных статистических данных проводится вероятностный анализ опасностей, производится построение деревьев опасности.

2. Модельные методы. По накопленным исходным данным и результатам наблюдений строят модели воздействия вредных и опасных факторов на отдельного человека, профессиональные и социальные группы населения.

3. Экспертные методы. Проводится оценка вероятностей опасных событий с помощью опроса экспертов в данной области науки, техники или технологий.

4. Социологические методы. Определяются вероятности опасных событий путем опроса населения.

Для более точной и достоверной оценки риска эти методы применяют совместно.

Качественные методы анализа опасностей позволяют определить источники возникновения опасностей, возможные аварии или несчастные случаи, разработать мероприятия для предотвращения опасных событий и снижения тяжести их последствий.

Перед проведением качественного анализа необходимо идентифицировать источники опасностей. Для этого собирают исходные данные и проводят предварительный анализ опасностей.

При анализе опасностей выбор определенного качественного метода зависит от цели анализа и особенностей технической системы. Существуют следующие качественные методы анализа опасностей:

- предварительный анализ опасностей;

- анализ последствий отказов;
- анализ опасностей с помощью «дерева причин»;
- анализ опасностей с помощью «дерева последствий»;
- анализ опасностей методом потенциальных отклонений;
- анализ ошибок персонала;
- причинно-следственный анализ.

Предварительный анализ опасностей (ПАО) заключается в выявлении источника опасностей, определении причин возникновения опасных состояний и характеристике опасностей в зависимости от вызываемых ими последствий.

Порядок предварительного анализа опасностей:

1. Определение технических характеристик технической системы, процесса, используемых источников энергии, материалов и их повреждающих свойств.

2. Поиск нормативно-технической документации, действие которой распространяется на данную техническую систему или процесс.

3. Проводят проверку используемой технической документации на ее соответствие нормам и правилам безопасности.

4. Составляют перечень опасностей, в котором указывают идентифицированные источники опасностей, возможные поражающие факторы, ход протекания потенциальных аварий и другие выявленные недостатки.

В ходе ПАО осуществляется первая попытка выявить потенциально опасные части технической системы и отдельные события, которые могут привести к возникновению опасностей. Этот анализ выполняется на начальном этапе разработки системы. Детальный анализ возможных событий обычно проводится после того, как система полностью определена с помощью дерева отказов.

Анализ последствий отказов (АПО) – качественный метод идентификации опасностей, основанный на системном подходе, позволяющий сделать определенные прогнозы. АПО – анализ индуктивного типа, с помощью которого систематически, на основе последовательного рассмотрения одного элемента за другим анализируются все возможные виды отказов или аварийные ситуации и выявляется их результирующее воздействие на систему.

Изучение отдельных аварийных ситуаций и отказов элементов позволяет определить их воздействие на другие близлежащие элементы и систему в целом. АПО проводят в следующем порядке:

1. Техническую систему подразделяют на составляющие компоненты.

2. Для каждого составляющего систему компонента выявляют все возможные отказы.

3. Изучают все потенциальные аварии, которые могут быть вызваны отказами компонентов исследуемого объекта.

4. Отказы ранжируют по степени опасности и разрабатывают меры, позволяющие избежать возникновения этих отказов.

При помощи АПО можно оценить потенциальную опасность любого технического объекта.

Анализ опасностей с помощью «дерева причин» потенциальной аварии (АОДП) позволяет выявить комбинации отказов оборудования, ошибок персонала и внешних воздействий, приводящих к аварийной ситуации (основному событию). АОДП выполняют в следующем порядке:

1. Выбирают возможное событие – аварию или отказ, которые могут привести к аварии.

2. Выявляют факторы, которые могут привести к заданной аварии.

3. Строят ориентированный граф – «дерево», вершина (корень) которого является потенциальной аварией.

Проведение анализа с помощью дерева причин возможно только после детального изучения рабочих функций всех компонентов рассматриваемой технической системы. На работу системы оказывает влияние человеческий фактор, например, возможность совершения оператором ошибки. Поэтому желательно все потенциальные инциденты – «отказы операторов» вводить в содержание дерева причин-отказов. Дерево отражает статический характер событий. Построением нескольких деревьев можно отразить их динамику, т. е. развитие событий во времени. Для определения последовательности событий при аварии, включающей сложные взаимодействия между техническими системами обеспечения безопасности, используется дерево событий.

Анализ опасностей с помощью «дерева последствий» потенциальной аварии (АОДПО) отличается от АОДП тем, что в этом случае задается критическое событие – инициатор, и исследуют всю группу событий – последствий, к которым оно может привести. Анализ причин последствий начинается с выбора критического события. Критические события выбирают таким образом, чтобы они служили удобными отправными точками для анализа, причем большинство

аварийных ситуаций развивается за критическим событием в виде цепи отдельных событий. Процедура построения диаграммы – дерева последствий – состоит из выбора первого инициирующего события, за которым следуют другие события, определенные на данном этапе работы.

При анализе «причин – последствий» используются комбинированные методы дерева отказов (выявить причины) и дерева событий (показать последствия), причем все явления рассматриваются в естественной последовательности их появления.

Анализ опасностей методом потенциальных отклонений (АОМПО) включает процедуру искусственного создания отклонений с помощью ключевых слов. Для этого разбивают технологический процесс или техническую систему на составные части и, создавая с помощью ключевых слов отклонения, систематично изучают их потенциальные причины и те последствия, к которым они могут привести на практике.

Анализ ошибок персонала (АОП) – один из важнейших элементов методологии оценки опасностей; позволяет учесть воздействие человеческого фактора, т. е. учесть как ошибки, инициирующие или усугубляющие аварийную ситуацию, так и способность персонала совершать корректирующие действия по управлению аварией.

АОП включает следующие этапы:

1) выбор системы и вида работы;
2) определение цели;
3) идентификацию вида потенциальной ошибки;
4) идентификацию последствий;
5) идентификацию возможности исправления ошибки;
6) идентификацию причины ошибки;
7) выбор метода предотвращения ошибки;
8) оценку вероятности ошибки;
9) оценку вероятности исправления ошибки;
10) расчет риска;
11) выбор путей снижения риска.

Причинно-следственный анализ (ПСА) выявляет причины происшедшей аварии или катастрофы и является составной частью общего анализа опасностей. Он завершается прогнозом новых авварий и составлением плана мероприятий по их предупреждению. ПСА включает следующие этапы:

1. Точном и объективное описании аварии.

2. Определение событий, предшествовавших аварии.

3. Построение ориентированного графа – дерева причин, начиная с последней стадии развития событий, т. е. с самой аварии.

4. Выявление логических связей дерева причин;

5. Разработка предупредительных мер для исключения повторения аналогичных аварий.

Количественная оценка риска

Количественный анализ опасностей дает возможность расчитать вероятности возникновения опасных событий и тяжесть последствий этих событий. Для проведения количественного анализа применяются статистический анализ и различные методы расчета вероятностей.

Для удобства расчетов сложные системы разбивают на подсистемы. *Подсистемой* называют часть системы, которую выделяют по определенному признаку, отвечающему конкретным целям и задачам функционирования системы. Подсистема может рассматриваться как самостоятельная система, состоящая из других подсистем, т. е. иерархическая структура сложной системы может состоять из подсистем различных уровней, где подсистемы низших уровней входят составными частями в подсистемы высших уровней. В свою очередь, подсистемы состоят из *компонентов* – частей системы, которые рассматриваются без дальнейшего деления как единое целое.

Логический анализ внутренней структуры системы и определение вероятности нежелательных событий как функции отдельных составляющих событий являются одной из задач анализа опасностей.

Подсистемой «И» называют ту часть системы, компоненты которой соединены параллельно. К отказу такой подсистемы приводит отказ всех ее компонентов.

Если отказы компонентов можно считать взаимно независимыми, то вероятность отказа в подсистеме «И» запишем

$$P(A) = \prod_{i=1}^{n} P(A_i),$$

где $P(A)$ – вероятность события A (отказ всей подсистемы «И»);
$P(A_i)$ – вероятность отказа i-го компонента подсистемы «И»;
n – общее количество компонентов подсистемы «И».

На практике подсистемы «И» создают дублированием или резервированием. Данный технический прием применяют в случае, если

необходимо достичь высокой степени надежности системы, особенно в системах, обеспечивающих безопасность.

Подсистемой «ИЛИ» называют часть системы, компоненты которой соединены последовательно. К нежелательному событию в такой подсистеме приводит отказ любого компонента.

Если отказы компонентов взаимно независимы, то вероятность отказа в подсистеме «ИЛИ» запишем:

$$P(A) = 1 - \prod_{i=1}^{n}\left(1 - P(A_i)\right)$$

Для равновозможных отказов вероятность отказа в этой подсистеме

$$P(A) = 1 - (1 - p)^n.$$

Выражение (6.12) свидетельствует о высокой вероятности отказа в сложных системах, даже состоящих из элементов с высокой надежностью. Например, при вероятности отказа компонента $p = 0{,}05$ подсистема «ИЛИ», состоящая из 20 компонентов ($n = 20$), имеет вероятность того, что отказа в подсистеме не произойдет, равную

$(1 - p)^n = (1 - 0{,}05)^{20} \approx 0{,}358.$

При анализе риска следует учитывать следующие аспекты:

1. Устройства, операции, действия персонала, которые с точки зрения безопасности выполняют одни и те же функции в системе, могут считаться соединенными параллельно.
2. Устройства, операции, действия персонала, каждое из которых необходимо для предотвращения опасного события, должны рассматриваться как соединенные последовательно.

На практике, зачастую подсистемы «И» или «ИЛИ» могут состоять из компонентов, в свою очередь соединенных в подсистемы «И» или «ИЛИ» в любых комбинациях.

Вероятность возникновения опасности – величина, существенно меньшая единицы. Кроме того, точки реализации опасности распределены в пространстве и времени. Это значит, что, например, вероятность пожара в одном здании населенного пункта гораздо выше, чем вероятность одновременного пожара всех зданий этого населенного пункта, или вероятность пяти подряд очень холодных зим гораздо ниже вероятности одной очень холодной зимы.

Таким образом, чем больший отрезок времени или количество рискующих субъектов мы возьмем, тем определённее станет величина ущерба, который субъекты получат в совокупности за этот отрезок времени.

В терминах риска принято описывать и опасности от достоверных событий, происходящих с вероятностью, равной единице. Таким примером является загрязнение окружающей среды отходами конкретного промышленного предприятия. В этом случае «риск» эквивалентен степени риска и соответственно величина риска равна величине ущерба.

Обычно при оценке степени риска его характеризуют двумя величинами – вероятностью события P и последствиями X, которые в ыражении математического ожидания выступают как сомножители:

$$R = PX.$$

По отношению к источникам опасностей оценка риска предусматривает разграничение нормального режима работы $R_н$ и аварийных ситуаций $R_{ав}$:

$$R = R_н + R_{ав} = P_н X_н + P_{ав} X_{ав}.$$

В случае, когда последствия неизвестны, то под риском понимают вероятность наступления определенного сочетания нежелательных событий

$$R = \Sigma P_i . R = \sum_{i=1}^{n} P_i.$$

При необходимости можно использовать определение риска как вероятности превышения предела x:

$$R = P\{\xi > x\},$$

где ξ – случайная величина.

Техногенный риск оценивают по формуле, включающей вероятность нежелательного события и величину последствий в виде ущерба U:

$$R = PU.$$

Если каждому нежелательному событию, происходящему с вероятностью P_i, соответствует ущерб U_i, то величина риска будет представлять собой ожидаемую величину ущерба U^*:

$$R = U^* = \sum_{i=1}^{n} P_i U_i.$$

Если все вероятности наступления нежелательного события одинаковые ($P_i = P,\ i = 1, \ldots, n$), то

$$R = P \sum_{i=1}^{n} U_i.$$

Когда существует опасность здоровью и материальным ценностям, риск целесообразно представлять в векторном виде с различными единицами измерения по координатным осям

$$\vec{R} = \vec{U}\vec{P}.$$

Перемножение в правой части этого уравнения производится покомпонентно, что позволяет сравнивать риски.

Индивидуальный риск можно определить как ожидаемое значение причиняемого ущерба U^* за интервал времени T и отнесенное к группе людей численностью M человек:

$$R = U^*/MT.$$

Общий риск для группы людей (коллективный риск)

$$R = U^*/T.$$

Пример 1. Провести численную оценку риска чрезвычайного происшествия в технической системе, состоящей из трех подсистем, с независимыми отказами. Вероятности отказов подсистем: $P_1 = 10^{-3}$, $P_2 = 10^{-4}$, $P_3 = 10^{-2}$, ожидаемые ущербы от отказов подсистем $U_1 = 10^6$ руб., $U_2 = 5 \cdot 10^6$ руб., $U_3 = 10^5$ руб.

Решение.

Определим величину риска чрезвычайного происшествия технической системы как ожидаемую величину ущерба

$$R = U = \sum_{i=1}^{3} P_i U_i = P_1U_1 + P_2U_2 + P_3U_3 = 10^{-3}\cdot 10^6 + 10^{-4}\cdot 5\cdot 10^6 +$$

$$+ 10^{-2}\cdot 10^5 = 2\,500 \text{ руб.}$$

Пример 2. Провести численную оценку риска чрезвычайного происшествия в технической системе, состоящей из пяти подсистем, с независимыми равновозможными отказами $P = 10^{-2}$. Ожидаемые ущербы от отказов подсистем $U_1 = 10^6$, $U_2 = 10^7$, $U_3 = 10^8$, $U_4 = 10^9$, $U_5 = 10^{10}$.

Решение.

Определим величину риска чрезвычайного происшествия технической системы с равновозможными отказами подсистем как ожидаемую величину ущерба

$$R = U = P\sum_{i=1}^{5} U_i = P(U_1+U_2+U_3+U_4+U_5) = 10^{-2}(1 +10 +10^2 +10^3 +10^4)10^6 =$$

$$= 11\,110\,000 \text{ руб.}$$