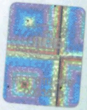
РУКОВОДСТВА ПО БЕЗОПАСНОСТИ
в области использования атомной энергии



РЕКОМЕНДАЦИИ ПО ПОРЯДКУ ВЫПОЛНЕНИЯ АНАЛИЗА НАДЕЖНОСТИ СИСТЕМ И ЭЛЕМЕНТОВ АТОМНЫХ СТАНЦИЙ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ, И ИХ ФУНКЦИЙ

РБ-100-15

gost.e-ecolog.ru

ФБУ «НТЦ ЯРБ»

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ЭКОЛОГИЧЕСКОМУ, ТЕХНОЛОГИЧЕСКОМУ И АТОМНОМУ НАДЗОРУ

УТВЕРЖДЕНО
приказом Федеральной службы
по экологическому, технологическому
и атомному надзору
от 28 января 2015 г. № 26

РУКОВОДСТВО ПО БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ АТОМНОЙ ЭНЕРГИИ «РЕКОМЕНДАЦИИ ПО ПОРЯДКУ ВЫПОЛНЕНИЯ АНАЛИЗА НАДЕЖНОСТИ СИСТЕМ И ЭЛЕМЕНТОВ АТОМНЫХ СТАНЦИЙ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ, И ИХ ФУНКЦИЙ» (РБ-100-15)

Введено в действие
с 28 января 2015 г.

Москва 2015

РУКОВОДСТВО ПО БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ АТОМНОЙ ЭНЕРГИИ «РЕКОМЕНДАЦИИ ПО ПОРЯДКУ ВЫПОЛНЕНИЯ АНАЛИЗА НАДЕЖНОСТИ СИСТЕМ И ЭЛЕМЕНТОВ АТОМНЫХ СТАНЦИЙ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ, И ИХ ФУНКЦИЙ» (РБ-100-15)

Федеральная служба по экологическому, технологическому и атомному надзору

Москва 2015

Настоящее Руководство по безопасности разработано в соответствии со статьей 6 Федерального закона от 21 ноября 1995 г. № 170-ФЗ «Об использовании атомной энергии» в целях содействия соблюдению требований федеральных норм и правил в области использования атомной энергии «Общие положения обеспечения безопасности атомных станций» (ОПБ-88/97), утвержденных постановлением Госатомнадзора России от 14 ноября 1997 г. № 9 , федеральных норм и правил в области использования атомной энергии «Требования к содержанию отчета по обоснованию безопасности АС с реактором типа ВВЭР» (НП-006-98), утвержденных постановлением Госатомнадзора России от 3 мая 1995 г. № 7, федеральных норм и правил в области использования атомной энергии «Требования к содержанию отчета по обоснованию безопасности атомных станций с реакторами на быстрых нейтронах» (НП-018-05), утвержденных постановлением Ростехнадзора от 2 декабря 2005 г. № 9.

Руководство по безопасности содержит рекомендации Федеральной службы по экологическому, технологическому и атомному надзору по порядку выполнения и представления результатов анализа надежности систем и элементов, важных для безопасности, а также выполняемых ими функций.

Руководство по безопасности предназначено для использования проектными и конструкторскими организациями, а также эксплуатирующими организациями.

Выпускается впервые.[1]

---

[1]Разработано коллективом авторов в составе: Ланкин М.Ю., к.т.н., Самохин Г.И., к.т.н., Носков Д.Е., Марьенков А.А. (ФБУ «НТЦ ЯРБ», г. Москва), Ершов Г.А., проф., д.т.н. (ОАО «Атомпроект», г. С-Петербург), Токмачев Г.В. к.т.н., Калинкин И.В., Юрьев Р.В. к.т.н., Байкова Е.В. (ОАО «Атомэнергопроект», г. Москва), Былов И.А., к т.н. (ОАО «ОКБМ Африкантов», г. Нижний Новгород), Антонов А.В., проф., д.т.н. (ИАТЭ НИЯУ МИФИ, г. Обнинск).

I. Общие положения

1. Настоящее руководство по безопасности при использовании атомной энергии «Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций» (РБ-100-15) (далее – Руководство по безопасности) разработано в соответствии со статьей 6 Федерального закона от 21 ноября 1995 г. № 170-ФЗ «Об использовании атомной энергии» в целях содействия соблюдению требований пункта 4.1.12 федеральных норм и правил в области использования атомной энергии «Общие положения обеспечения безопасности атомных станций» ОПБ-88/97 (НП-001-97), утвержденных постановлением Госатомнадзора России от 14 ноября 1997 г. № 9, в части выполнения анализа надежности, оценки показателей надежности и представления результатов анализа надежности для систем атомных станций нормальной эксплуатации, важных для безопасности, и их элементов, отнесенных к классам безопасности 1 и 2, а также систем и элементов безопасности атомных станций; пункта 1.8.1, а также подраздела 4 раздела «Общие требования» федеральных норм и правил в области использования атомной энергии «Требования к содержанию отчета по обоснованию безопасности АС с реактором типа ВВЭР» (НП-006-98) (ПНАЭ Г-01-036-95), утвержденных постановлением Госатомнадзора России от 3 мая 1995 г. № 7, в части представления информации о надежности элементов систем, важных для безопасности; пункта 1.8.1 федеральных норм и правил в области использования атомной энергии «Требования к содержанию отчета по обоснованию безопасности атомных станций с реакторами на быстрых нейтронах» (НП-018-05), утвержденных постановлением Ростехнадзора от 2 декабря 2005 г. № 9 (зарегистрировано Минюстом России 26 января 2006 г., регистрационный № 7413), в части представления информации о надежности выполнения функций безопасности.

2. Настоящее Руководство по безопасности содержит рекомендации Федеральной службы по экологическому, технологическому и атомному надзору по целям, объему, порядку выполнения анализа надежности систем и элементов, важных для безопасности, применению результатов оценок,

а также по содержанию и объему отчетной документации при выполнении указанного анализа.

3. Настоящее Руководство по безопасности предназначено для использования проектными и конструкторскими организациями, а также эксплуатирующими организациями.

4. Требования федеральных норм и правил в области использования атомной энергии могут быть выполнены с использованием других методик анализа надежности выполнения функций системами и элементами атомных станций, важными для безопасности, в том числе анализа надежности (функциональной безопасности) сложных технологических комплексов, чем те, которые содержатся в настоящем Руководстве по безопасности, при обоснованности выбранных способов (методов) для обеспечения безопасности.

5. Перечень сокращений, использованных в настоящем Руководстве по безопасности, приведен в приложении № 1 к настоящему Руководству по безопасности, термины и определения приведены в приложении № 2 к настоящему Руководству по безопасности, список источников, рекомендуемых для использования при выполнении анализа надежности в соответствии с рекомендациями настоящего Руководства по безопасности, приведен в приложении № 3 к настоящему Руководству по безопасности.

6. Анализ надежности систем и элементов, важных для безопасности, в том числе анализ надежности (функциональной безопасности) сложных технологических комплексов, выполняется для проектируемых, сооружаемых и эксплуатируемых блоков АС.

7. Анализ надежности выполняется в отношении:

систем нормальной эксплуатации, важных для безопасности;

систем безопасности;

элементов систем нормальной эксплуатации, относящихся к классам безопасности 1, 2;

специальных технических средств по управлению запроектными авариями;

иных систем и элементов АС, для которых установлены нормируемые показатели надежности;

функций, важных для безопасности (в том числе функций безопасности), если в выполнении функции, важной для безопасности, участвуют более одной системы (в том числе сложные технологические комплексы).

8. Представленные в настоящем Руководстве по безопасности рекомендации по порядку выполнения анализа надежности систем относятся также к анализу надежности выполнения функций безопасности и иных требуемых функций.

При условии разработки анализа надежности выполнения функций безопасности (иных требуемых функций), которые осуществляются за счет совместной работы нескольких систем (в том числе сложных технологических комплексов), допускается не выполнять анализ надежности отдельных систем из числа указанных (в том числе систем, входящих в сложные технологические комплексы) по выполнению соответствующих функций.

9. Качественный анализ надежности систем, важных для безопасности, выполняется в соответствии с положениями главы II настоящего Руководства по безопасности.

Анализ надежности (определение показателей надежности) элементов АС выполняется в соответствии с положениями главы III настоящего Руководства по безопасности.

Количественный анализ надежности систем, важных для безопасности, выполняется в соответствии с положениями главы IV настоящего Руководства по безопасности.

При количественном анализе надежности (функциональной безопасности) сложных технологических комплексов наряду с положениями главы IV учитываются также положения главы V настоящего Руководства по безопасности.

10. Результатом анализа надежности является определение (оценка) показателей надежности выполнения системами и элементами АС функций безопасности и иных требуемых функций. Рекомендуется в составе показателей надежности принимать показатели, характеризующие безотказность анализируемой системы (элемента).

11. При выполнении анализа надежности систем определяются все функции, важные для безопасности (в том числе функции безопасности), которые выполняет система при нормальной эксплуатации АС, а также при нарушении нормальной эксплуа-

тации АС, включая аварии. Анализ надежности выполняется отдельно для каждой из установленных в соответствии с данным пунктом функций системы.

12. Анализ надежности системы выполняется отдельно для каждого из выявленных состояний нормальной эксплуатации, а также состояний с нарушением нормальной эксплуатации АС, при которых необходимо выполнение системой требуемой функции, если справедливо хотя бы одно из условий:

для рассматриваемого состояния АС критерий отказа на выполнение системой требуемой функции отличается от критерия отказа для других состояний;

для рассматриваемого состояния АС конфигурация системы (набор элементов системы, состояние которых влияет на выполнение системой требуемой функции) отличается от конфигурации системы в других состояниях;

в рассматриваемом состоянии АС различаются требования со стороны анализируемой системы к состоянию обеспечивающих или управляющих систем, работа которых необходима для выполнения системой требуемой функции;

для рассматриваемого состояния перечень отказов элементов системы, способных оказать влияние на выполнение системой требуемой функции, отличается от перечня таких отказов для других состояний.

13. Результаты анализа надежности систем (элементов), для которых установлены нормируемые показатели надежности, сравниваются с указанными показателями.

14. Результаты анализа надежности систем (элементов) рекомендуется использовать при выполнении анализов безопасности (в частности, вероятностного анализа безопасности), а также при разработке рекомендаций по повышению безопасности АС.

15. При анализе надежности систем (элементов) эксплуатируемых блоков АС учитываются реальное состояние систем (элементов) АС, действующие процедуры эксплуатации, технического обслуживания, испытаний и ремонта (при их наличии), а также опыт эксплуатации блока АС, для которого выполняется анализ надежности и опыт эксплуатации аналогичных блоков АС.

16. При анализе надежности системы учитывается надежность обеспечивающих систем и систем управления, от которых зависит выполнение анализируемой системой своих функций.

17. При анализе надежности системы учитываются возможные ошибки персонала, а также отказы по общим причинам (отказы общего вида).

II. Качественный анализ надежности системы

18. Качественный анализ надежности системы выполняется после сбора информации о системе и определения границ моделирования, осуществляемых в соответствии с приложением № 4 к настоящему Руководству по безопасности.

19. Качественный анализ надежности системы заключается в определении последствий отказов элементов и ошибок персонала и выполняется в следующей последовательности отдельно для каждой функции системы, учитываемой в соответствии с пунктом 11 настоящего Руководства по безопасности:

определение критериев отказа выполнения системой требуемых функций;

разработка упрощенной схемы системы;

определение последствий отказов и неготовности элементов, а также неправильных действий персонала;

графическое представление условий работоспособности системы (функций системы).

20. Упрощенная схема системы разрабатывается на основе полной схемы системы. В упрощенную схему включаются только те элементы, которые включены в границы моделирования системы в соответствии с приложением № 4 к настоящему Руководству по безопасности.

21. Определяются группы элементов системы, для которых возможно возникновение отказов по общим причинам (отказов общего вида).

При определении групп элементов системы, подверженных отказам по общим причинам (отказам общего вида) учитываются следующие причины, которые могут приводить к таким отказам:

общность конструкции элементов;

одинаковые условия использования элементов, включая режимы работы и условия окружающей среды;

одинаковые условия технического обслуживания и ремонта.

22. Определение последствий отказов элементов и ошибок персонала выполняется в следующей последовательности:

для каждого элемента системы составляется перечень возможных видов отказов данного элемента;

для каждого элемента, либо группы элементов, подверженных отказам по общим причинам, либо действия персонала оценивается тяжесть последствий отказа элемента, ошибки персонала, отказа группы элементов (например, отказ системы, отказ канала системы, снижение уровня резервирования);

выделяются отказы элементов и ошибки персонала, а также отказы групп элементов, подверженных отказам по общим причинам, которые приводят к отказу системы, с включением в перечень критичных отказов (ошибок).

III. Определение показателей надежности элементов

23. Для каждого элемента, включенного в границы моделирования системы в соответствии с рекомендуемым порядком, представленным в приложении № 4 к настоящему Руководству по безопасности, устанавливаются возможные виды отказов, способные сказаться на надежности выполнения анализируемой системой требуемых функций.

Учитываются следующие виды отказов:

отказ на требование (включая отказ на запуск, отказ на открытие, отказ на закрытие, отказ на изменение положения);

отказ при работе (включая отказ типа несанкционированного срабатывания).

24. Анализируется необходимость учета в модели надежности системы событий, связанных с неготовностью элементов системы, каналов системы, либо системы в целом из-за технического обслуживания, ремонта или испытаний.

25. Решение о необходимости учета в модели надежности системы конкретных видов отказов элементов системы, а также событий неготовности элементов системы, каналов системы, либо системы в целом из-за технического обслуживания, ремонта или испытаний принимается по результатам выполнения для системы анализа видов отказов и их последствий и представляется в виде таблицы, пример которой представлен в приложении № 6 к настоящему Руководству по безопасности.

26. Для расчета показателей надежности элементов АС используются следующие типы исходных данных:

данные, полученные при эксплуатации анализируемой системы (элементов), либо анализируемой АС (специфические данные);

данные, полученные при эксплуатации аналогичных систем (элементов) АС (обобщенные данные).

27. Расчет показателей надежности элементов системы выполняется с использованием специфических данных, а при их отсутствии – с использованием обобщенных данных.

28. Для оценки показателей надежности элементов рекомендуется определять следующие характеристики элементов:

суммарная наработка (в часах) в режиме ожидания;

суммарная наработка (в часах) в режиме работы;

количество требований на срабатывание (например, требований на запуск, на открытие, на закрытие);

количество отказов за наработку в режиме ожидания;

количество отказов за наработку в режиме работы;

количество отказов на требование.

29. При оценке суммарной наработки элемента учитываются все периоды нахождения в режиме ожидания (готовности к выполнению требуемой функции) или в режиме работы (выполнения заданной функции) при нахождении блока АС в рассматриваемом состоянии.

При подсчете числа требований на срабатывание элемента учитываются все требования на срабатывание, возникающие при:

проверках работоспособности (для определения частоты проверки работоспособности конкретного оборудования используется соответствующая документация по проверкам работоспособности);

нормальной эксплуатации АС (автоматически защитами и блокировками или вручную оператором);

возникновении иных ситуаций, требующих срабатывания (запуска) элемента.

Требования на срабатывание (запуск) рекомендуется классифицировать в соответствии с видами отказов, определенных для элемента данного типа (например, требование на открытие, закрытие, запуск).

30. Для определения показателей надежности системы на выполнение требуемых функций (вероятности безотказного функционирования), как правило, необходимы следующие данные по надежности ее элементов:

интенсивность отказов элементов системы в режиме ожидания и в режиме работы;

период между проверками работоспособности элементов системы;

длительность выполнения проверки работоспособности;

вероятность отказов на требование элементов системы;

среднее время неготовности системы (элементов системы) из-за проведения технического обслуживания, ремонта либо испытаний;

допустимое время неготовности системы (элементов системы) при сохранении режима работы блока АС.

31. Рекомендуемый порядок определения видов отказов и количественной оценки показателей надежности элементов АС представлен в приложении № 6 к настоящему Руководству по безопасности.

IV. Количественный анализ надёжности системы

32. Количественный анализ надёжности системы выполняется для каждой из требуемых функций системы, учитываемых в соответствии с пунктом 11 настоящего Руководства по безопасности.

33. Количественный анализ надёжности выполняется в следующей последовательности:

выполняется качественный анализ надёжности системы (в соответствии с рекомендуемым порядком, представленным в главе II настоящего Руководства по безопасности);

определяются показатели надёжности элементов системы (вероятности отказов элементов системы, в том числе вероятности неготовности из-за технического обслуживания, ремонтов и испытаний) в соответствии с порядком, представленным в главе III настоящего Руководства по безопасности;

выполняется учёт влияния персонала на надёжность выполнения системой требуемых функций (в соответствии с рекомендуемым порядком, представленным в приложении № 5 к настоящему Руководству по безопасности);

выполняется учёт ООВ (в соответствии с рекомендуемым порядком, представленным в приложении № 7 к настоящему Руководству по безопасности);

определяется вид графического представления структурно-логической модели системы, используемой для проведения количественного анализа надёжности системы (деревья отказов, схемы функциональной целостности, марковские схемы и др.);

разрабатываются структурно-логические модели системы (например, деревья отказов) для каждой из требуемых функций системы;

рассчитываются показатели надежности системы для каждой из требуемых функций;

выполняется оценка уровня надёжности системы (в том числе сопоставление с нормируемыми показателями надёжности, если такие установлены).

34. При проведении количественного анализа надежности системы рекомендуется также выполнить:

оценку неопределенности расчетов показателей надежности системы;

оценку значимости элементов системы и действий (ошибок) персонала;

оценку чувствительности результатов расчетов показателей надежности системы к исходным данным, использованным при их выполнении.

35. При анализе чувствительности к принятым допущениям и упрощениям рекомендуется:

рассматривать все принятые допущения и упрощения, влияющие на результаты анализа надежности систем;

приводить обоснования принятых допущений и упрощений с необходимыми ссылками;

оценивать влияние допущений и упрощений на результаты и выводы анализа надежности системы.

36. При разработке структурно-логической модели системы учитываются зависимости события отказа (безотказного функционирования) системы при выполнении требуемой функции (в соответствии с установленными критериями отказа системы) от возникновения следующих событий, оказывающих влияние на надёжность выполнения системой требуемой функции:

отказы (безотказное функционирование) элементов системы;

неготовность элементов системы (каналов системы, системы в целом) из-за технического обслуживания, ремонта или испытаний;

ошибки (безошибочные действия) персонала;

отказы (безотказное функционирование) обеспечивающих или управляющих систем;

ООВ;

исходное событие аварии и воздействия, возникающих при нарушениях нормальной эксплуатации, включая аварии (для функций, выполняемых при авариях), условия окружающей среды.

37. Состав отчета по анализу надежности систем АС представлен в приложении № 8 к настоящему Руководству по безопасности. Пример выполнения анализа надежности системы представлен в приложении № 9 к настоящему Руководству по безопасности.

V. Анализ надежности (функциональной безопасности) сложного технологического комплекса

38. Анализ надежности (функциональной безопасности) сложного технологического комплекса выполняется в следующем порядке:

сбор и анализ проектной и эксплуатационной информации о сложном технологическом комплексе, включая определение границ моделирования сложного технологического комплекса и состава входящих в него систем (элементов);

установление функций, важных для безопасности, выполняемых сложным технологическим комплексом и определение критериев отказа по отношению к каждой из функций;

определение и описание технологического процесса (технологических процессов), выполняемых сложным технологическим комплексом, выделение базовых интервалов;

анализ зависимости технологического комплекса от обеспечивающих и управляющих систем;

учет влияния персонала на надежность (функциональную безопасность) комплекса;

учет ООВ;

определение показателей надежности элементов (систем), входящих в сложный технологический комплекс;

построение структурно-логической модели сложного технологического комплекса и определение показателей его надежности (функциональной безопасности) по выполнению им требуемых функций;

оценка результатов анализа.

39. Сбор и анализ проектной и эксплуатационной информации о сложном технологическом комплексе осуществляется для каждой из входящих в состав указанного комплекса систем в соответствии с рекомендуемым порядком, представленным в приложении № 4 к настоящему Руководству по безопасности.

Основными источниками исходных данных о сложном технологическом комплексе являются проектная и эксплуатационная документация, опыт эксплуатации и результаты испытаний.

Для находящихся в эксплуатации сложных технологических комплексов при сборе исходных данных кроме технической документации рекомендуется также проводить ознакомление с ТП, реализуемым данным комплексом. Ознакомление с ТП на АС преследует следующие основные цели:

проверку данных, содержащихся в технической документации;

определение возможности отказов по общей причине;

уточнение порядка действий персонала по управлению ТП, выявление возможности выполнения персоналом ошибочных действий, а также факторов, оказывающих влияние на надежность выполнения персоналом действий по месту расположения оборудования.

40. При определении и описании ТП, выполняемых сложным технологическим комплексом, на основании проектной и эксплуатационной документации выделяются все технологические операции, входящие в состав указанного ТП, устанавливаются последовательность их выполнения, начальная и конечная технологические операции. Для каждой выделенной технологической операции определяется состав элементов (систем) сложного технологического комплекса, участвующих в ее выполнении, а также необходимые действия персонала АС.

41. По результатам выделения технологических операций, входящих в ТП, осуществляемый сложным технологическим комплексом, выделяются базовые интервалы, то есть части ТП, характеризующиеся постоянством условий наступления отказа сложного технологического комплекса на выполнение требуемой функции.

42. При установлении критериев отказа для сложного технологического комплекса учитывается, что комплекс может выполнять несколько требуемых функций, в частности, функцию, связанную с функционированием по прямому назначению (функция первого типа), а также функцию, связанную с предотвращением нарушений требований нормативной и (или) конструкторской документации (функция второго типа). Соответственно, для каждой из требуемых функций назначаются различные критерии отказа и проводится отдельный анализ надежности.

При выполнении требуемых функций второго типа из числа указанных выше сложный технологический комплекс считается отказавшим при нарушении установленных требований нормативной и (или) конструкторской документации даже в случае, если он сохраняет способность функционирования по прямому назначению (то есть сохраняет способность выполнения функции первого типа из указанных выше требуемых функций).

Например, при анализе надежности технологического комплекса ТТО с ядерным топливом в качестве первой функции может рассматриваться способность осуществления процесса ТТО (критерий отказа на выполнение данной требуемой функции – непредусмотренное прекращение ТТО), а в качестве второй функции – недопущение нарушения требований нормативных документов или проектной (конструкторской) документации к выполнению ТТО (например, непревышение допустимой скорости перемещения, допустимого усилия при извлечении ТВС, ненарушение требований ядерной и радиационной безопасности).

Анализ надежности сложного технологического комплекса на выполнение требуемых функций, аналогичных второй из указанных выше функций, допускается называть анализом функциональной безопасности сложного технологического комплекса.

43. При определении последствий нарушений в функционировании отдельных систем (элементов) сложного технологиче-

ского комплекса выполняется выявление возможных причинно-следственных связей, приводящих к отказу сложного технологического комплекса.

Определение последствий нарушений в работе сложного технологического комплекса рекомендуется выполнять по отдельности для каждого из выделенных базовых интервалов.

При анализе сначала определяется перечень элементов и (или) действий персонала, задействованных в выполнении ТП на каждом конкретном базовом интервале. Затем определяются характерные для рассматриваемого базового интервала нарушения ТП и выполняется анализ их последствий.

Определение последствий нарушений в работе сложного технологического комплекса выполняется с учетом работы предусмотренных в сложном технологическом комплексе защит и блокировок.

При определении последствий нарушений в работе сложного технологического комплекса учитывается, что выявляемые нарушения могут привести к отказу сложного технологического комплекса не на базовом интервале, к которому относится нарушение, а на каком-либо из последующих базовых интервалов.

Результаты определения последствий нарушений функционирования сложного технологического комплекса представляются в формате табл. № 1.

Таблица № 1

Образец представления результатов определения последствий нарушений функционирования сложного технологического комплекса

Базовый интервал	Перечень элементов (систем), действий персонала	Перечень нарушений технологического процесса	Предусмотренные защиты и блокировки	Последствия нарушения (при неработоспособности защит и блокировок)

Примечание:

В столбец «Базовый интервал» заносится перечень базовых интервалов, выделенных при определении и описании ТП.

В столбце «Перечень элементов (систем), действий персонала» указываются элементы (системы) сложного технологического комплекса, используемые для выполнения технологических операций соответствующего базового интервала, а также указываются необходимые действия персонала.

В столбце «Перечень нарушений технологического процесса» указываются нарушения ТП, возникновение которых возможно на соответствующем базовом интервале.

В столбец «Предусмотренные защиты и блокировки» заносятся защиты и блокировки, препятствующие переходу нарушения ТП в отказ сложного технологического комплекса.

В столбец «Последствия нарушения (при неработоспособности защит и блокировок)» заносится информация о последствиях, к которым могут привести выявленные нарушения технологического комплекса при неработоспособности защит и блокировок.

44. Определение причин возникновения нарушений ТП выполняется с целью установления причинно-следственных связей отказов элементов систем и ошибок персонала с нарушениями ТП.

Определение причин возникновения нарушения ТП выполняется с учетом предусмотренных в сложном технологическом комплексе защит и блокировок.

Результат определения причин возникновения нарушений ТП представляется в формате табл. № 2.

Таблица № 2

Образец представления результатов определения причин возникновения нарушений ТП

Нарушение технологического процесса	Отказы элементов (систем), ошибки персонала, приводящие к нарушению технологического процесса	Предусмотренные защиты и блокировки

45. Разрабатывается структурно-логическая модель сложного технологического комплекса, которая представляет собой последовательное (то есть с использованием логического оператора «или») соединение моделей отказа сложного технологического комплекса на отдельных базовых интервалах.

46. Рекомендуемый порядок определения показателей надежности элементов сложного технологического комплекса аналогичен порядку, представленному в главе III настоящего Руководства по безопасности.

47. Рекомендуемый порядок учета влияния персонала аналогичен рекомендуемому порядку, представленному в приложении № 5 к настоящему Руководству по безопасности.

48. Рекомендуемый порядок учёта ООВ аналогичен рекомендуемому порядку, представленному в приложении № 7 к настоящему Руководству по безопасности.

49. При построении структурно-логической модели (например, дерева отказов) сложного технологического комплекса используются результаты анализа последствий нарушений функционирования сложного технологического комплекса, выполняемого в соответствии с пунктом 43 настоящего Руководства по безопасности, а при построении структурно-логической модели (например, дерева отказов) сложного технологического комплекса на отдельных базовых интервалах - результаты анализа причин возникновения нарушений ТП, выполняемого в соответствии с пунктом 44 настоящего Руководства по безопасности.

50. Пример выполнения анализа надежности (функциональной безопасности) сложного технологического комплекса представлен в приложении № 10 к настоящему Руководству по безопасности.

VI. Особенности анализа надежности систем с пассивными элементами

51. Анализ надежности систем с учетом особенностей, излагаемых в настоящей главе, рекомендуется выполнять в отношении систем, модель надежности которых учитывает работоспособность пассивных элементов, испытывающих воздействие от эксплуатационных нагрузок, таких как собственный вес, давление рабочей среды (давление теплоносителя, топлива или масла, питательной или охлаждающей воды в трубопроводе или теплообменном агрегате, давление газа в сосуде давления, гидростатическое давление в емкости для хранения или баке запаса), температурные нагрузки и т.п., а также испытывающих воздействие аварийных и особых нагрузок (например, аварийное давление, температура, ударные нагрузки, включая гидроудар, пожарные нагрузки, аварийное давление в защитной оболочке) и нагрузок от внешних воздействий (например, инерционные нагрузки, ударные нагрузки).

52. Рекомендуется действующие эксплуатационные, особые и аварийные нагрузки объединять в режимы нагружения, которые характеризуются видом нагружения, параметрами нагружения и частотой реализации нагружения.

53. Рекомендуется при анализе надежности учитывать, что отказ пассивного элемента может быть результатом возникновения в элементе предельного напряженного состояния в результате воздействия нагрузок. Также рекомендуется учитывать, что отказ элемента может быть вызван процессами накопления повреждений, причинами которых может быть воздействие циклических нагрузок или воздействие со стороны рабочей

среды (с течением времени в процессе эксплуатации воздействие циклических нагрузок может привести к появлению и накоплению повреждений, зарождению и развитию трещин; характерными процессами при этом могут быть механическая усталость или термическая усталость).

При выполнении анализа надежности пассивных элементов рекомендуется учитывать, что воздействие со стороны рабочей среды (внутренней и внешней) с течением времени в процессе эксплуатации может также привести к процессу накопления повреждений, который может характеризоваться деградацией свойств материала, зарождением трещин и (или) выносом частиц материала рабочей средой (например, коррозия, эрозия). При этом воздействие нагрузок может ускорить или качественно изменить процесс (например, коррозия под напряжением). Процесс может привести к снижению несущей способности пассивных элементов (например, в результате уменьшения толщины стенок сосудов, трубопроводов). Это может привести к достижению предельного состояния и деградационному отказу элемента.

54. При выполнении анализа надежности пассивных элементов рекомендуется установить критерии предельного состояния элемента, а также установить, какие режимы нагружения и процессы при эксплуатации потенциально могут привести к возникновению предельных состояний по действующим напряжениям или по условиям накопления повреждений (рисунок 1).

55. Оценки вероятности отказа (безотказной работы) выполняются расчетными методами с привлечением данных о статистических характеристиках прочности материалов и данных, учитывающих потенциальный разброс характеристик режимов нагружения и воздействия среды.

56. Для оценки надежности пассивных элементов по предельным состояниям рекомендуется применять следующие расчетные методы:

метод коэффициентов запаса (модель «нагрузка-прочность»);

методы двух моментов (метод надежности первого порядка «FORM» и метод надежности второго порядка «SORM»);

методы статистического моделирования (например, метод Монте-Карло, метод Монте-Карло с выборкой по значимости, моделирование с районированной выборкой, например, метод латинского гиперкуба).

Подходы, наиболее часто применяемые при оценке надежности элементов, отказ которых обусловлен силовым действием

нагрузок, подробно описаны в литературных источниках, представленных в Приложении № 3 к настоящему Руководству по безопасности.

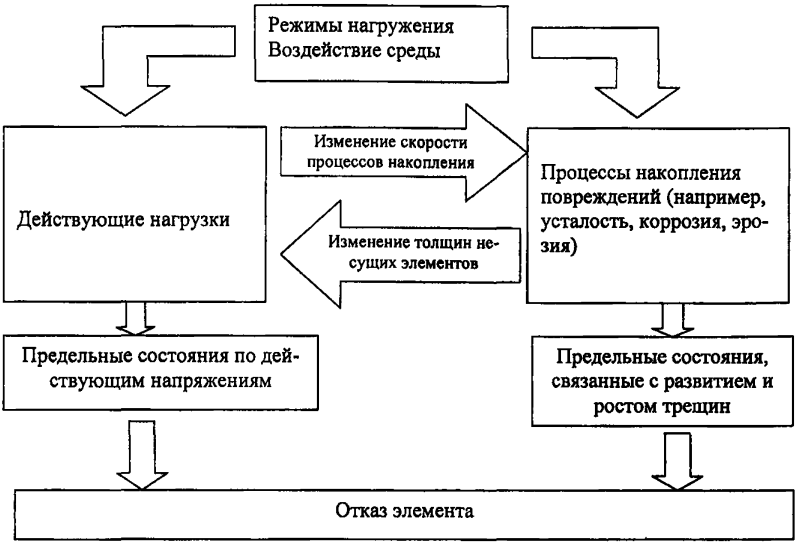


Рис. 1. Факторы, подлежащие учету при анализе надежности систем с пассивными элементами

57. Для пассивных элементов, которые находятся под воздействием циклической нагрузки и (или) влиянием воздействия рабочей среды (например, коррозии, эрозии) оценку надежности рекомендуется выполнять вероятностными методами механики разрушения с привлечением данных о характеристиках материалов. Рекомендуется также использовать статистические данные о распределении несплошностей и дефектов материалов, полученных по результатам неразрушающего контроля. Подходы по применению вероятностных методов механики разрушения к оценке надежности подробно описаны в литературных источниках, перечисленных в Приложении № 3 к настоящему Руководству по безопасности, и кратко представлены в приложении № 11 к настоящему Руководству по безопасности.

58. Рекомендуется выполнить анализ неопределенностей, целью которого является определение доверительных границ показателя надежности исследуемого элемента, для чего оценивается и используется неопределенность параметров нагрузок, прочности материалов, частоты реализации каждого режима нагружения и возможных сочетаний режимов.

VII. Особенности анализа надежности программно-технических средств

59. При анализе надежности программно-технических средств, использующих ПО, рекомендуется учитывать как возможные отказы аппаратных (технических) средств, так и отказы вследствие ошибок в ПО. Рекомендуется учитывать возможность взаимного влияния на надежность технических средств и ПО. Например, некоторые отказы ПО могут быть вызваны дефектами технических средств (сбои в работе ячеек памяти, искажение информации в каналах связи).

60. При анализе надежности технических средств рекомендуется использовать подход, описанный в главах II-IV настоящего Руководства по безопасности. При выполнении указанного анализа надежности рекомендуется учитывать возможности выявления отказов с помощью встроенных модулей самопроверки.

61. Для оценки вероятности возникновения ошибок в ПО рекомендуется использовать специализированные методы, описания и примеры применения которых представлены в приложении № 12 к настоящему Руководству по безопасности и (или) экспертные оценки.

62. Показатели надежности программно-технических средств характеризуют их способность выполнять заданные функции в соответствии с заданными требованиями в условиях отклонений в среде функционирования, вызванных различными дестабилизирующими факторами. К числу указанных факторов относятся, в частности, изменения условий работы технических средств, их отказы и сбои, изменения во входных данных, изменения в распределении ресурсов памяти.

63. При выполнении анализа надежности ПО рекомендуется разделять ошибки ПО, которые препятствуют выполнению системой требуемых функций, и ошибки, которые не влияют на выполнение системой требуемых функций.

64. При анализе надежности ПО рекомендуется рассматривать в модели два вида отказов ПО: сбои и глобальные ошибки программирования, потенциально приводящие к невыполнению требуемых функций программно-техническими средствами сразу в нескольких каналах АСУ ТП.

65. Сбои ПО вызываются невыявленными программными ошибками, которые, главным образом, влияют на организацию обмена данными. Вследствие наличия таких ошибок, ПО выдает неправильные результаты, несмотря на то, что входные данные удовлетворяют требованиям, например, из-за проблем с динамическим распределением ресурсов. При этом, хотя коренная причина отказа ПО не устраняется, и в такой же точно ситуации отказ должен повториться, точное повторение данных и, соответственно, связанного с ним отказа маловероятно. Поэтому указанная ошибка при разработке ПО проявляется в виде перемежающихся отказов, то есть сбоев, которые устраняются преимущественно автоматизированными методами (повторной инициализацией ПО).

66. Наиболее характерным последствием сбоев в функционировании ПО, которое рекомендуется рассматривать при анализе надежности, является отказ типа «несрабатывание» соответствующего технического средства. Как правило, все сбои ПО технических средств проявляются явно.

67. Если ПО, реализуемое на программируемых технических средствах, представляет собой достаточно простые программы прямого действия, то есть не происходит обмена данными с другими программными комплексами и библиотеками, то это значительно уменьшает вероятность сбоев как таковых и исключает ситуации, которые приводят к самопроизвольному генерированию выходного сигнала при отсутствии входного сигнала (то есть отказов типа «ложное срабатывание»).

68. Ошибки программирования могут приводить к отказу всего ПО по общей причине при реализации не предусмотренных при программировании конфигураций и граничных условий. Рекомендуется полагать, что такие отказы по общей причине возможны только в отношении отказов типа «несрабатывание» и приводят к отказу всех резервируемых каналов анализируемой системы, в составе которых есть аналогичные программируемые

технические средства (то есть в случае, когда резервируемые каналы не отвечают принципу разнообразия). Вероятность такого глобального отказа не может быть оценена из опыта эксплуатации и при условии соблюдения надлежащих процедур обеспечения качества на всех этапах жизненного цикла ПО может экспертно приниматься равной $1{,}0 \cdot 10^{-5}$ на требование.

ПРИЛОЖЕНИЕ № 1
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому и атомному надзору
от 28 января 2015 г. № 26

Перечень сокращений

АВР	–	автоматический ввод резерва
АС	–	атомная станция
АЭС	–	атомная электростанция
АСУ ТП	–	автоматизированная система управления технологическими процессами
БВ	–	бассейн выдержки
БИ	–	базовый интервал
БПУ	–	блочный пункт управления
КИПиА	–	контрольно-измерительные приборы и автоматика
МП	–	машина перегрузочная
ОК	–	обратный клапан
ООБ	–	отчет по обоснованию безопасности
ООВ	–	отказ общего вида
ОТВС	–	отработавшая тепловыделяющая сборка
ОЯТ	–	отработавшее ядерное топливо
ПО	–	программное обеспечение
РПУ	–	резервный пункт управления
РШ	–	рабочая штанга
СКУ	–	система контроля и управления
СКУ ПЗ	–	система контроля и управления противопожарной защитой
ТВС	–	тепловыделяющая сборка
ТВШ	–	телевизионная штанга
ТП	–	технологический процесс
ТТО	–	транспортно-технологическая операция
ТУ	–	технические условия
ТУК	–	транспортный упаковочный комплект
УГ	–	универсальное гнездо
ЧСТ	–	чехол со свежим топливом
ХОЯТ	–	хранилище отработавшего ядерного топлива

ПРИЛОЖЕНИЕ № 2
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому и атомному надзору
от 28 января 2015 г. № 26

Термины и определения

В целях настоящего Руководства по безопасности используются следующие термины и определения

Анализ надежности – анализ, выполняемый с целью определения показателей надежности системы (элемента).

Апостериорное распределение – распределение случайной величины, которое описывает конечное знание о параметре надежности после учета эксплуатационной информации по количеству и хронологии отказов системы (элемента).

Априорное распределение – распределение случайной величины, описывающей исходное знание о параметре надежности до момента получения эксплуатационной информации по количеству и хронологии отказов компонента.

Базисное событие – событие, рассматриваемое в качестве элементарного, не зависящего от наступления иных событий, рассматриваемых в анализе надежности системы.

Базовый интервал – совокупность технологических операций, характеризующаяся постоянством условий наступления отказа системы (сложного технологического комплекса).

Безотказность – способность системы (элемента) непрерывно сохранять работоспособное состояние в течение определенного календарного времени или наработки.

Вероятность безотказной работы – вероятность того, что в заданном интервале времени или в пределах заданной наработки отказ системы (элемента) не возникнет.

Вероятность отказа на требование – вероятность, с которой система (элемент) отказывает в выполнении требуемой функции, отнесенная к требованию на ее выполнение.

Внешние воздействия – воздействия характерных для площадки АС природных явлений и деятельности человека, например, землетрясения, высокий и низкий уровень наземных и подземных вод, ураганы, аварии на воздушном, водном и наземном транспорте, пожары, взрывы на прилегающих к АС объектах и т.п.

Время восстановления – продолжительность восстановления работоспособного состояния системы (элемента).

Время ремонта – суммарная продолжительность операций по восстановлению работоспособности системы (элемента).

Дефект – каждое отдельное несоответствие системы (элемента) установленным требованиям.

Зависимый отказ – отказ, обусловленный другими отказами, либо внешним воздействием.

Интенсивность отказов – условная плотность вероятности возникновения отказа системы (элемента), определяемая при условии, что до рассматриваемого момента времени отказ не возник.

Исправное состояние системы (элемента) – состояние системы (элемента), при котором она соответствует всем требованиям нормативных документов и (или) конструкторской (проектной) документации.

Испытание – периодическая поверка работоспособности системы (элемента) путем опробования от ключа управления или действия технологических защит и блокировок.

Критерий отказа – признак или совокупность признаков нарушения работоспособного состояния объекта, установленные в нормативной или проектной (конструкторской) документации.

Критический отказ – событие, при котором система (элемент) полностью утрачивают способность выполнять требуемую функцию в момент времени, когда требуется ее (его) работа.

Минимальное сечение – наименьшее сочетание событий (например, отказов элементов, ошибок персонала), приводящее к реализации события отказа системы. Минимальное сечение представляет собой логическое произведение входящих в него базисных событий, а набор минимальных сечений – логическую сумму отдельных минимальных сечений.

Надежность системы (элемента) – свойство системы (элемента) сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, а также при техническом обслуживании.

Надежность системы (элемента) является комплексным свойством, которое может включать безотказность, долговечность, ремонтопригодность и сохраняемость или определенные сочетания этих свойств. В настоящем Руководстве по безопасности надежность систем (элементов) рассматривается только в части их безотказности.

Наработка – продолжительность или объем работы системы (элемента).

Наработка может быть как непрерывной величиной (например, продолжительность работы в часах), так и целочисленной величиной (например, число рабочих циклов, число запусков).

Наработка до отказа – наработка системы (элемента) от начала эксплуатации до возникновения первого отказа.

Независимый отказ – отказ, не обусловленный другими отказами и внешними воздействиями.

Неинформативное распределение – специальный вид априорного распределения, который содержит максимально малое количество информации о параметре надежности по отношению к той информации, которая может быть получена из эксплуатации.

Нормируемый показатель надежности – показатель надежности, значение которого установлено нормативными документами и (или) конструкторской (проектной) документацией.

Обобщенное распределение – распределение случайной величины, которое описывает вариативность параметра надежности относительно более широкой популяции (генеральной совокупности), по сравнению с той группой, к которой принадлежит данный элемент..

Отказ – событие, состоящее в нарушении работоспособного состояния системы (элемента).

Отказы общего вида – разновидность отказов по общей причине, являющихся следствием человеческих ошибок при проектировании, сооружении и эксплуатации объектов или следствием неблагоприятных воздействий окружающей среды.

Отказы по общей причине – отказы систем (элементов), возникающие вследствие одного отказа или ошибки персонала, или внешнего или внутреннего воздействия, или иной внутренней причины.

Осредненный параметр потока отказов – отношение математического ожидания числа отказов восстанавливаемой системы (элемента) за конечную наработку к значению этой наработки.

Ошибка персонала – единичное непреднамеренное неправильное действие при управлении оборудованием или единичный пропуск правильного действия; или единичное непреднамеренное неправильное действие при техническом обслуживании систем и элементов АС.

Параметр потока отказов – отношение математического ожидания числа отказов восстанавливаемой системы (элемента) за достаточно малую его наработку к значению этой наработки.

Повреждение – событие, заключающееся в нарушении исправного состояния при сохранении работоспособного состояния.

Показатель надежности – количественная характеристика одного или нескольких свойств, составляющих надежность системы (элемента).

Предельное состояние – состояние системы (элемента), при котором ее (его) дальнейшая эксплуатация недопустима или нецелесообразна, либо восстановление ее (его) работоспособного состояния невозможно или нецелесообразно.

Работоспособное состояние системы (элемента) – состояние системы (элемента), при котором значения всех параметров, характеризующих способность выполнять требуемые функции, соответствуют требованиям нормативных документов и (или) конструкторской (проектной) документации.

Расчетный показатель надежности – показатель надежности, значение которого определяется расчетным методом.

Ремонт – комплекс операций по восстановлению исправности или работоспособности систем (элементов) и восстановлению ресурсов систем, элементов или их составных частей.

Ремонтопригодность – свойство системы (элемента), заключающееся в приспособленности к поддержанию и восстановлению работоспособного состояния путем технического обслуживания и ремонта.

Система – совокупность элементов, предназначенная для выполнения заданных функций.

Скрининговая оценка (вероятности ошибки персонала) – упрощенная (консервативная) оценка действий персонала, выполняемая по упрощенным моделям.

Скрытый отказ – отказ, не обнаруживаемый визуально или штатными методами и средствами контроля и диагностирования, но выявляемый при проведении технического облуживания или специальными методами диагностики.

Сложный технологический комплекс – совокупность систем (элементов), выполняющих последовательность технологических операций для реализации единого технологического процесса по заданному алгоритму, характеризующаяся тем, что показатели надежности выполнения технологическим комплексом каждой из технологических операций могут существенно отличаться друг от друга, а нормируемые показатели надежности (функциональной безопасности) устанавливаются к выполнению требуемых функций технологическим комплексом в целом.

Средняя наработка до отказа – математическое ожидание наработки системы (элемента) до первого отказа.

Средняя наработка на отказ – отношение суммарной наработки восстанавливаемой системы (элемента) к математическому ожиданию числа его отказов в течение этой наработки.

Техническое обслуживание – комплекс операций или операция по поддержанию работоспособности системы (элемента).

Технологический процесс – совокупность технологических операций, выполняемых по заданному алгоритму, каждая из которых может реализовываться как идентичными, так и различными системами, входящими в состав сложного технологического комплекса.

Требуемая функция – функция, выполнение которой проектом АС требуется от системы, либо от совокупности систем. Требуемые функции подразделяются на функции безопасности и иные функции.

Фактор ошибки – отношение 95 % квантиля случайной величины к ее медианному значению.

Функциональная безопасность – надежность (безотказность) системы (либо сложного технологического комплекса) при выполнении функции, важной для безопасности.

Функция безопасности – конкретная цель и действия, обеспечивающие ее достижение, направленные на предотвращение и ограничение последствий аварий, которые не удалось предотвратить системами нормальной эксплуатации.

Функция, важная для безопасности – требуемая функция, выполняемая системой, важной для безопасности (либо совокупностью систем, по меньшей мере, одна из которых относится к важным для безопасности), при условии, что отказ данной функции приведет к одному из следующих последствий:

к отказу функции безопасности;

к нарушению нормальной эксплуатации АС, или к препятствиям в устранении нарушений нормальной эксплуатации АС, если при этом условная вероятность перехода рассматриваемого отказа в тяжелую запроектную аварию составляет 10^{-6} или более;

к превышению установленных значений допустимых выбросов или сбросов радиоактивных веществ, либо допустимых уровней загрязненности помещений АС.

Элементы – оборудование, приборы, трубопроводы, кабели, строительные конструкции и другие изделия, обеспечивающие выполнение заданных функций самостоятельно или в составе систем и рассматриваемые в проекте в качестве структурных единиц при выполнении анализов надежности и безопасности.

Явный отказ – отказ, обнаруживаемый визуально или штатными методами и средствами контроля и диагностирования при подготовке системы (элемента) к вводу в эксплуатацию или в процессе ее (его) эксплуатации.

ПРИЛОЖЕНИЕ № 3
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому и атомному надзору
от 28 января 2015 г. № 26

**Список источников,
рекомендуемых для использования при выполнении анализа надежности**

1. Райзер В.Д. Теория надежности в строительном проектировании. - М: АСВ, 1998.
2. Болотин В.В. Прогнозирование ресурса машин и конструкций. - М: Машиностроение, 1984.
3. G.W. Hannaman., F.J.Spurgin and J.R. Fragola. Systematic Human Action Relaibility Procedure (SHARP), NP-3583, Electric Power Research Institute, 1984.
4. A.D. Swain & H.E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application, NUREG/CR-1278, US NRC, USA, 1983.
5. G.W. Hannaman et.al. Human Cognitive Reliability Model for PRA Analysis, NNUS-4531 (EPRI), Nuclear Utility Service Corp., 1984.
6. Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis NUREG/CR-5801, 1993.
7. IAEA-TECDOC-648, Procedures for Conducting Common Cause Failure analysis in probabilistic safety assessment, Safety Series, IAEA, 1992.
8. NUREG/CR-5485, Guidelines on Modeling CCFs in PSA. Prepared by A. Mosleh, D.M. Rasmuson and F.M. Marshall for USNRC, November 1998.
9. Тейер Т., Липов М., Нельсон Э. Надежность программного обеспечения. - М.: Мир, 1981.
10. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. - Ульяновск: Печатный двор, 2012.
11. Военный стандарт США. MIL-STD-2629A Procedures for Performing

Failure Mode, Effects and Criticality Analysis.

12. Г.Н. Черкесов. Надежность аппаратно-программных комплексов.- СПб: Питер, 2005.
13. Alan Wood. Software Reliability Growth Model. Technical Report 96.1, 1996.
14. Военный стандарт США. MIL-STD-756A. Моделирование и прогнозирование безотказности.
15. International Standard. Software dependability through the software life-cycle processes. Application guide. IEC-61713.
16. Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments. NUREG/CR-6901.
17. ГОСТ 27.002-89 Надежность в технике. Основные понятия, термины и определения.

ПРИЛОЖЕНИЕ № 4
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому и атомному надзору
от 28 января 2015 г. № 26

Рекомендуемый порядок сбора информации о системе и определения границ моделирования

1. Источниками исходных данных о системе для анализа надежности являются материалы проекта АС, ТУ на оборудование, пусконаладочная документация и документация об испытаниях, опыт эксплуатации, эксплуатационная документация, включая технологический регламент безопасной эксплуатации, инструкции по эксплуатации и технические описания систем, перечни защит и блокировок, схемы технологических систем.

2. Собираемые исходные данные при документировании сопровождаются ссылками на источники информации.

3. При выполнении документирования результатов сбора информации о системе используется принятое в проектной (эксплуатационной) документации название системы и ее обозначение.

4. Границы моделирования системы устанавливаются таким образом, чтобы, с одной стороны, учесть при анализе все элементы, влияющие на надежность выполнения системой требуемых функций, а с другой стороны, чтобы не допустить многократного учета одних и тех же элементов в составе разных систем.

5. Границы между системами устанавливаются по следующим критериям.

1) Для гидравлических и пневматических систем границы по рабочей среде проходят:

на напорных трубопроводах – в месте соединения напорного трубопровода данной системы с трубопроводом или сосудом другой системы (той, в которую подается среда);

на трубопроводах подачи среды из обеспечивающих систем – в месте врезки во всасывающий трубопровод данной системы напорных трубопроводов обеспечивающей системы.

Теплообменники, к которым подводится охлаждающая среда от обеспечивающих систем, включаются в состав основной системы. При

этом, если на трубопроводах подвода охлаждающей среды к теплообменнику имеется индивидуальная запорная арматура, то эти трубопроводы входят в состав основной системы вместе с этой арматурой.

2) Для систем электроснабжения граница системы электроснабжения с потребителями устанавливается по месту присоединения ввода от шины питания к выключателю потребителя. Рекомендуется при определении границы системы в месте подвода силового электропитания к электроприводным элементам (например, арматуре, насосам, компрессорам) учитывать в составе системы (элемента) - потребителя электродвигатель (соленоид) и выключатель.

3) Границы между системами электроснабжения устанавливаются по месту присоединения токопровода к секции.

4) Управляющая система, важная для безопасности, начинается с датчиков (первичных приборов) и заканчивается на выходных контактах, которые используются для управления приводом выключателя исполнительного устройства элемента.

5) Границы моделирования системы устанавливаются, как правило, в соответствии с описанием системы в проектно-конструкторской документации.

6. Подлежат учету все элементы системы, чей отказ либо неготовность способны привести к отказу данной системы или к снижению надежности ее функционирования по выполнению требуемой функции.

7. Рекомендуется включать в границы моделирования системы следующие ее элементы:

тепломеханическое оборудование: все элементы, имеющие движущиеся части (электронасосы; турбонасосы, вентиляторы, компрессоры; арматуру, в том числе ОК, и др.); водоструйные насосы, эжекторы и инжекторы; баки; сосуды, работающие под давлением (в том числе, гидроаккумуляторы, ресиверы); теплообменники; трубопроводы, по которым среда подается при выполнении требуемой функции к потребителю, а также трубопроводы, отказ которых приводит к нарушению выполнения системой требуемой функции; фильтры, в том числе фильтрующие конструкции приямков;

электротехническое оборудование, средства АСУ ТП: генераторы; дизель-генераторы; аккумуляторные батареи; инверторы; обратимые двигатели-генераторы; выпрямители; электрические шкафы, секции и сборки; трансформаторы, включая автотрансформаторы; автоматические выключатели; разъединители; ключи (переключатели), а также электронные устройства коммутации; электронные устройства СКУ (включая программируемые устройства); реле; измерительные трансформаторы (тока и напряжения); первичные приборы (датчики); вторичные приборы; электродвигатели (для случая, когда они не являются

частью иных элементов); соленоиды (шаговые исполнительные механизмы).

Приведенный перечень элементов не является исчерпывающим и уточняется применительно к анализируемой системе.

8 Границы элементов устанавливаются таким образом, чтобы, по возможности, облегчить определение показателей их надежности на основе имеющихся специфических и обобщенных данных. Установление границ элементов выполняется в соответствии с описанием элементов в проектно- конструкторской документации.

9. Границы элементов определяются таким образом, чтобы при построении модели надежности системы был обеспечен учет всех видов отказов, которые могут повлиять на способность системы выполнять требуемую функцию.

10. Границы системы и границы моделируемых элементов в документации по анализу надежности отображаются при помощи упрощенной технологической схемы (блок-схемы).

11. Собирается и документируется информация обо всех состояниях нормальной эксплуатации АС, а также состояниях, характеризующихся нарушением нормальной эксплуатации АС, при которых требуется выполнение системой своих функций.

12. Собирается и документируется информация об основных элементах системы в следующем объеме:

тип и эксплуатационное обозначение элемента;

основные технические характеристики элемента;

состояние элемента в разных режимах нормальной эксплуатации (нарушений нормальной эксплуатации);

наличие дистанционного (ручного) или автоматического управления элементом;

месторасположение элемента;

потребности элемента в энергоснабжении, охлаждении, кондиционировании воздуха и вентиляции, смазке от внешних систем, в работе других вспомогательных систем;

предельные значения параметров, от которых зависит эксплуатация элемента;

критерии предельного состояния.

13. Собирается и документируется информация о контролируемых параметрах системы, включающая измеряемые параметры, перечень защит и блокировок системы.

14. Собирается и документируется информация о связях анализируемой системы с другими системами, которые требуются для обеспечения ее работоспособности или сами зависят от нее. Подлежат учету следующие связи:

связи по энергоснабжению (электроснабжение, снабжение сжатым воздухом, снабжение топливом);

связи по охлаждению активных элементов (водой различных контуров, воздухом, маслом);

связи по вентиляции помещений, в которых размещены элементы системы;

связи с СКУ (не входящими в состав рассматриваемой системы), в которых формируются управляющие сигналы для элементов системы (включая сигналы на запуск, останов оборудования, запреты на включение/отключение, изменение положения арматуры);

связи, обусловленные зависимостью от программного обеспечения;

прочие связи, которые могут включать другие зависимости между системами (например, технологические связи по перекачиваемой среде, по подаче смазки).

Документирование информации о связях с другими системами (элементами) сопровождается таблицей (матрицей) зависимостей, в которой показываются связи этих систем (элементов) с системами (элементами) анализируемой системы.

15. Собирается и документируется информация о действиях персонала АС, которые могут повлиять на функционирование системы.

16. Собирается и документируется информация об условиях безопасной эксплуатации, сформулированных для системы. Эта информация используется для того, чтобы определить возможность реализации того или иного режима работы оборудования, конфигурации системы.

17. Собирается и документируется информация о порядке выполнения технического обслуживания, испытаний системы, в частности, данные о периодичности и объеме проверок работоспособности и плановых технических обслуживаний системы или ее элементов.

ПРИЛОЖЕНИЕ № 5
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому и атомному надзору
от 28 января 2015 г. № 26

Рекомендуемый порядок учета влияния персонала

1. Для учета влияния персонала формируется перечень действий персонала, которые могут оказать влияние на выполнение анализируемой системой требуемых функций, описывается способ моделирования этих действий и оцениваются вероятности соответствующих ошибок (безошибочных действий) персонала.

2. Учет влияния персонала АС на надежность выполнения системой требуемой функции выполняется с учетом предположения, что свои действия персонал выполняет в соответствии с требованиями эксплуатационной документации.

3. При формировании перечня действий персонала разделяются на следующие категории:

действия при подтверждении работоспособного состояния (в том числе при испытаниях), техническом обслуживании или ремонте системы (действия до выполнения системой требуемой функции);

действия персонала в процессе выполнения системой требуемой функции, приводящие к отказу системы или ее элементов;

действия при нарушениях нормального функционирования системы (корректирующие действия).

Учитываются следующие виды ошибок персонала:

ошибки выполнения (ошибки выбора);

ошибки несвоевременного выполнения (несвоевременное обнаружение, диагностирование);

ошибки невыполнения (пропуск действия).

4. Учитываются действия персонала, связанные с техническим обслуживанием системы (ее элементов), которые могут привести к неготовности системы выполнить требуемые функции.

5. Вероятности ошибок персонала оцениваются с применением специализированных методов анализа надежности персонала.

6. При определении вероятности ошибок персонала действия персонала относят к одному из типов действий (поведения) персонала:

основанные на навыке;

основанные на правилах;

основанные на знаниях.

7. Учитываются следующие факторы, влияющие на вероятность совершения ошибки персонала:

временной фактор (время, которым располагает персонал АС для выполнения тех или иных требуемых действий). Временной фактор характеризуется резервами времени, которыми персонал располагает для принятия решения о выполнении действий, а также временем, необходимым для выполнения требуемых действий;

простота/сложность требуемых действий, степень детализации требуемых действий в эксплуатационной документации;

подготовка (опыт) персонала к действиям в аналогичных ситуациях;

отработанность взаимодействия и качество обмена информацией между различными категориями персонала АС, вовлеченными в выполнение требуемых действий;

возможность контроля и восстановления (наличие возможности проверить правильность поданной команды (выполненного действия), возможности повторить действие, выполнить операцию другим способом);

уровень стресса;

степень несоответствия условий окружающей среды, при которых выполняются требуемые действия, нормальным условиям;

качество интерфейса «человек-машина» (например, удобство считывания информации с показывающих приборов, работы с органами управления);

нагрузка на персонал (дискретные (поэтапные) операции, не требующие оперативного вмешательства в ход процесса, или динамичные операции, требующие высокой концентрации внимания);

зависимости в действиях персонала (например, выполнение неправильного действия вследствие неправильного считывания информации с контрольно-измерительных приборов).

8. Учитываются зависимости в действиях персонала, влияющие на надежность персонала, в том числе:

зависимости между действиями, выполняемыми одним и тем же оператором в рамках одной задачи;

зависимости внутри группы персонала, участвующего в решении одной задачи, включая контроль ее выполнения;

зависимости между разными задачами, решаемыми персоналом в процессе управления системой.

9. Учет влияния персонала выполняется последовательно в четыре этапа.

Этап 1. Анализ исходной информации:

определение перечня действий (ошибок) персонала, оказывающих влияние на надежность выполнения анализируемой системой требуемой функции;

анализ конструкторской и эксплуатационной документации;

анализ условий выполнения действий (ошибок) персонала;

опрос персонала - непосредственных исполнителей анализируемых действий (ошибок) (по возможности).

Этап 2. Отборочный анализ:

оценка надежности персонала при техническом обслуживании системы (элементов);

оценка надежности персонала при эксплуатации системы;

оценка надежности выполнения корректирующих действий персоналом при возникновении нарушений в работе системы;

выбор наиболее важных действий для детального анализа (по результатам предварительного количественного анализа надежности системы).

Этап 3. Детальный анализ надежности персонала (выполняется при необходимости):

определение последовательности действий при выполнении каждой задачи и критичных шагов;

анализ функций персонала на каждом шаге;

построение модели действий персонала;

анализ зависимостей в действиях персонала;

определение предварительных («номинальных») значений вероятностей ошибок (безошибочных действий) персонала;

оценка относительного влияния формирующих поведение факторов;

оценка фактора восстановления и уровней зависимости;

определение показателей надежности персонала.

Этап 4. Оценка неопределенности значений вероятности ошибок персонала.

10. При предварительном анализе надежности системы, когда отсутствует конструктивная и схемная проработка оборудования, а также эксплуатационная документация, допускается проводить только отборочный анализ надежности персонала. При этом могут не рассматриваться действия персонала по предотвращению и прекращению возможных нарушений функционирования системы (корректирующие действия).

11. Для отборочного анализа используются скрининговые оценки действий персонала.

В табл. № 1 настоящего приложения представлены данные по оценкам вероятностей ошибочных действий персонала при техническом об-

служивании систем и в процессе эксплуатации, рекомендованные для отборочного анализа.

Таблица № 1

Вероятности ошибочных действий персонала при техническом обслуживании системы, а также в процессе эксплуатации (использования системы по прямому назначению) [3]

Вид действий	Тип поведения		
	Действия, основанные на навыках	Действия, основанные на правилах	Действия, основанные на знаниях
Тестирование (испытания)	$2 \cdot 10^{-3}$	$2 \cdot 10^{-2}$	—
Техническое обслуживание	$1 \cdot 10^{-2}$	$1 \cdot 10^{-2}$	$5 \cdot 10^{-2}$
Эксплуатация (использование по прямому назначению)	$3 \cdot 10^{-3}$	$3 \cdot 10^{-2}$	$1 \cdot 10^{-1}$

Для оценки вероятностей ошибок персонала при выполнении действий, вызывающих нарушения нормальной эксплуатации АС при «ручном» выполнении операций по управлению системой (элементом), также могут быть использованы значения, представленные в табл. № 1 настоящего приложения.

12. В табл. № 2 настоящего приложения представлены рекомендуемые оценки вероятностей ошибочных действий персонала при нарушениях функционирования системы, которые учитывают факторы, влияющие на надежность персонала, и могут быть использованы для отборочного анализа.

Таблица № 2

Вероятности ошибочных действий персонала при нарушениях функционирования системы [3]

Располагаемое время	Тип поведения		
	Действия, основанные на навыках	Действия, основанные на правилах	Действия, основанные на знаниях
Принятие решения			
Менее 5 минут	0,1	0,5	1,0
От 5 минут до 1часа	$1 \cdot 10^{-3}$	$3 \cdot 10^{-2}$	0,3
Более 1часа	$3 \cdot 10^{-4}$	$3 \cdot 10^{-3}$	$1 \cdot 10^{-2}$
Исполнение принятого решения			
–	$3 \cdot 10^{-3}$	$3 \cdot 10^{-2}$	0,3

13. Для оценки вероятности невыполнения определенной задачи, включающей набор действий персонала, используются следующие соотношения.

В случае, если невыполнение любого из набора действий, связанных с рассматриваемой задачей, приводит к ее невыполнению (неправильному выполнению), то результирующая вероятность ошибки персонала (Q) (для задачи в целом) определяется по формуле:

$$Q = 1 - \prod_i (1 - q_i) \quad , \tag{1}$$

где: q_i – вероятность ошибки при выполнении i-го действия.

В случае, если невыполнение задачи является следствием одновременного невыполнения каждого из набора действий, то вероятность ошибки персонала определяется по формуле:

$$Q = \prod_i q_i \tag{2}$$

14. На основе отборочного анализа и результатов предварительного количественного анализа определяется набор действий персонала, которые оказывают значимое влияние на показатели надежности системы. Далее каждый отобранный набор действий персонала разбивается на элементарные действия и анализируются возможные ошибки при выполнении этих действий, например:

неправильное диагностирование ситуации;
невыполнение инструкции для определенного действия;
ошибочное считывание показаний приборов;
ошибочный выбор органов управления оборудованием.

Для каждого из элементарных действий определяются последствия их невыполнения (неправильного выполнения) с точки зрения влияния на выполнение задачи в целом.

15. Для каждого из определенных выше элементарных действий персонала оцениваются предварительные («номинальные») значения вероятностей ошибки, которые не учитывают факторов, формирующих поведение персонала, факторов контроля и восстановления (исправления) ошибок. Для оценки предварительных значений вероятностей ошибочных действий персонала, связанных с принятием решения, используются значения, представленные в табл. № 3 настоящего приложения.

Таблица № 3

Предварительные («номинальные») значения вероятностей ошибочных действий персонала, связанных с принятием решения в зависимости от располагаемого времени [4]

Время, располагаемое на принятие решения, мин.	Вероятность ошибки при диагностике одиночного события	Вероятность ошибки при диагностике второго события	Фактор ошибки
1	1,0	-	-
10	0,1	1,0	5
20	0,01	0,5	10
30	0,001	0,1	10
60	0,0001	0,001	10
1500 (одни сутки)	0,00001	0,0001	30

В табл. № 4, 5, 6 настоящего приложения представлены справочные данные для предварительных («номинальных») значений вероятностей ошибочных действий персонала при непосредственном выполнении действий (то есть ошибочных действий, не связанных с принятием решения).

Таблица № 4

Предварительные («номинальные») значения вероятностей ошибочных действий персонала, не связанных с принятием решения

Характеристика инструкции и ситуации	Вероятность ошибки персонала	Фактор ошибки
Инструкции с обеспечением отметки о выполнении используются правильно:		
короткий список (< 10 пунктов)	0,001	3
длинный список (> 10 пунктов)	0,003	3
Инструкции без отметки об исполнении:		
короткий список (< 10 пунктов)	0,003	3
длинный список (> 10 пунктов)	0,01	3
Инструкции имеются и должны быть использованы, но не используются		
	0,05	5

Таблица № 5

Предварительные («номинальные») значения вероятностей ошибочных действий персонала, не связанных с принятием решения

Показывающий прибор или выполняемая задача	Вероятность ошибки	Фактор ошибки
Аналоговый измеритель	0,003	3
Считывание числа (4 цифры или менее)	0,001	3
Регистратор диаграмм	0,006	3
Печатающий регистратор с большим количеством параметров	0,05	5
Графики	0,01	3
Снятие показаний с индикаторных ламп, используемых как показывающий прибор	0,001	3
Определение того, что прибор, с которого считывается информация, неисправен при отсутствии индикации неисправности	0,1	5
Запись показаний: число цифр или букв, которое надо записать:		
три или менее	пренебрежимо мала	
более трех	0,001 (на символ)	3
Простые арифметические расчеты с калькулятором или без него	0,01	3
Определение неверных расчетов	0,05	5

Таблица № 6

Предварительные («номинальные») значения вероятностей ошибочных действий персонала, не связанных с принятием решения

Потенциально возможные ошибки	Вероятность ошибки персонала	Фактор ошибки
Неверный выбор органа управления на панели из группы одинаковых органов, которые:		
различаются только маркировкой	0,003	3
разбиты на четко ограниченные функциональные группы	0,001	3
являются частью наглядной мнемосхемы	0,005	10

16. К факторам, оказывающим влияние на надежность персонала, относятся уровень подготовки (квалификация) персонала, уровень нагрузки (дискретность выполняемых операций, динамичность задачи), условия взаимодействия персонала, уровень стресса. Исходя из сочетания указанных факторов, оценивается коэффициент формирующих поведение факторов как сомножитель к предварительным («номинальным») оценкам вероятностей ошибок персонала. Справочные данные для учета формирующих поведение факторов ($К_{фп}$) содержатся в литературных источниках (в частности, в источниках, перечисленных в Приложении № 3 к настоящему Руководству по безопасности). Так же в литературных источниках содержатся значения условной вероятности ($F_{к/в}$) того, что ошибка не будет проконтролирована и восстановлена в зависимости от условий контроля, наличия второго оператора или контролирующего лица, резерва времени, квалификации персонала, уровня стресса.

17. Зная время, необходимое для выполнения персоналом задачи (действия) $Т_{необх.}$, располагаемое время $Т_{расп.}$ и используя данные зависимости, можно получить вероятность ошибки персонала. На рис. 1 настоящего приложения представлена зависимость ошибки персонала от нормализованного времени, которое определяется по формуле:

$$Т_{норм.} = \frac{T_{расп.}}{T_{необх.}} \qquad (3)$$

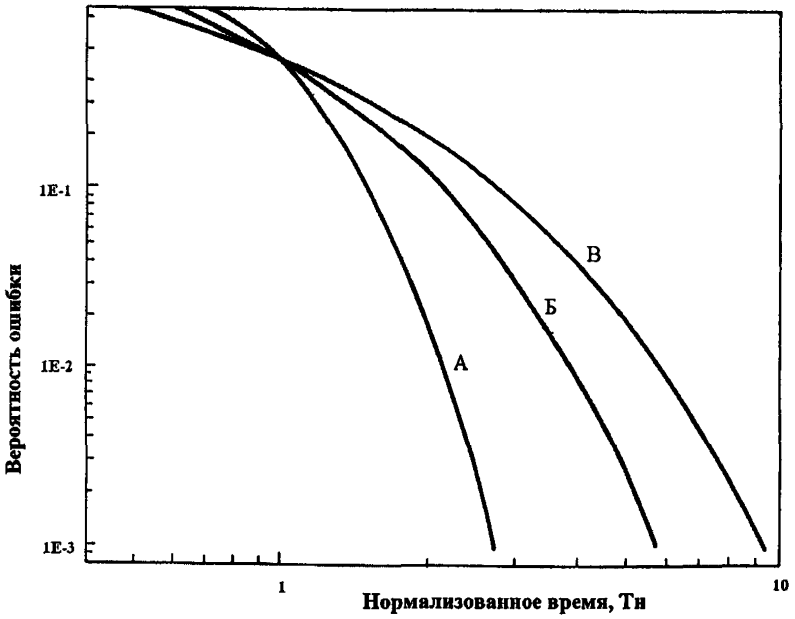


Рис. 1. Зависимости вероятности ошибки персонала от располагаемого времени и типа поведения (А – действия, основанные на навыках, Б – действия, основанные на правилах, В - действия, основанные на знаниях)

18. В тех случаях, когда любое из элементарных ошибочных действий является критичным для выполнения задачи в целом, вероятность ошибочного невыполнения задачи определяется по формуле (1) настоящего приложения. При этом в оценках вероятности ошибок персонала q_i номинальные значения корректируются с учетом формирующих поведение факторов (коэффициент $К_{фп}$) и факторов контроля и восстановления – исправления ошибок, с вероятностью невыполнения $F_{к/в}$, учитывающих зависимость вероятностей ошибок между разными действиями, выполняемыми командой операторов (либо одним оператором):

$$q_i = q_i^{ном} \cdot К_{фп} \cdot F_{к/в}. \qquad (4)$$

В отдельных случаях результирующая вероятность невыполнения задачи в целом определяется по соотношению (2) настоящего приложения как произведение вероятностей отдельных ошибочных действий, когда только сочетание всех ошибок приводит к невыполнению задачи. При более разветвленных зависимостях выполнения задачи от элементарных действий расчет результирующего показателя надежности персонала прово-

дится в соответствии со структурной моделью (например, деревом событий), специального разрабатываемой для анализа надежности персонала в рассматриваемой задаче при одновременном использовании соотношений (1) и (2) настоящего приложения.

19. Границы неопределенности для вероятностей элементарных ошибочных действий персонала задаются с помощью фактора ошибки для показателя (отношение 95 % квантиля к медиане распределения). В отношении скрининговых оценок вероятностей ошибок персонала рекомендуется использовать следующие значения фактора ошибки:

поэтапные действия (при нормальных условиях):

1) оцененная вероятность < 0,001.....10

2) оцененная вероятность 0,001 – 0,01.....3

3) оцененная вероятность > 0,01.....5

динамичные действия (в напряженных аварийных условиях):

1) оцененная вероятность < 0,001.....10

2) оцененная вероятность 0,001 – 0,1.....5

3) оцененная вероятность > 0,1.....3

Рекомендации по выбору границ неопределенности для оцененных вероятностей ошибок персонала приведены в табл. № 7 настоящего приложения.

Таблица № 7

Рекомендации по выбору границ неопределенности для оцененных вероятностей ошибок персонала

Выполняемая задача	Фактор ошибки
Выполнение оператором поэтапной операции в обычных условиях (например, проверка, техобслуживание или калибровка); уровень стресса – оптимальный	
Оцененная вероятность <0,001	10
Оцененная вероятность 0,001 – 0,01	3
Оцененная вероятность >0,01	5
Выполнение оператором поэтапной операции в ненормальных условиях; уровень стресса относительно высок	
Оцененная вероятность <0,001	10
Оцененная вероятность ≥0,001	5
Относительно динамичное взаимодействие оператора с системой индикации в обычных условиях, уровень стресса – оптимальный	
Оцененная вероятность <0,001	10
Оцененная вероятность ≥0,001	5
Относительно динамичное взаимодействие оператора с системой индикации в ненормальных условиях; уровень стресса относительно высок	10
Любая задача, выполняемая при экстремально высоком уровне стресса, например, неоднозначное состояние безопасности АС, неверно принятое предыдущее решение и недостаток времени	5

ПРИЛОЖЕНИЕ № 6
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому и атомному надзору
от 28 января 2015 г. № 26

Рекомендуемый порядок определения видов отказов и количественной оценки показателей надежности элементов АС

1. Определение видов отказов элементов.

Тепломеханическое оборудование.

Основные виды отказов тепломеханических элементов представлены в табл. № 1 настоящего приложения.

Классификация отказов механических элементов дана в отношении как критических отказов, так и повреждений. Эта классификация может варьироваться в зависимости от конкретных условий. Приведенные ниже примеры служат, в основном, для получения общего представления о предмете.

Таблица № 1

Виды отказов тепломеханических элементов

Элементы	Критические отказы	Некритические отказы
Насосы	Отказ на запуск. Отказ на перезапуск. Отказ при работе	Незначительная течь. Шум, вибрация
Запорная арматура	Отказ на открытие /закрытие. Отказ на повторное открытие / закрытие. Ложное изменение положения	Отказ контроля и индикации. Незначительная течь
Регулирующая арматура	Отказ на открытие/закрытие. Ложное изменение положения. Отказ по функции регулирования	Отказ контроля и индикации. Незначительная течь
Обратные клапаны	Отказ на открытие/закрытие. Внутренняя течь	Отказ контроля и индикации. Незначительная течь
Предохранительные или паросбросные клапаны	Ложное открытие. Отказ на открытие. Отказ на закрытие после открытия	Отказ контроля и индикации. Незначительная течь

Элементы	Критические отказы	Некритические отказы
Поглощающие стержни и приводы	Ложное введение стержня. Отказ на ввод стержня. Ложное изменение положения стержня. Ложное извлечение стержня	Незначительная течь
Теплообменники	Большая течь. Засорение. Завоздушивание	Незначительная течь
Баки	Большая течь	Незначительная течь

Электротехническое оборудование.

К критическим отказам электротехнического оборудования относятся:

1) дизель-генераторы:
отказ на запуск;
отказ при работе.
2) аккумуляторные батареи:
потеря емкости;
короткое замыкание.
3) инверторы, зарядные устройства:
отказ по функции электроснабжения.
4) электрические секции (сборки):
ложный разрыв цепи;
короткое замыкание;
короткое замыкание на землю.
5) выключатели, реле, контакторы:
отказ на разрыв цепи;
отказ на замыкание цепи;
ложное срабатывание.

В общем случае классификация видов отказов должна учитывать специфическое влияние каждого вида отказов на способность анализируемой системы выполнить требуемую функцию, а также условия их обнаружения и восстановления работоспособности.

2. Определение показателей надежности элементов системы.

Оценка интенсивности отказов.

Оценку интенсивности отказов элемента рекомендуется выполнять по следующей формуле:

$$\lambda = \frac{r}{T}, \qquad (1)$$

где:

r – зафиксированное количество отказов рассматриваемого типа (формулу рекомендуется применять при r≥10);

T – суммарная наработка, за которую было зафиксировано r отказов.

Оценка вероятности отказа на требование.

Оценку вероятности отказа на требование элемента рекомендуется выполнять по следующей формуле:

$$p = \frac{r}{D}, \qquad (2)$$

где:

r – зафиксированное количество отказов на требование рассматриваемого типа;

D – суммарное количество требований, за которое было зафиксировано r отказов.

Оценка частоты и средней длительности опробования, технического обслуживания и ремонта.

Частоту и среднюю длительность опробования, технического обслуживания и ремонта рекомендуется оценивать для отдельных элементов или каналов систем. Частоту опробования, технического обслуживания (как планового, так и непланового) и ремонта рекомендуется определять по следующей формуле:

$$\lambda_{\text{т/м}} = \frac{f_{\text{т/м}}}{T}, \qquad (3)$$

где:

$f_{\text{т/м}}$ - количество опробований обслуживаний и ремонтов, проведенных для данного элемента или канала системы;

T - суммарное время работы системы, в течение которого было проведено $f_{\text{т/м}}$ опробований, обслуживаний и ремонтов.

Среднюю длительность опробования, технического обслуживания или ремонта рекомендуется определять по формуле:

$$\bar{\tau}_{\text{т/м}} = \frac{\sum_{i=1}^{N} T_i}{f_{\text{т/м}}}, \qquad (4)$$

где:

T_i - длительность *i*-го опробования, технического обслуживания или ремонта для данного элемента или канала системы;

N – количество различных видов опробований, технических обслуживаний или ремонтов.

Оценку неготовности из-за опробования, технического обслуживания и ремонтов для элемента или канала системы рекомендуется выполнять по следующей формуле:

$$\bar{Q}_{\text{т/м}} = \lambda_{\text{т/м}} \cdot \bar{\tau}_{\text{т/м}} \qquad (5)$$

При отсутствии специфических данных для оценки параметров надежности оборудования (интенсивности отказов или вероятности отказа на требование) наиболее предпочтительно использовать данные с аналогичных АС. При этом учитываются возможные различия в определении границ и видов отказов для рассматриваемых типов элементов. Также предполагается использование других источников обобщенных данных или экспертных оценок.

Если для рассматриваемого типа элементов отказов не наблюдалось, то для определения показателей надежности элемента (интенсивности отказов или вероятности отказа элемента на требование) рекомендуется выполнять байесовское оценивание с использованием обобщенных данных согласно следующему алгоритму.

При ограниченном количестве или отсутствии обобщенных данных в качестве априорного используется неинформативное распределение. В этом случае оценку интенсивности отказов элемента рекомендуется определять по формуле:

$$\lambda = \frac{2r+1}{2T} \qquad (6)$$

При неинформативном априорном распределении оценку вероятности отказа на требование элемента рекомендуется определять по формуле:

$$p = \frac{r+0{,}5}{D+1} \qquad (7)$$

При выборе в качестве априорного логнормального распределения для выполнения байесовского оценивания рекомендуется определить стандартное отклонение логнормального распределения обобщенных данных:

$$\sigma = \frac{\ln(ef)}{z_{.95}}, \qquad (8)$$

где:

σ - параметр логнормального распределения;

ef - фактор ошибки логнормального распределения обобщенных данных;

$z_{.95}$ - 95-процентиль нормированного нормального распределения (≈1,645).

Затем рекомендуется определить дисперсию распределения обобщенных данных:

$$Var = \overline{x^2}\,(e^{\sigma^2} - 1), \tag{9}$$

где:

$\overline{x}$ - среднее значение обобщенного параметра.

Далее рекомендуется определить параметры распределения α и β.

Если байесовское оценивание выполняется для интенсивности отказов, то параметры α и β являются параметрами гамма-распределения:

$$\alpha = \frac{\overline{x}^2}{Var} \tag{10}$$

$$\beta = \frac{\overline{x}}{Var} \tag{11}$$

Если байесовское оценивание выполняется для вероятности отказов на требование, то α и β являются параметрами бета-распределения:

$$\alpha = \frac{\overline{x}^2(1-\overline{x})}{Var} - \overline{x} \tag{12}$$

$$\beta = \frac{\overline{x}(1-\overline{x})^2}{Var} - 1 + \overline{x} \tag{13}$$

Далее выполняется байесовская модификация путем вычисления параметров апостериорного распределения α' и β' по следующим формулам:

для интенсивностей отказов:

$$\alpha' = \alpha + f_T \tag{14}$$

$$\beta' = \beta + T, \tag{15}$$

где:

f_T -полное число отказов, зафиксированных для данного типа элементов;

T - полная наработка для данного типа элементов, ч.

для вероятностей отказов на требование:

$$\alpha' = \alpha + f_D \tag{16}$$

$$\beta' = \beta + D, \tag{17}$$

где:

f_D - число отказов на требование, зафиксированных для данного типа элементов;

D - полное число требований на срабатывание, зафиксированных для данного типа элементов.

Затем определяется среднее значение и дисперсия апостериорного распределения:

для интенсивности отказов:

$$\overline{x'} = \frac{\alpha'}{\beta'} \tag{18}$$

$$\overline{Var'} = \frac{\alpha'}{\beta'^2} \tag{19}$$

для вероятности отказа на требование:

$$\overline{x'} = \frac{\alpha'}{\alpha' + \beta'} \tag{20}$$

$$\overline{Var'} = \frac{\alpha'\beta'}{(\alpha' + \beta' + 1)(\alpha' + \beta')^2}, \tag{21}$$

где:

$\overline{x'}$ - апостериорное среднее;

Var' - апостериорная дисперсия.

Фактор ошибки ef' для апостериорного распределения определяется по следующей формуле:

$$ef' = exp\left[z_{.95} \sqrt{ln\left(1 + \frac{Var'}{\overline{x'}^2}\right)} \right] \tag{22}$$

ПРИЛОЖЕНИЕ № 7
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому и атомному надзору
от 28 января 2015 г. № 26

Рекомендуемый порядок учета отказов по общим причинам

1. Отказы по общим причинам систем (элементов) вследствие зависимостей от обеспечивающих и управляющих систем учитываются посредством включения обеспечивающих и управляющих систем в структурно-логическую модель анализируемой системы (в соответствии с рекомендуемым порядком, представленным в главе IV настоящего Руководства по безопасности).

2. Отказы по общим причинам вследствие ошибок персонала учитываются посредством включения в структурно-логическую модель анализируемой системы ошибок персонала, учитываемых в порядке, установленном в приложении № 5 к настоящему Руководству по безопасности.

4. Отказы по общим причинам вследствие внешних воздействий на АС природного и техногенного характера, а также вследствие воздействий, возникающих при нарушениях нормальной эксплуатации, включая аварии, учитываются посредством учета в структурно-логической модели анализируемой системы возникновения зависимых отказов элементов АС вследствие внешних воздействий природного и техногенного характера или внутренних воздействий, возникающих при нарушениях нормальной эксплуатации, включая аварии.

5. Помимо указанных в пунктах 2-4 настоящего приложения видов отказов по общим причинам в модели надежности системы учитываются также ООВ. ООВ характеризуют меру незнания возможных причин зависимых отказов и относятся к «остаточным» зависимым отказам, то есть к отказам, не моделируемым в структурно-логической модели системы непосредственно, а определяемым с помощью математических моделей, компенсирующих заниженную оценку вероятности совместного отказа нескольких резервирующих друг друга по выполняемым функциям элементов (или каналов системы).

6. Основной задачей моделирования ООВ является учет возможной корреляции потоков отказов элементов, являющихся дублирующими по

требуемым функциям системы. Учет ООВ позволяет устранить излишний оптимизм при оценке вероятности выполнения функций системами, имеющими резервирование по каналам и (или) по оборудованию.

7. Учет ООВ в модели надежности системы выполняется в пять этапов.

Этап 1. Определение групп элементов анализируемой системы, подверженных ООВ и определение соответствующих видов отказов.

Этап 2. Выбор модели ООВ и анализ данных. На этом этапе, исходя из количества элементов, входящих в группу ООВ, и имеющихся данных по опыту эксплуатации, принимается математическая модель, позволяющая вычислить вероятности ООВ для различного числа элементов. На данном этапе допускается использование консервативных моделей ООВ и обобщенных данных по параметрам моделей.

Этап 3. Выполнение количественного анализа надежности системы и определение вклада ООВ в вероятность отказа системы при выполнении ею требуемой функции. При выявлении низкой степени влияния ООВ на вероятность отказа системы выполняется этап 5, минуя этап 4.

Этап 4. Уточнение групп ООВ, корректировка моделей ООВ и уточнение параметров моделей ООВ с целью устранения консерватизма анализа.

Этап 5. Документирование результатов анализа ООВ.

8. Формирование групп элементов, подверженных ООВ, является наиболее ответственной частью анализа ООВ, так как необоснованное исключение элементов из группы ООВ может приводить к существенной недооценке вероятности отказа системы при выполнении требуемой функции. Целью формирования групп ООВ является определение всех элементов, потенциально подверженных ООВ, таким образом, чтобы возможный субъективизм был сведен к минимуму. Указанная цель достигается путем выявления всех элементов системы, потенциально подверженных ООВ.

9. В одну группу ООВ включают элементы, одновременно удовлетворяющие приведенным ниже критериям (трем обязательным критериям, и, по меньшей мере, одному необязательному):

критерий 1 (обязательный). Все элементы группы ООВ относятся к одному и тому же виду оборудования, и структурно-логическая модель надежности системы включает для всех элементов группы одни и те же виды отказа;

критерий 2 (обязательный). Единичный отказ любого из элементов, образующих группу ООВ, не приводит к отказу системы на выполнение всех требуемых функций;

критерий 3 (обязательный). Совместный отказ всех элементов, образующих группу ООВ, приводит к отказу системы на выполнение какой-либо из требуемых функций;

критерий 4 (необязательный). Элементы, включаемые в группу ООВ, имеют общего изготовителя или имеют аналогичные заводские марки (типы) разных изготовителей (общность конструкции);

критерий 5 (необязательный). На элементы, включаемые в группу ООВ, в ходе различных аварийных сценариев воздействуют одинаковые физические факторы: температура, давление, влажность, вибрация, радиоактивное, электромагнитное излучение и т.п. (не обязательно все) (общность условий функционирования);

критерий 6 (необязательный). Элементы, включаемые в группу ООВ, имеют одинаковые процедуры техобслуживания, ремонта и испытаний (общность обслуживания).

10. При формировании групп ООВ рекомендуется, по возможности, учитывать потенциальные ООВ для элементов, относящихся к различным каналам системы.

11. Для отобранных групп ООВ используют одну из следующих моделей для определения вероятности ООВ:

модель β-фактора и ее модификации [6];

модель греческих букв (Multiple Greek Letter model) [6];

модель α-фактора [7, 6, 8];

модель базового параметра [7, 6];

биномиальная модель [6].

12. Модель β-фактора.

Данная модель является наиболее консервативной и предполагает, что все элементы, включенные в группу ООВ, отказывают по общей причине с вероятностью $P_{оов}$, равной:

$$P_{оов} = \beta \cdot P, \quad (1)$$

где:

β - вероятность отказа всех элементов в группе ООВ при условии, что произошел отказ одного элемента;

P – вероятность отказа одного элемента из группы ООВ, полученная на основании опыта эксплуатации и статистики всех отказов элемента;

Соответственно, вероятность независимого отказа $P_н$ любого элемента в группе ООВ вычисляется по формуле:

$$P_н = (1-\beta)\, P \quad (2)$$

При отсутствии специфических данных рекомендуется принимать значения β в диапазоне $\beta \approx 0{,}07 - 0{,}1$.

13. Модель α –фактора.

Данная модель учитывает частичные и полные отказы элементов групп ООВ и рекомендуется как предпочтительная модель оценки вероятности событий ООВ.

$$P_k^{(m)} = \frac{m}{\binom{m}{k}} \cdot \frac{\alpha_k^{(m)}}{\alpha_T^{(m)}} \cdot P_T$$

$$\alpha_T = \sum_{k=1}^{m} k \cdot \alpha_k^{(m)} \qquad (3)$$

где:

α_k– вероятность, что в событии ООВ откажет ровно k из группы m элементов (α-фактор);

P_T – вероятность отказа одного элемента из группы ООВ, полученная на основании опыта эксплуатации и статистики всех отказов элементов;

$\binom{m}{k}$ - число сочетаний k элементов из m.

Формула (3) настоящего приложения предназначена для расчетов вероятности ООВ в случае, если проверки работоспособности оборудования, входящего в группу ООВ, осуществляются одновременно (без сдвига во времени). Если элементы, входящие в группу ООВ, проверяются со сдвигом во времени, то рекомендуется использовать формулу (4) настоящего приложения.

$$P_k^{(m)} = \frac{m}{\binom{m-1}{k-1}} \alpha_k^{(m)} \cdot P_T \qquad (4)$$

При отсутствии специфических данных рекомендуется использовать значения α-факторов, приведенных в табл. № 1 (для отказов на требование) и № 2 (для отказов при работе) [8] настоящего приложения.

Таблица № 1

Рекомендуемые значения α-факторов для отказов на требование

Размер группы ООВ	α_1	α_2	α_3	α_4	α_t
2	0,95	0,05	-	-	1,05
3	0,95	0,04	0,01	-	1,06
4	0,95	0,035	0,01	0,005	1,07
более 4	0,995	-	-	0,005	-

Таблица № 2

Рекомендуемые значения α-факторов для отказов при работе

Размер группы ООВ	α_1	α_2	α_3	α_4	α_t
2	0,975	0,025	-	-	1,025
3	0,975	0,02	0,005	-	1,03
4	0,975	0,0175	0,005	0,0025	1,035
более 4	0,9975	-	-	0,0025	-

14. Для групп ООВ, вносящих значимый вклад в оценку показателей надежности системы, рекомендуется использование модели α-фактора с реалистичными значениями α-факторов (то есть со значениями α-факторов, учитывающими, по возможности, имеющиеся специфические данные по надежности элементов). Вклад группы ООВ в оценку показателей надежности системы полагается значимым, если показатель безотказности системы с учетом вероятности возникновения ООВ элементов рассматриваемой группы отличается от показателя безотказности, рассчитанного в предположении невозможности ООВ указанных элементов более чем на 10 %.

15. ООВ включают в структурно-логическую схему анализируемой системы посредством выделения (указания) набора соответствующих базисных событий ООВ. Пример включения событий ООВ в логико-вероятностную модель системы показан графически на примере дерева отказов на рис. 1 настоящего приложения.

16. При документировании результатов учета ООВ представляется обоснование выполненного формирования групп ООВ, а также принятых моделей ООВ и их параметров.

17. Пример включения элементов в группы ООВ показаны в табл. № 3 настоящего приложения (на примере клапанов системы, схематично показанных на рис. 2 и рис. 3 настоящего приложения, отличающихся одним или несколькими признаками).

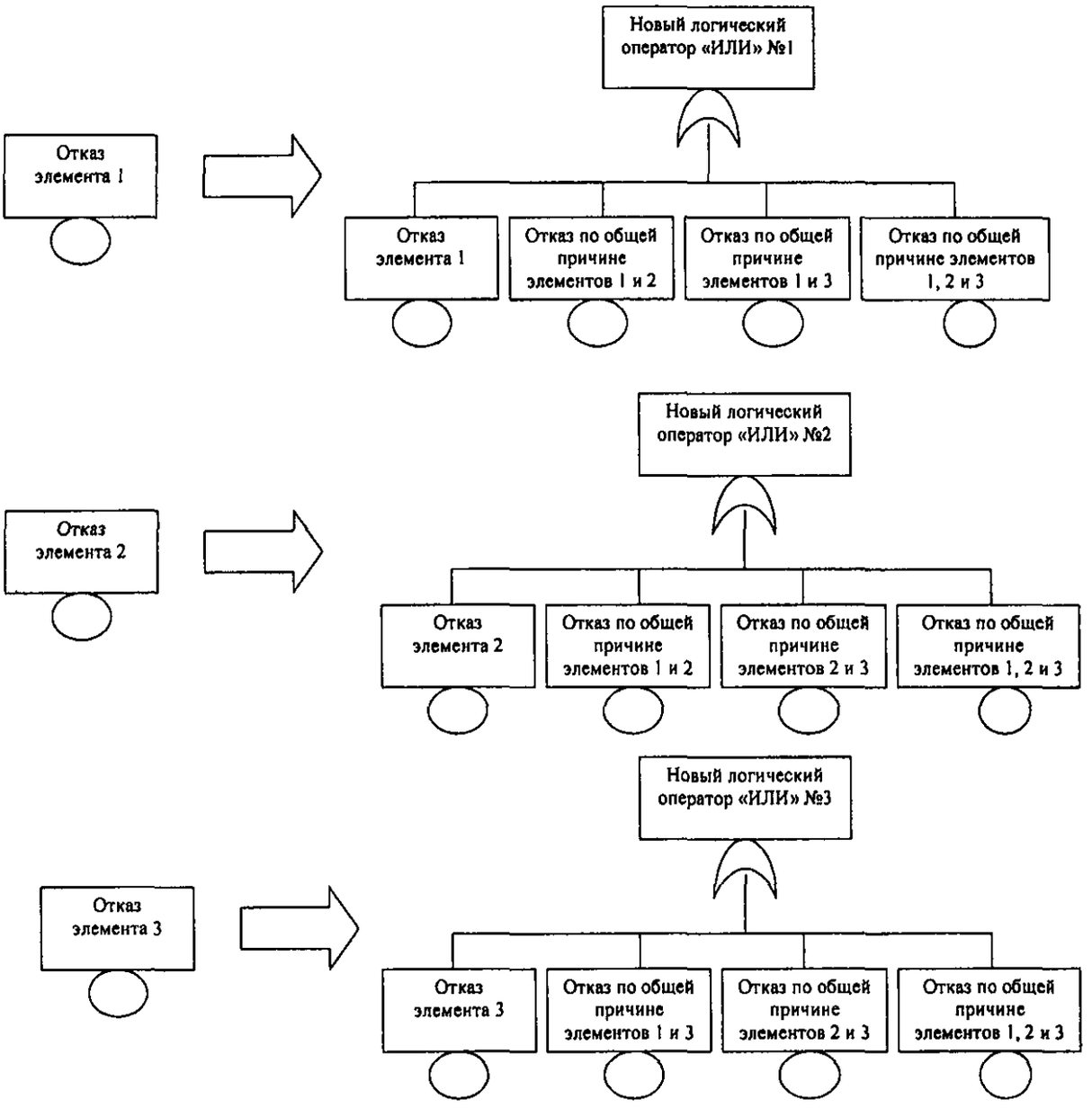
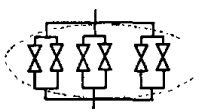
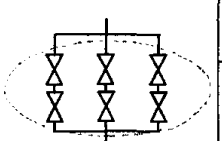
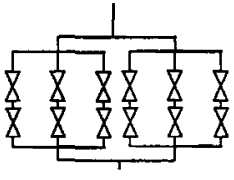


Рис 1. Пример включения ООВ в модель (дерево отказов) системы

Таблица № 3

Пример включения элементов в группы ООВ

Описание элементов	Количество элементов	Вид отказа	Интервал между опробованиями	Дополнительные условия	Рекомендованная модель	Параметры модели ООВ	Уточненные параметры модели ООВ или другие изменения модели ООВ
Система, включающая шесть клапанов, резервирующих (а) или частично (б) резервирующих друг друга (рис.2) а)  б) 	6 (Ду 100)		1 раз в месяц	Изготовлены одним производителем. Находятся в нормальных условиях в режиме ожидания	α-фактор	Основаны на обобщенных данных [8]	Не требуется
	То же		То же	Изготовлены разными производителями. Находятся в нормальных условиях в режиме ожидания	То же	То же	При высокой значимости ООВ в показателях надежности системы возможно уточнение параметров модели с целью снижения веса ООВ по причине разных производителей оборудования
	То же		3 - 1 раз в месяц 3- 1 раз в год	Изготовлены одним производителем. Находятся в нормальных условиях в режиме ожидания	α-фактор. Принимается максимальный интервал между опробованиями (1 раз в год)	То же	При высокой значимости ООВ в показателях надежности системы возможно уточнение параметров модели с целью снижения веса ООВ по причине разных тестовых интервалов
	3 (Ду 100) 3 (Ду 150)		То же	То же	То же	То же	При высокой значимости ООВ в показателях надежности системы возможно уточнение параметров модели с целью снижения веса ООВ по причине: разных тестовых интервалов; разных диаметров

Описание элементов	Количество элементов	Вид отказа	Интервал между опробованиями	Дополнительные условия	Рекомендованная модель	Параметры модели ООВ	Уточненные параметры модели ООВ или другие изменения модели ООВ
Система, включающая 12 клапанов, частично резервирующих друг друга (рис. 3) 	12 (Ду 100)	Отказ на изменение положения по требованию	1 раз в месяц	Изготовлены одним производителем. Находятся в нормальных условиях в режиме ожидания.	β-фактор	β= 0,1	При высокой значимости ООВ в показателях надежности системы возможно уточнение параметров модели с целью снижения веса ООВ. Уточнение параметров осуществляется с использованием данных по опыту эксплуатации *аналогичного оборудования* на блоках российских АЭС. Также допускается использование модели α-фактор с присвоением параметрам α_5, α_6, α_7 и α_8 значений, принятых для α_4
			6 – 1 раз в год 6 - 1 раз в год			β= 0,07	При высокой значимости ООВ в показателях надежности системы возможно: уточнение параметров модели с целью снижения веса ООВ. Уточнение параметров осуществляется с использованием данных по опыту эксплуатации аналогичного оборудования на блоках российских АЭС; использование других моделей ООВ (например, унифицированного частичного метода β-фактора) Также допускается использование модели α-фактора с присвоением параметрам α_5, α_6, α_7 и α_8 значений, принятых для α_4

ПРИЛОЖЕНИЕ № 8
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому
и атомному надзору
от 28 января 2015 г. № 26

Состав отчета по анализу надежности систем АС

Результаты анализа надежности систем АС представляются в соответствии с приведенной ниже структурой.

1. Наименование и обозначение системы.

1.1. Наименование системы.

1.2. Обозначение системы на схемах и в эксплуатационной документации АС.

1.3. Код системы, используемый в структурно-логической модели.

2. Описание системы.

2.1. Назначение системы.

2.2. Технологическая схема системы.

2.3. Краткая характеристика и состав системы.

2.3.1. Краткая характеристика системы.

2.3.2. Описание элементов системы.

2.3.3. Обеспечивающие и управляющие системы.

2.4. Функционирование системы при нормальной эксплуатации АС.

2.5. Функционирование системы при нарушениях нормальной эксплуатации АС, включая аварии.

2.6. Контроль и управление системой, включая защиты и блокировки.

2.7. Условия безопасной эксплуатации системы.

2.8. Опробования и техническое обслуживание системы.

2.9. Действия персонала по управлению и обслуживанию системы.

3. Функции и критерии отказа (успеха) системы.

3.1. Функции, выполняемые системой (функции безопасности и иные требуемые функции).

3.2. Критерии отказа (успеха) системы.

4. Определение объема моделирования системы.

4.1. Границы моделирования системы.

4.2. Исходное состояние системы.

4.3. Предположения и допущения, принятые при моделировании.

4.4. Определение границ элементов системы.

4.5. Перечень элементов системы, учитываемых при моделировании.

4.6. Виды отказов элементов, учитываемые при моделировании.

4.7. Исключенные из рассмотрения элементы.

4.8. Упрощенная схема системы.

5. Обоснование способа моделирования надежности системы.

6. Перечень и описание элементов структурно-логической модели системы.

6.1. События, связанные с отказами (безотказной работой) элементов системы.

6.2. События, связанные с неготовностью элементов системы из-за технического обслуживания, испытаний, ремонта.

7. Ошибки персонала.

7.1. Действия при техническом обслуживании, испытаниях, ремонте (действия до выполнения системой требуемой функции).

7.2. Действия в процессе выполнения системой требуемых функций.

8. Учет зависимостей и ООВ.

8.1. Учет зависимостей системы.

8.2. Учет ООВ.

9. Описание расчетной программы.

10. Количественные показатели надежности элементов системы.

11. Структурно-логические модели системы.

11.1. Структурно-логическая модель для требуемой функции № 1.

11.2. Структурно-логическая модель для требуемой функции № 2.

11.3. - 11.N. Структурно-логические модели для требуемых функций № 3 - N.

12. Результаты расчета показателей надежности системы.

13. Выводы и рекомендации по результатам анализа.

Список литературы.

Примечание: В список литературы рекомендуется включать источники, из которых были получены данные по надежности оборудования, надежности персонала, параметрам моделей ООВ и т.д.

ПРИЛОЖЕНИЕ № 9
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому
и атомному надзору
от 28 января 2015 г. № 26

Пример выполнения анализа надежности системы

1. Наименование и обозначение системы.

1.1. Наименование системы.

Вытяжная система вентиляции узла свежего топлива.

1.2. Обозначение системы на схемах и в эксплуатационной документации АС.

4KLE81

1.3. Код системы, используемый в структурно-логической модели.

KLE81

2. Описание системы.

2.1. Назначение системы.

Вытяжная система 4KLE81 предназначена для удаления воздуха из помещений хранилища свежего топлива.

2.2. Технологическая схема системы.

Принципиальная схема вытяжной системы 4KLE81 представлена на рис. 1 настоящего приложения.

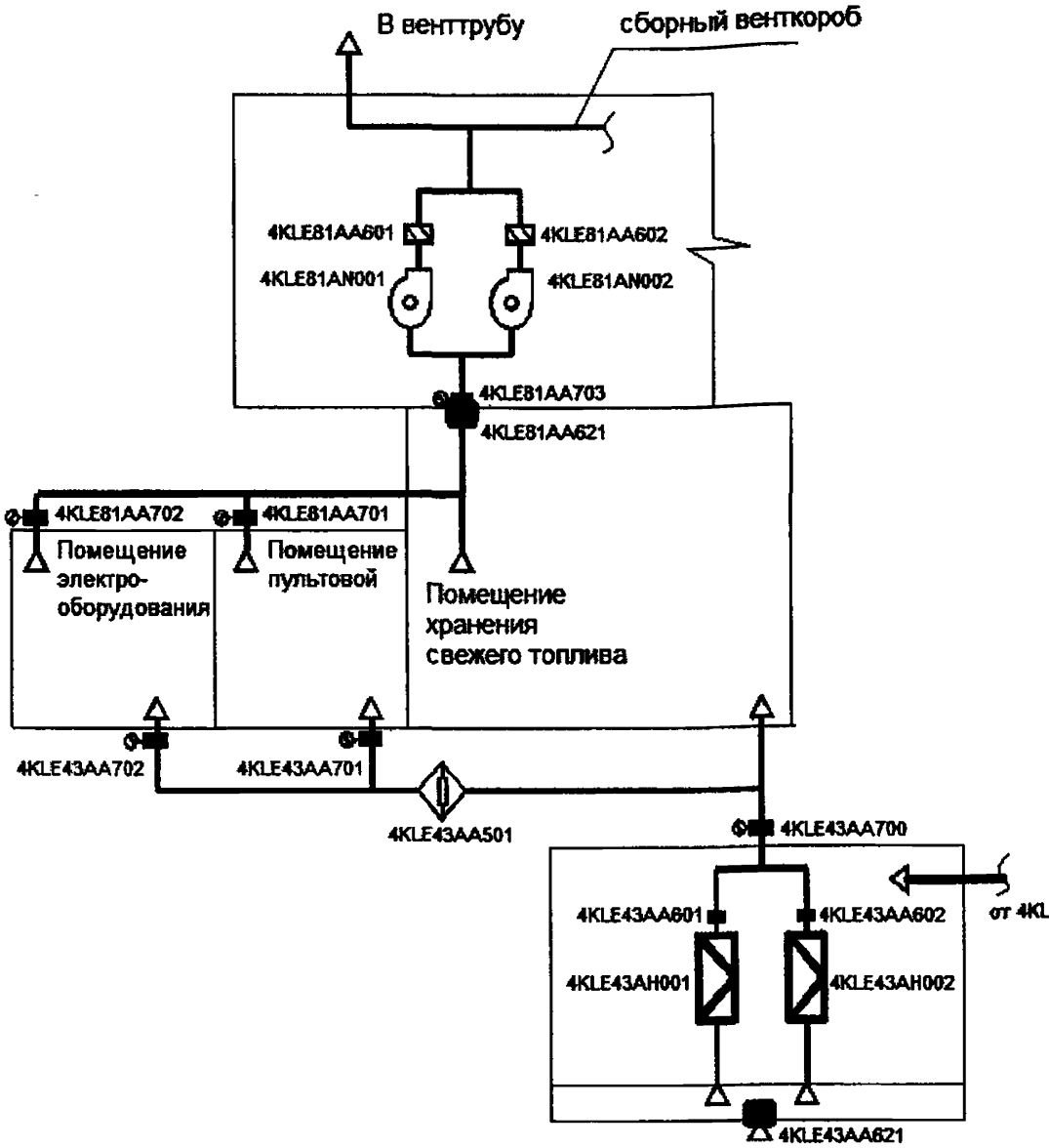


Рис. 1. Принципиальная схема вытяжной системы вентиляции помещений узла свежего топлива (4KLE81)

2.3. Краткая характеристика и состав системы.

2.3.1. Краткая характеристика системы.

Система по назначению относится к системам нормальной эксплуатации, по влиянию на безопасность – к важным для безопасности. Элементы системы относятся к 3 классу безопасности по Общим положениям обеспечения безопасности атомных станций и к I категории сейсмостойкости по Нормам проектирования сейсмостойких атомных станций.

Система имеет две требуемые функции.

Функция 1 - обеспечение (при нормальной эксплуатации АС, а также при нарушениях нормальной эксплуатации АС) направленности движения потоков воздуха из мест меньшего загрязнения в места большего загрязнения; обеспечение необходимого разрежения в узле свежего топлива.

Функция 2 - изоляция воздуховодов противопожарными клапанами по сигналу от пожарного извещателя при пожаре.

В состав вытяжной системы 4KLE81 входят рабочий и резервный вентиляторные агрегаты в комплекте с преобразователем частоты, защитное устройство для предотвращения воздействия воздушной ударной волны, противопожарные клапаны, воздуховоды.

Выброс в атмосферу вытяжного воздуха от системы 4KLE81 предусмотрен по сборному вентиляционному коробу через вентиляционную трубу, расположенную на кровле здания спецкорпуса.

Подача воздуха в периодически обслуживаемые помещения и удаление воздуха из них осуществляется непосредственно воздуховодами приточной и вытяжной систем. Количество удаляемого воздуха превышает количество приточного. При такой схеме вентиляции исключается перетекание воздуха из «грязных» помещений в «чистые».

Схема вентиляции помещений с постоянным пребыванием персонала предусматривает непосредственную подачу и удаление одинакового количества воздуха воздуховодами приточных и вытяжных систем.

В случае пожара в помещениях хранилища свежего топлива предусмотрено автоматическое закрытие противопожарных клапанов на притоке и противопожарных клапанов на вытяжке.

Технические характеристики элементов системы представлены в табл. № 1 настоящего приложения.

Таблица № 1

Технические характеристики элементов системы 4KLE81

Станционное обозначение		**Наименование, техническая характеристика**	**Количество**
элемента	помещения		
4KLE81AN001 4KLE81AN002	4UKS15251 4UKS15251	Вентилятор радиальный секционный, сейсмостойкий, специсполнения, комплектный Расход – летом 23880 м^3/час, зимой 9480 м^3/час, напор 800 Па	2
4KLE81AA601 4KLE81AA602	4UKS15251 4UKS15251	Обратные клапаны служат для отсечения от сети неработающего вентилятора	2
4KLE81AA621	4UKS	Устройство перекрытия вентиляционных каналов предназначено для защиты вентиляционного канала от воздушной ударной волны	1
4KLE81AA701 4KLE81AA702	3UKS06321 3UKS06322	Противопожарные огнезадерживающие клапаны, установленные	3

Станционное обозначение		Наименование, техническая характеристика	Количество
элемента	помещения		
4KLE81AA703	4UKS15251	на воздуховодах при пересечении ими ограждающих конструкций пожароопасных помещений и венткамер, постоянно открыты и закрываются по сигналу пожара в соответствующем помещении, отсекая его от сети воздуховодов	

Участки транзитных воздуховодов имеют огнестойкую изоляцию с пределом огнестойкости, равным пределу огнестойкости пересекаемой противопожарной преграды.

2.3.2. Описание элементов системы.

Состояние элементов системы 4KLE81 в различных режимах работы системы представлено в табл. № 2 настоящего приложения.

Таблица № 2

Состояние элементов в различных режимах работы системы 4KLE81

Наименование элемента	Станционное обозначение	Состояние		Вид отказа		Возможность восстановления	Период между опробованиями, ч	Последствия отказа
		в резерве	в работе	в резерве	в работе			
Устройство перекрытия вентиляционных каналов	4KLE81 AA621	Открыто	Открыто	–	Ложное закрытие	Да	–	Отказ системы
Клапан обратный	4KLE81 AA601 4KLE81 AA602	Закрыт	Открыт	Отказ на закрытие	-	Да	672	Отказ системы (после перехода на резервный канал)
				-	Отказ на открытие			Отказ канала системы, снижение резервирования
Клапан противопожарный на линии вытяжки из помещений	4KLE81 AA701 4KLE81 AA702 4KLE81 AA703	Открыт	Открыт	–	Ложное закрытие	Да	–	Отказ системы

Наименование элемента	Станционное обозначение	Состояние		Вид отказа		Возможность восстановления	Период между опробованиями, ч	Последствия отказа
		в резерве	в работе	в резерве	в работе			
Вентилятор	4KLE81 AN001 4KLE81 AN002	Отключен	Включен	-	Отказ на запуск Отказ при работе	Да	672	Отказ канала системы, снижение резервирования

2.3.3. Обеспечивающие и управляющие системы.

Для обеспечения выполнения анализируемой системой своих функций необходимо функционирование следующих систем:

система электроснабжения собственных нужд (функции 1 и 2);

СКУ (функция 1);

СКУ ПЗ (функция 2).

Система электроснабжения собственных нужд обеспечивает электроснабжение всех электроприводных элементов системы 4KLE81. Описание системы электроснабжения собственных нужд представлено в разделе 8.4 ООБ.

СКУ реализует необходимые блокировки для управления работой элементов системы и контроль состояния системы в процессе ее работы. Описание СКУ представлено в разделе 7.1 ООБ.

СКУ ПЗ обеспечивает электроснабжение, управление и контроль состояния противопожарных клапанов, входящих в состав системы. Описание СУ ПЗ представлено в раздел 7.7 ООБ.

Матрица зависимости элементов системы 4KLE81 от обеспечивающих и управляющих систем представлена в табл. № 3 настоящего приложения.

2.4. Функционирование системы при нормальной эксплуатации АС.

При нормальной эксплуатации АС в работе находится один вентагрегат системы 4KLE81, второй вентагрегат находится в резерве.

Таблица № 3

Матрица зависимости элементов системы 4KLE81 от обеспечивающих и управляющих систем

Наименование элемента	Станционное обозначение	Электроснабжение			Управляющий сигнал	
		~6 кВ	~0,4 кВ	=220 В	СКУ	СКУ ПЗ
Клапан противопожарный на линии подачи в по-	4KLE81AA701	-	-	Сборка 4PH12	-	+
	4KLE81AA702	-	-	Сборка 4PH13	-	+

Наименование элемента	Станционное обозначение	Электроснабжение			Управляющий сигнал	
		~6 кВ	~0,4 кВ	=220 В	СКУ	СКУ ПЗ
мещения	4KLE81AA703	-	-	Сборка 4PH14	-	+
Вентилятор	4KLE81AN001	-	Секция 4PB20	-	+	-
	4KLE81AN002	-	Секция 4PB40	-	+	-

2.5. Функционирование системы при нарушениях нормальной эксплуатации АС, включая аварии.

При нарушениях нормальной эксплуатации АС, не связанных с обесточиванием собственных нужд АС или пожаром, работа системы аналогична работе при нормальной эксплуатации.

При обесточивании собственных нужд АС система утрачивает способность выполнения функции 1 и не утрачивает способность выполнения функции 2.

При возникновении пожара по сигналу от пожарного извещателя система выполняет функцию 2.

2.6. Контроль и управление системой, включая защиты и блокировки

Управление вытяжной системой 4KLE81 осуществляется со щита управления спецкорпуса 1UKS, куда выводятся показания измеряемых параметров, сигнализация, показания состояния активных элементов систем.

При выходе из строя работающей установки включается резервная установка.

Управление противопожарными клапанами системы 4KLE81 и контроль ее состояния предусматривается от СКУ ПЗ БПУ, РПУ.

Перечень защит и блокировок системы 4KLE81 представлены в табл. № 4 настоящего приложения.

Таблица № 4

Перечень защит и блокировок системы

Номер блокировки	Наименование элемента	Условия защит и блокировок
4KLE81 Б.1	Вентилятор 4KLE81AN001 4KLE81AN002	Включение: дистанционное оператором с щита управления спецкорпуса; дистанционное оператором по месту установки; по АВР автоматическое включение резервного вентилятора по датчику давления во всасывающем коллекторе 4KLE81CP001>500 Па с задержкой 15 с

Номер блокировки	Наименование элемента	Условия защит и блокировок
		Отключение: дистанционное - оператором с щита управления спецкорпуса; дистанционное - оператором по месту установки; автоматическое - по сигналу пожара в помещении венткамеры; автоматическое - по датчику давления во всасывающем коллекторе 4KLE81CP001 > -500Па с задержкой 15 с
4KLE81 Б.2	Огнезадерживающий клапан 4KLE81AA701 4KLE81AA702 4KLE81AA703	нормально открыт: закрытие и открытие - дистанционно оператором со СКУ ПЗ БПУ, РПУ; автоматическое закрытие - по сигналу пожарного извещателя в защищаемом помещении

2.7. Условия безопасной эксплуатации системы.

В соответствии с требованиями главы 16 ООБ рассматриваемая система (по меньшей мере, один вентилятор) должна работать постоянно. Условий безопасной эксплуатации, связанных с работой системы KLE81, не установлено.

2.8. Опробования и техническое обслуживание системы.

Система 4KLE81 и ее элементы проходят проверку на соответствие проектным характеристикам после изготовления, при вводе в эксплуатацию, после ремонта и периодически в течение всего срока службы АС.

Для проверки и подтверждения проектных функций системы проводятся испытания:

проверка аэродинамических характеристик;

комплексное опробование.

Эксплуатационные испытания предусматривают контроль элементов системы с периодичностью 1 раз в 3 месяца.

Наличие резервирования позволяет проводить эксплуатационные испытания при любом состоянии нормальной эксплуатации АС без вывода системы из работоспособного состояния.

При нормальной эксплуатации АС проводится техническое обслуживание системы, которое включает в себя обслуживание арматуры и воздуховодов, а именно:

проверку внешним осмотром;

малый ремонт, профилактический ремонт, восстановление лакокрасочных покрытий, проверку прочности крепления всех элементов, состояния уплотнительных элементов.

Критерием работоспособности после проведения испытаний является соответствие параметров оборудования требованиям, приведенным в ТУ на оборудование, а также отсутствие замечаний по управлению оборудованием и арматурой от ключей управления.

Для достижения требуемого уровня готовности вентилятора, находящегося в режиме ожидания, предусматривается периодический контроль состояния элементов и переход с рабочего вентилятора на резервный 1 раз в 14 суток.

2.9. Действия персонала по управлению системой.

В системе 4KLE81 реализован принцип автоматического включения в работу резервного оборудования при отказе работающего, поэтому действий персонала по управлению системой при нахождении ее в работе не требуется.

3. Критерии отказа системы.

Функция 1 считается выполненной, если обеспечивается удаление воздуха из помещений узла свежего топлива за счет работы хотя бы одного из двух вентиляторов системы в течение 8766 часов.

Функция 2 считается выполненной при закрытии всех огнезадерживающих клапанов по сигналу от пожарного извещателя в случае возникновения пожара.

4. Определение объема моделирования системы.

4.1. Границы моделирования системы.

1) Границы по тепломеханическому оборудованию:

по напорным линиям – точки врезки в вентиляционную трубу;

по источникам подаваемой среды – вход воздуховодов в вентилируемые помещения.

2) Границы по электротехническому оборудованию:

по цепям управления - точки подключения СКУ к исполнительным механизмам. Реле входят в состав системы KLE81;

по силовому питанию вентиляторов и электроприводной арматуры - места подключения питающих кабелей к шинам питания;

по питанию схем управления и электромагнитов включения оборудования и арматуры - места подключения питающих кабелей к соответствующим шинам питания, которые не входят в состав системы KLE81.

4.2. Исходное состояние системы.

Принимаются следующие допущения относительно исходного состояния системы:

вентилятор KLE81AN001 в работе;

вентилятор KLE81AN002 в состоянии ожидания;

обратный клапан KLE81AA601 открыт;

обратный клапан KLE81AA602 закрыт;

противопожарные клапаны KLE81AA701…703 открыты.

4.3. Предположения и допущения, принятые при моделировании.

При моделировании системы приняты следующие предположения и допущения:

не рассматриваются ООВ электроприводной арматуры на сохранение положения;

учитывается возможность нахождения резервных элементов системы во внеплановом ремонте;

отказы, повышающие надежность выполнения функции, не моделируются;

не моделируются комбинации отказов на изменение положения арматуры и на сохранение положения той же арматуры;

не учитывается быстрое восстановление отказавших элементов, не имеющих резерва.

4.4. Определение границ элементов системы.

Границы для рассматриваемых в настоящем анализе элементов системы были определены следующим образом:

вентилятор включает в себя механическую часть, электродвигатель, муфту или редуктор, схему питания электродвигателя, выключатель, СКУ;

электроприводная арматура включает в себя механическую часть, электропривод, выключатель, СКУ;

выключатель включает в себя исполнительную часть, привод, передаточный механизм, схему питания привода, изоляцию, дугогасительную камеру, цепи управления выключателя;

остальное электротехническое оборудование и КИПиА - границами элемента являются входные и выходные контакты.

4.5. Перечень элементов системы, учитываемых при моделировании.

В структурно-логической модели системы учитываются элементы системы, указанные в табл. № 5 настоящего приложения.

Таблица № 5

Перечень элементов системы, учитываемых при моделировании

Наименование элемента	**Станционное обозначение**	**Функция системы, при моделировании которой учитывается элемент**
Клапан обратный	4KLE81AA601 4KLE81AA602	Функция 1
Клапан противопожарный на линии вытяжки из помещений	4KLE81AA701 4KLE81AA702 4KLE81AA703	Функция 1

Наименование элемента	Станционное обозначение	Функция системы, при моделировании которой учитывается элемент
Вентилятор	4KLE81AN001 4KLE81AN002	Функция 2

4.6. Виды отказов элементов, учитываемых при моделировании.

В структурно-логических моделях системы учитываются виды отказов элементов системы, представленные в табл. № 6 настоящего приложения.

Таблица № 6

Виды отказов элементов системы

Элемент	Критические отказы	Функция системы, при моделировании которой учитывается вид отказа
Вентилятор	1) Отказ на включение или недостижение рабочих параметров при включении (отказ на запуск) 2) Отказ при работе	Функция 1
Клапан обратный	Отказ на открытие/закрытие	Функция 1
Клапан противопожарный на линии вытяжки из помещений	Несанкционированное (ложное) закрытие	Функция 1
	Отказ на закрытие	Функция 2

4.7. Исключенные из рассмотрения элементы системы.

Из рассмотрения исключены следующие элементы системы:

вся арматура, не влияющая на работу системы при изменении своего положения, поэтому в данном анализе приведены только упрощенные фрагменты технологической схемы системы KLE81;

устройства перекрытия вентиляционных каналов 4KLE81AA621 как пассивные элементы, срабатывающие только при внешнем воздействии.

4.8. Упрощенная схема системы.

Упрощенная технологическая схема системы KLE81 приведена на рис. 2 настоящего приложения. На схеме показаны только те элементы системы, которые рассматриваются в анализе надежности системы (включены в границы моделирования).

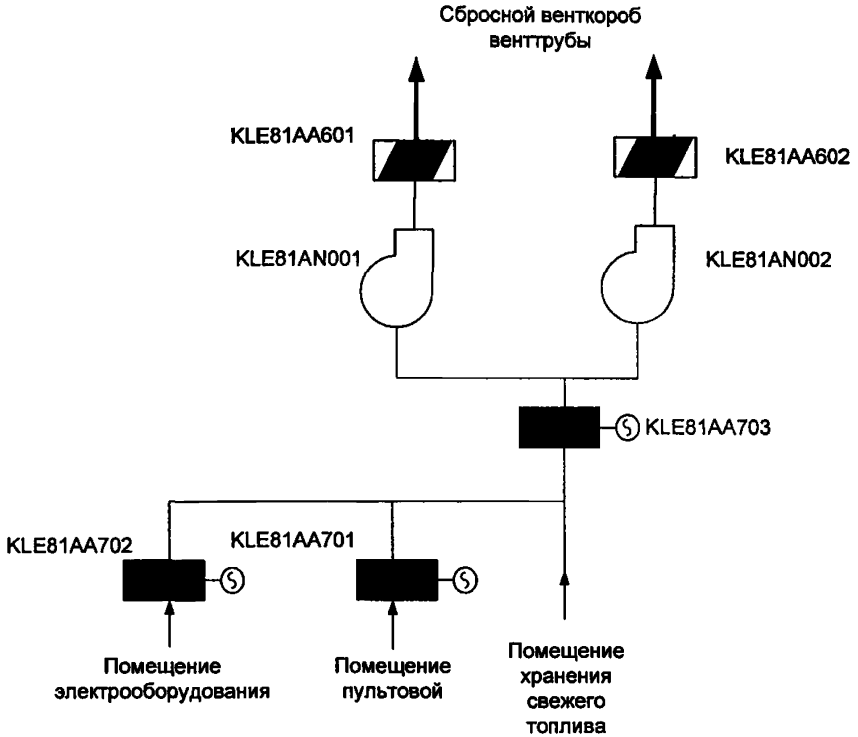


Рис. 2. Упрощенная схема системы вентиляции 4KLE81

5. Обоснование способа моделирования надежности системы.

Отказ системы моделируется при помощи разработки дерева отказов, так как для данной системы невозможно выделить один характерный доминантный отказ и, соответственно, для разработки модели отказа системы целесообразна разработка графа.

6. Перечень и описание элементов структурно-логической модели системы.

6.1. Базисные события, связанные с отказами элементов системы.

Перечень базисных событий, связанных с отказами элементов приведен в табл. № 7 настоящего приложения.

Таблица № 7

Перечень базисных событий, связанных с отказами элементов

Элемент и его идентификатор	Параметры отказа			Временные характеристики работы элемента		Модель отказа
	Тип отказа	Идентификатор базисного события	Параметр надежности (в соответствии с таблицей № 10 настоящего приложения)	Требуемое время работы, ч	Периодичность опробований, ч	
Клапан обратный на линии рабочего вентилятора 4KLE81AA601	Отказ на закрытие (при отказе рабочего вентилятора)	KLE81AA601VCC	FR-VCC-A	-	672	Периодически тестируемый элемент
Клапан обратный на линии резервного вентилятора 4KLE81AA602	Отказ на открытие	KLE81AA602VCO	FR-VCO-A	-	672	Периодически тестируемый элемент
Клапан противопожарный на линии вытяжки из помещений 4KLE81AA701 4KLE81AA702 4KLE81AA703	Ложное закрытие	KLE81AA701VMU KLE81AA702VMU KLE81AA703VMU	FR-VMU-F	8766	-	Вероятность отказа пропорциональна наработке
	Отказ на закрытие	KLE81AA701VMC KLE81AA702VMC KLE81AA703VMC	FR-VMC-F	-	8766	Периодически тестируемый элемент
Рабочий вентилятор 4KLE81AN001	Отказ при работе	KLE81AN001FAR	FR-FAR	8766	-	Вероятность отказа пропорциональна наработке
Резервный вентилятор 4KLE81AN002	Отказ на запуск	KLE81AN002FAS	FR-FAS	-	672	Периодически тестируемый элемент
	Отказ при работе	KLE81AN002FAR	FR-FAR	8766	-	Вероятность отказа пропорциональна наработке

6.2. Базисные события, связанные с неготовностью элементов системы из-за технического обслуживания, испытаний, ремонта.

Испытания и техническое обслуживание системы и ее элементов не сказываются на готовности системы выполнять свои функции.

Вероятность неготовности элемента (P_{UMT}) из-за вывода во внеплановый ремонт вследствие отказа на запуск при вводе в работу из резерва

равна произведению вероятности отказа на запуск (Q) и отношения времени восстановления (TR) к времени нахождения в резерве ($T_{рез}$):

$$P_{UMT} = Q \cdot \frac{TR}{T_{рез}}, \quad (1)$$

Если задана интенсивность отказа на запуск, то вероятность отказа на запуск при плановом вводе в работу из резерва равна произведению интенсивности отказа (λ) и интервала между опробованиями (T_i):

$$Q = \lambda \cdot T_i, \quad (2)$$

Таким образом, вероятность неготовности равна:

$$P_{UMT} = \lambda \cdot T_i \cdot \frac{TR}{T_{рез}} = \lambda \cdot TR \cdot \frac{T_i}{T_{рез}} \quad (3)$$

Время нахождения в резерве для элементов системы KLE81 составляет две недели из четырех. Таким образом, вероятность нахождения элементов системы KLE81 во внеплановом ремонте вследствие отказов на запуск равна:

$$P_{UMT} = \lambda \cdot TR \cdot \frac{T_i}{1/2 T_i} = 2 \cdot \lambda \cdot TR \quad (4)$$

Неготовность вентилятора системы равна сумме неготовностей отдельных элементов линии вентилятора систем.

Подставляя в формулу (4) интенсивность отказов и время восстановления элементов, учитываемые при расчете неготовности вентилятора из-за вывода во внеплановый ремонт, получаем:

$$P_{UMT_VENT} = 2 \cdot \left(FR_{FAS} \cdot TR_{FAN} + FR_{VCO} \cdot TR_{VC} + FR_{VCC} \cdot TR_{VC}\right), \quad (5)$$

где:

FR_{FAS} – интенсивность отказа при пуске вентилятора;

FR_{VCC} – интенсивность отказа на закрытие ОК;

FR_{VCO} – интенсивность отказа на открытие ОК;

TR_{FAN} – время восстановления вентилятора;

TR_{VC} – время восстановления ОК.

В табл. № 8 настоящего приложения приведены значения времени восстановления и интенсивности отказов для базисных событий, связанных с неготовностью элементов линии резервного вентилятора 4KLE81AN002 из-за вывода во внеплановый ремонт.

Таблица № 8

Значения времени восстановления и интенсивности отказов для базисных событий, связанных с неготовностью элементов линии резервного вентилятора 4KLE81AN002 из-за вывода во внеплановый ремонт

Базисное событие	Интенсивность отказа (FR), 1/ч	Время восстановления (TR), ч	Неготовность, связанная с отказом
KLE81AN002FAS	$1{,}0 \cdot 10^{-5}$	10	$2{,}00 \cdot 10^{-4}$
KLE81AA602VCO	$1{,}2 \cdot 10^{-6}$	6	$1{,}44 \cdot 10^{-5}$
KLE81AA602VCC	$1{,}2 \cdot 10^{-6}$	6	$1{,}44 \cdot 10^{-5}$
Суммарная неготовность резервного вентилятора:			$2{,}29 \cdot 10^{-4}$

В данном анализе рассматривается одно базисное событие «Неготовность KLE81AN002 из-за вывода во внеплановый ремонт», оно приведено в табл. № 9 настоящего приложения.

Таблица № 9

Перечень базисных событий, связанных с неготовностью элементов системы KLE81 из-за вывода во внеплановый ремонт

Событие	Модель	Значение	Обозначение в дереве отказов
Неготовность KLE81AN002 из-за вывода во внеплановый ремонт	Непосредственно назначаемая вероятность	$2{,}29 \cdot 10^{-4}$	KLE81AN002_____M

7. Ошибки персонала.

7.1. Действия при техническом обслуживании (действия до выполнения системой требуемой функции).

Необнаруживаемые до поступления требования на срабатывание ошибки персонала, связанные с техническим обслуживанием и ремонтом элементов системы, уже учтены в данных по надежности элементов системы. Отдельного их учета в модели системы не требуется.

7.2. Действия в процессе выполнения системой требуемых функций.

Управление системой в процессе выполнения ею требуемых функций не осуществляется, вследствие чего учет действий персонала при управлении системой не производится.

8. Учет зависимостей и ООВ.

8.1. Учет зависимостей.

Матрица зависимости элементов системы KLE81 от обеспечивающих и управляющих систем приведена в табл. № 3 настоящего приложения.

8.2. Учет ООВ.

При формировании групп ООВ учитывались отказы элементов, отвечающих критериям 1-3 в соответствии с пунктом 8 приложения № 5 к настоящему Руководству по безопасности, а также отвечающим одному из следующих требований:

элементы, входящие в группу ООВ, имеют общего изготовителя;

элементы, входящие в группу ООВ, имеют общую процедуру технического обслуживания и ремонта;

элементы, входящие в группу ООВ, характеризуются общностью расположения.

Образована группа ООВ из двух вентиляторов при выполнении функции 1 по критериям общности изготовителя и общности процедур технического обслуживания и ремонта. Для расчетов вероятностей ООВ применена модель β-фактора со значением параметра модели 0,1. При выполнении функции 2 ООВ не моделируются вследствие отсутствия резервируемых по выполняемым функциям элементов.

9. Описание расчетной программы.

Моделирование и расчет надежности системы выполнялись с помощью программы Risk Spectrum. Программа аттестована для применения в области вероятностного анализа риска и надежности методом деревьев отказов и деревьев событий (аттестационный паспорт №159 от 28 марта 2003 г.)

10. Количественные показатели надежности элементов системы.

10.1. Параметры надежности элементов системы.

В связи с отсутствием специфических данных по надежности, использовались обобщенные данные из зарубежных источников, а также данные по надежности оборудования АЭС с реакторами типа ВВЭР-1000.

Количественные показатели надежности элементов системы KLE81 представлены в табл. № 10 настоящего приложения.

11. Структурно-логические модели системы.

11.1. Деревья отказов системы на выполнение функции 1.

Структурно-логическая модель (дерево отказов) системы на выполнение функции 1 представлена на рис. 3 настоящего приложения.

Таблица № 10

Количественные показатели надежности элементов системы KLE81

Вид элемента	Идентификатор параметра в модели	Тип параметра	Значение параметра
Вентилятор	FR-FAS	Интенсивность отказа при пуске, 1/ч	$1{,}0 \cdot 10^{-5}$
Вентилятор	FR-FAR	Интенсивность отказа при работе, 1/ч	$3{,}8 \cdot 10^{-5}$
Вентилятор	TR-FAN	Время восстановления, ч	24
Вентилятор	T_i	Интервал опробований, ч	672
Клапан обратный	FR-VCO-A	Интенсивность отказов на открытие, 1/ч	$1{,}2 \cdot 10^{-6}$
Клапан обратный	FR-VCC-A	Интенсивность отказов на закрытие, 1/ч	$1{,}2 \cdot 10^{-6}$
Клапан обратный	TR-VC-A	Время восстановления, ч	6
Клапан противопожарный	FR-VMC-F	Интенсивность отказов на закрытие, 1/ч	$2 \cdot 10^{-6}$
Клапан противопожарный	FR-VMU-F	Ложное закрытие	$4{,}8 \cdot 10^{-8}$

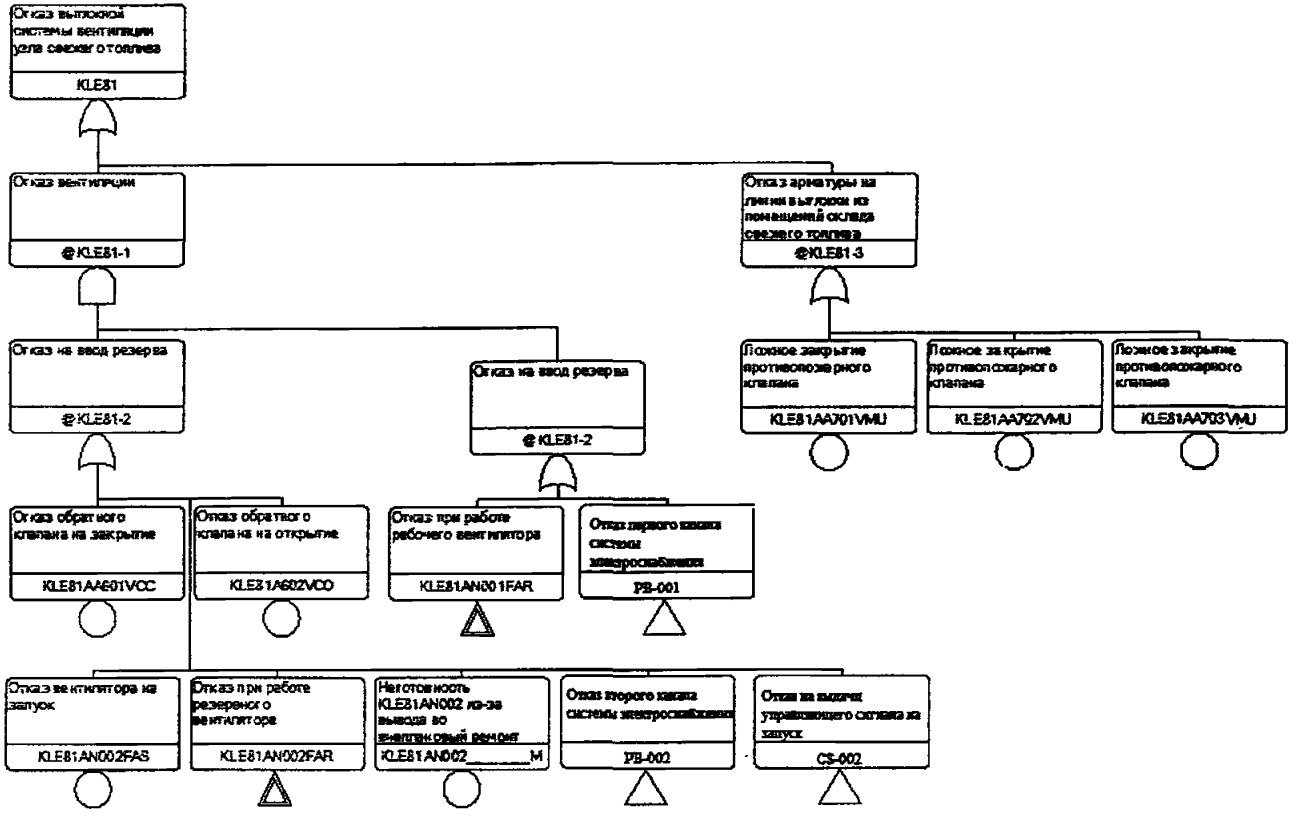


Рисунок 3. Дерево отказов «Отказ системы KLE81 на выполнение функции по удалению воздуха из узла свежего топлива» (кружком обозначены базисные события, не входящие в группы ООВ, двойным треугольником – базисные события, входящие в группу ООВ, треугольником – ссылки на модели надежности обеспечивающих и управляющих систем)

11.2. Деревья отказов системы на выполнение функции 2.

Структурно-логическая модель (дерево отказов) системы на выполнение функции 2 представлена на рис. 4 настоящего приложения.

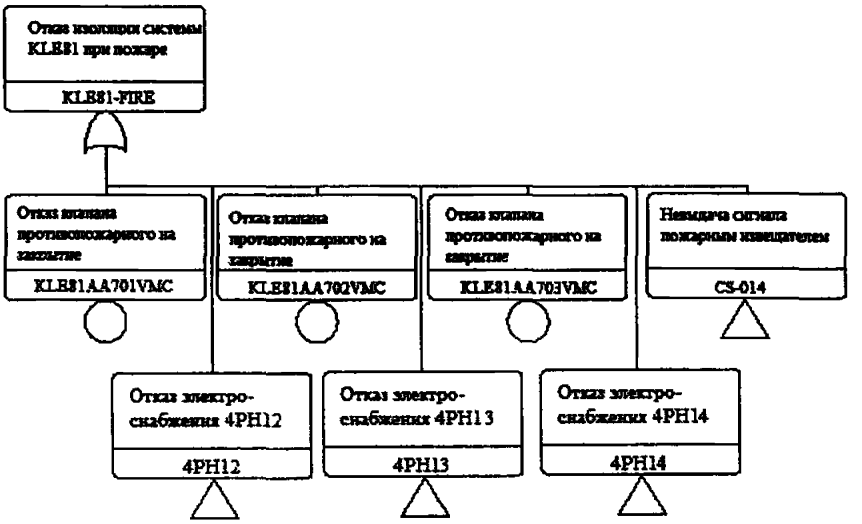


Рис. 4. Дерево отказов «Отказ на изоляцию системы KLE81 при пожаре» (обозначения аналогичны рис. 3)

12. Результаты расчета показателей надежности системы.

12.1. Результаты расчета безотказности системы для требуемой функции «Удаление воздуха из помещений узла свежего топлива».

Расчеты вероятности невыполнения функции проводились с использованием критерия отбрасывания $1{,}0 \cdot 10^{-15}$.

Оцененное среднее значение вероятности отказа системы на выполнение требуемой функции составило $2{,}76 \cdot 10^{-3}$.

Доминирующие минимальные сечения отказов приведены в табл. № 11 настоящего приложения.

Таблица № 11

Доминирующие минимальные сечения отказа на выполнение системой KLE81 функции 1

Вероятность	Вклад, %	Базисные события	Описание
$9,5 \cdot 10^{-4}$	34,4	KLE81AN001FAR	Отказ рабочего вентилятора при работе
		KLE81AN002FAS	Отказ резервного вентилятора на запуск
$4,21 \cdot 10^{-4}$	15,2	KLE81AA701VMU	Несанкционированное закрытие противопожарного клапана
$4,21 \cdot 10^{-4}$	15,2	KLE81AA703VMU	Несанкционированное закрытие противопожарного клапана
$4,21 \cdot 10^{-4}$	15,2	KLE81AA702VMU	Несанкционированное закрытие противопожарного клапана
$2,58 \cdot 10^{-4}$	9,36	KLE81AN001FAR	Отказ рабочего вентилятора при работе (в том числе по общей причине)
		KLE81AN002FAR	Отказ резервного вентилятора при работе (в том числе по общей причине)
$1,14 \cdot 10^{-4}$	4,14	KLE81AN001FAR	Отказ рабочего вентилятора при работе
		KLE81AA602VCO	Отказ на открытие ОК
$1,14 \cdot 10^{-4}$	4,14	KLE81AN001FAR	Отказ рабочего вентилятора при работе
		KLE81AA601VCC	Отказ на закрытие ОК
$6,49 \cdot 10^{-5}$	2,35	KLE81AN001FAR	Отказ рабочего вентилятора при работе
		KLE81AN002____M	Неготовность KLE81AN002 из-за вывода во внеплановый ремонт
$1,38 \cdot 10^{-5}$	0,51	PB001	Отказ первого канала системы электроснабжения
		PB002	Отказ второго канала системы электроснабжения

12.2. Результаты расчета безотказности системы для требуемой функции «Изоляция системы KLE81 при пожаре».

Расчеты вероятности невыполнения требуемой функции проводились с использованием критерия отбрасывания $1{,}0 \cdot 10^{-15}$.

Оцененное среднее значение вероятности отказа системы на выполнение требуемой функции составило $1{,}05 \cdot 10^{-3}$.

Доминирующие минимальные сечения отказов (имеющие вклад более 1 % в порядке убывания вероятности реализации) приведены в табл. № 12 настоящего приложения.

Таблица № 12

Доминирующие минимальные сечения отказа на выполнение системой KLE81 функции 2

Вероятность	Вклад, %	Базисные события	Описание
$2 \cdot 10^{-4}$	19	PH12	Отказ системы электроснабжения противопожарного клапана
$2 \cdot 10^{-4}$	19	PH13	Отказ системы электроснабжения противопожарного клапана
$2 \cdot 10^{-4}$	19	PH14	Отказ системы электроснабжения противопожарного клапана
$1{,}1 \cdot 10^{-4}$	10,5	KLE81AA701VMC	Незакрытие противопожарного клапана
$1{,}1 \cdot 10^{-4}$	10,5	KLE81AA702VMC	Незакрытие противопожарного клапана
$1{,}1 \cdot 10^{-4}$	10,5	KLE81AA703VMC	Незакрытие противопожарного клапана

13. Выводы и рекомендации по результатам анализа надежности.

Для системы не установлены нормируемые показатели надежности, в связи с чем сравнение с ними результатов анализа надежности не осуществляется.

Рекомендуется рассмотреть вопрос по снижению влияния событий с несанкционированным закрытием противопожарных клапанов на выполнение системой функции 1.

14. Список литературы.

Приводится список использованной литературы.

ПРИЛОЖЕНИЕ № 10
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому и атомному надзору
от 28 января 2015 г. № 26

Пример выполнения анализа надежности (функциональной безопасности) сложного технологического комплекса транспортно-технологических операций с ядерным топливом

1. Описание сложного технологического комплекса ТТО с ядерным топливом.

Свежее ядерное топливо поступает на блок АЭС с реактором ВВЭР-1000 в чехле для свежего топлива. На блоке АЭС чехол с ТВС извлекается из внутристанционной тележки полярным краном, оборудованным захватом чехла типа 1. Чехол устанавливается на пол в реакторном отделении, где с него полярным краном снимается крышка. После снятия крышки чехол помещается полярным краном на ступеньку БВ, для этого кран оборудуется сначала захватом чехла типа 1, а затем захватом чехла типа 2, и чехол перемещается со ступеньки БВ в УГ колодца БВ.

Колодец БВ заполняется водой, и все дальнейшие операции с ТВС производятся под водой. Операцию перестановки ТВС из чехла в стеллажи БВ, из стеллажей БВ в реактор и перестановку ОТВС из реактора в стеллажи БВ выполняет МП.

Транспортирование ОТВС из БВ в пристанционное ХОЯТ осуществляется в ТУК.

Для транспортирования ТУК с ХОЯТ на блок АЭС и обратно используется платформа внутристанционная, на которую ТУК устанавливается краном ХОЯТ, оборудованным траверсой. На блоке АЭС ТУК извлекается из платформы внутристанционной полярным краном, оборудованным траверсой. ТУК устанавливается на пол в реакторном отделении, где с него полярным краном, оборудованным захватом, снимаются крышки № 1 и № 2. Полярным краном, оборудованным траверсой, ТУК устанавливается в УГ колодца БВ. Перед тем, как производить перегрузочные работы с ОТВС, колодец БВ заполняется водой. Операцию установки ОТВС из стеллажей БВ в ТУК выполняет МП.

Крышка № 2 устанавливается в ТУК полярным краном. Для этого используется захват крышки контейнера. ТУК находится в УГ БВ, запол-

ненном водой. После того, как установлена крышка № 2, производится слив воды из колодца БВ и извлечение ТУК полярным краном, оборудованным траверсой. Далее производится дезактивация ТУК и установка полярным краном оборудованным захватом №1 крышки №1 в ТУК. Полярным краном, оборудованным траверсой, ТУК устанавливается на платформу внутристанционную. На платформе внутристанционной осуществляется транспортировка ТУК с блока АС в ХОЯТ АЭС.

2. *Определение границ моделирования сложного технологического комплекса.*

В состав сложного технологического комплекса, обеспечивающего выполнение ТТО по перегрузке ядерного топлива, входят следующие системы:

полярный кран (кран мостовой электрический специальный кругового действия грузоподъемностью 320+160/2х70т пролетом 43м) с захватами и траверсой;

перегрузочная машина МП-1000;

платформа внутристанционная;

ТУК.

3. Описание систем, входящих в сложный технологический комплекс.

3.1 Полярный кран.

Полярный кран устанавливается в здании реакторного отделения АЭС с реактором типа ВВЭР-1000, предназначен для выполнения ТТО по перегрузке топлива, ревизии реактора и т.д.

Конструктивно основой полярного крана является мост, состоящий из двух главных балок, соединенных двумя поперечными концевыми балками. Мост поворачивается относительно своей оси на ± 360°. По мосту крана по общему пути перемещаются две грузовые тележки: тележка главная и тележка вспомогательная. На тележках смонтированы силовые механизмы подъема: на тележке главной – грузоподъемностью 370 (200) т, на тележке вспомогательной – 160 (140) т и 2х70 т.

Управление краном производится дистанционно с основного пульта управления, установленного в кабине управления, или с резервного пульта, установленного в электроаппаратном помещении.

Управление механизмами подъемов 370 (200) т, 160 (140) т, 2х70 т и талей производится с помощью одного командоконтроллера. Выбор конкретного привода, включая совместную работу механизмов подъемов 160 (140) т и 2х70 т, осуществляется с помощью дополнительного переключателя на пульте управления. Переключение с одного привода подъема на другой осуществляется только при остановленных приводах подъема.

Оператор крана получает информацию о ходе процесса перемещения грузов, текущей операции, состоянии и положении механизмов крана автоматически или по запросу.

Электроснабжение полярного крана осуществляется от системы электроснабжения собственных нужд АС.

Синхронный подъем и спуск груза обеспечивается двумя резервированными системами подъема вспомогательной грузовой тележки грузоподъемностью 160 т и грузоподъемностью 2х70 т. При выходе из строя одной из систем подъема операцию транспортирования продолжает другая. Механизмы подъема могут работать как синхронно, так и раздельно, независимо друг от друга. Конструктивное исполнение механизмов подъема позволяет обеспечить окончание начатой технологической операции в случае выхода из строя одного из двигателей: подъем или спуск будет продолжен за счет второго двигателя, но с половинной скоростью. Подвеска грузоподъемностью 160 т оборудована двурогим пластинчатым крюком, который шарнирно с помощью оси соединен с вилкой, опирающейся на роликоподшипник. Вилка крюка снабжена механизмом вращения, который позволяет осуществлять автоматический поворот вилки с крюком на 270°. Для механического отсоединения крюка или груза от вилки последняя оборудована механизмом выдвижения оси крюка. Подвеска грузоподъемностью 2х70 т состоит из двух малых подъемов грузоподъемностью 70 т, соединенных между собой скобой. Малые подъемы оборудованы грузозахватными проушинами. Проушины опираются на упорный подшипник, благодаря чему могут поворачиваться вокруг вертикальной оси на 360°.

Кран полярный имеет следующие защиты и блокировки:

запрет работы крана с отключением главного контактора с наложением тормозов всех механизмов при превышении веса груза поднимаемого любым из подъемов более чем на 10 % от номинальной грузоподъемности;

запрет работы крана с отключением главного контактора с наложением тормозов всех механизмов при срабатывании аварийных концевых выключателей (крайние верхние положения подъемов);

запрет работы крана с отключением главного контактора с наложением тормозов всех механизмов при превышении скорости механизмов подъема на 30 % от номинальной;

запрет одновременной работы двух и более механизмов, за исключением совместной работы механизма передвижения крана и механизма передвижения главной или вспомогательной тележки, а также запрет одновременной работы механизмов подъема 160(140) т и 2х70 т вспомогательной тележки при транспортировании контейнера с ОЯТ;

запрет переключения выбора приводов подъемов (главного 370(200) т, главного 160(140) т, вспомогательного 2х70 т, синхронного 160(140) т и 2х70 т, талей 10 т) при работе одного из них;

запрет работы механизмов подъема 370(200) т и 160(140) т в направлении «вниз» при снижении веса груза ниже предельного заданного значения;

останов механизмов подъемов при достижении концевых выключателей крайних положений (движение возможно только в противоположном направлении);

переход механизмов подъемов на минимальную скорость при срабатывании предварительных концевых выключателей снижения скорости;

запрет работы механизмов выдвижения осей вилок 370(200) т и 160(140) т, если на подвеске есть груз;

останов механизмов выдвижения осей вилок 370(200) т и 160(140) т при превышении заданного значения крутящего момента;

останов механизмов передвижения главной и вспомогательной тележек, при достижении концевых выключателей крайних положений (движение возможно только в противоположном направлении);

запрет перемещения краном грузов над бассейном выдержки и шахтой реактора за исключением специальных транспортных операций в указанных зонах.

3.2 Перегрузочная машина МП-1000.

МП предназначена для выполнения ТТО, связанных с перегрузкой ядерного топлива.

МП состоит из моста, перемещающегося по рельсовому пути, и тележки, на которой установлены рабочие органы машины: РШ, труба направляющая с площадкой поворотной, привод поворота РШ, привод поворота ТВШ, два привода подрыва, ТВШ, устанавливаемая в гнездо площадки поворотной. Электроснабжение МП осуществляется через токоподвод моста от системы электроснабжения собственных нужд.

Управление МП производится со стационарного дистанционного пульта управления, размещаемого в специальном помещении, находящемся вне защитной оболочки реакторного отделения. На пульте управления расположены органы управления и контрольная аппаратура.

Перегрузка реактора осуществляется в полуавтоматическом режиме, когда наведение РШ на заданную координату, сцепление с перегружаемым изделием и извлечение его производится в автоматическом режиме, а команда на выполнение каждой следующей операции после выполнения предыдущей выдается оператором.

Например, после наведения МП на заданную координату сцепление с извлекаемым изделием производится после проверки правильности выхода на заданную координату путем сравнения показаний индикаторов перемещения моста и тележки с координатами, указанными в программе загрузки.

МП имеет следующие защиты и блокировки:

запрет на перемещение моста и тележки при достижении крайних положений;

запрет на поворот РШ при достижении крайних положений;

запрет на поворот ТВШ при достижении крайних положений;

запрет на поворот РШ за исключением разрешенных зон;

запрет на перемещение механизмов МП, кроме механизма перемещения моста, при нахождении МП над транспортным коридором;

запрет на перемещение захвата ТВС вверх при достижении на канате захвата ТВС предельной нагрузки;

запрет на перемещение захвата кластера вверх при достижении на канате захвата кластера предельной нагрузки;

запрет на перемещение захвата кластера вниз при уменьшении усилия на канате на величину более допустимой;

запрет на перемещение захвата ТВС вниз при уменьшении усилия на канате на величину более допустимой;

запрет на вертикальное перемещение РШ при достижении крайнего верхнего положения;

запрет на перемещение захвата ТВС при нахождении механизма поворота РШ не в разрешенном угловом положении;

запрет на перемещение ТВШ вниз при ослаблении каната ТВШ;

запрет на перемещение моста и тележки при нахождении РШ или ТВШ не в транспортном положении, за исключением работы МП при шаговом движении или при выполнении осмотра отсеков зоны обслуживания и контроля уровня установки ТВС в реакторе и движении на малой скорости;

исключение несанкционированного перемещения механизмов МП.

3.3. Платформа внутристанционная (приводится описание платформы внутристанционной).

3.4 ТУК (приводится описание ТУК).

4. Определение номенклатуры ТП, осуществляемых сложным технологическим комплексом.

ТТО, выполняемые сложным технологическим комплексом, сгруппированы в следующие ТП:

ТП1 - установка чехла с ТВС на пол реакторного отделения (из платформы внутристанционной);

ТП2 - перемещение чехла без крышки на ступеньку БВ;

ТП3 - перемещение чехла со ступеньки БВ в УГ;

ТП4 - перемещение ТВС из УГ в стеллаж БВ;

ТП5 - перемещение ТВС из стеллажа БВ в реактор;

ТП6 - перемещение ОТВС из реактора в стеллаж БВ;

ТП7 - перемещение ОТВС из БВ в УГ;

ТП8 - перемещение ТУК (с ОТВС) из УГ в мойку;

ТП9 - перемещение ТУК (с ОТВС) из мойки в вагон;

ТП10 - удаление ЧСТ из УГ;

ТП11 - установка ТУК в УГ.

5. Анализ технологических процессов.

По результатам анализа ТП, представленных в пункте 4 настоящего приложения, выделены следующие базовые интервалы.

Базовые интервалы технологического процесса ТП1:

БИ01 - установка на вилку главного подъема полярного крана захвата типа 1 для ЧСТ;

БИ02 - перемещение полярного крана с захватом типа 1 без ЧСТ на координаты извлечения ЧСТ из вагона;

БИ03 - вертикальное перемещение захвата типа 1 без ЧСТ от уровня транспортного положения до уровня посадки захвата на ЧСТ в вагоне;

БИ04 - сцепление захвата типа 1 с ЧСТ;

БИ05 - вертикальное перемещение захвата типа 1 с ЧСТ от уровня посадки захвата на ЧСТ в вагоне до уровня транспортного положения;

БИ06 - перемещение крана на координаты установки ЧСТ на пол реакторного отделения;

БИ07 - вертикальное перемещение захвата типа 1 с ЧСТ от уровня транспортного положения до уровня установки ЧСТ на пол реакторного отделения;

БИ08 - расцепление ЧСТ с захватом типа 1.

Базовые интервалы технологического процесса ТП2:

БИ09 - вертикальное перемещение захвата типа 1 с ЧСТ без крышки от уровня установки ЧСТ на пол реакторного зала до уровня транспортного положения;

БИ10 - перемещение полярного крана на координаты установки ЧСТ на ступеньку БВ;

БИ11 - вертикальное перемещение захвата типа 1 с ЧСТ от уровня транспортного положения до уровня установки ЧСТ на ступеньку БВ;

БИ12 - расцепление захвата типа 1 с ЧСТ;

БИ13 - снятие с вилки крана захвата типа 1;

БИ14 - установка на вилку захвата типа 2 для ЧСТ;

БИ15 - перемещение крана с захватом типа 2 без ЧСТ на координаты сцепления с ЧСТ на ступеньке БВ;

БИ16 - вертикальное перемещение захвата типа 2 без ЧСТ от уровня транспортного положения до уровня посадки захвата на ЧСТ на ступеньке БВ;

БИ17 - сцепление захвата типа 2 с ЧСТ.

Базовые интервалы технологического процесса ТП3:

БИ18 - вертикальное перемещение захвата типа 2 с ЧСТ от уровня установки ЧСТ на промежуточную площадку до уровня окончания снятия ЧСТ со ступеньки БВ;

БИ19 - перемещение крана с ЧСТ на координаты установки ЧСТ в УГ;

БИ20 - вертикальное перемещение захвата типа 2 с ЧСТ от уровня окончания снятия ЧСТ со ступеньки БВ до уровня установки ЧСТ в УГ;

БИ21 - расцепление захвата типа 2 с ЧСТ;

БИ22 - вертикальное перемещение захвата типа 2 без ЧСТ от уровня посадки захвата на ЧСТ до уровня транспортного положения;

БИ23 - снятие с вилки захвата типа 2.

Базовые интервалы технологических процессов ТП4, ТП5, ТП6, ТП7:

БИ24 - перемещение МП по реактору, БВ или УГ без ТВС;

БИ25 - перемещение МП по транспортному коридору без ТВС;

БИ26 - перемещение МП по реактору, БВ или УГ с ТВС;

БИ27 - перемещение МП по транспортному коридору с ТВС;

БИ28 - вертикальное перемещение захвата ТВС без ТВС из транспортного положения до уровня на 200 мм выше уровня головок установленных ТВС;

БИ29 - вертикальное перемещение захвата ТВС без ТВС от уровня на 200 мм выше уровня головок установленных ТВС до уровня посадки захвата ТВС на ТВС;

БИ30 - поворот фиксатора захвата ТВС при сцеплении с ТВС;

БИ31 - вертикальное перемещение захвата ТВС с ТВС от гнезда до положения хвостовика ТВС на 200 мм выше уровня головок установленных ТВС;

БИ32 - вертикальное перемещение захвата ТВС с ТВС от положения хвостовика ТВС на 200 мм выше уровня головок установленных ТВС до транспортного положения;

БИ33 - вертикальное перемещение захвата ТВС с ТВС из транспортного положения до уровня, соответствующего положению хвостовика ТВС на 200 мм выше уровня головок установленных ТВС;

БИ34 - вертикальное перемещение захвата ТВС с ТВС от уровня, соответствующего положению хвостовика ТВС на 200 мм выше уровня головок установленных ТВС до гнезда;

БИ35 - поворот фиксатора захвата ТВС при расцеплении с ТВС;

БИ36 - вертикальное перемещение захвата ТВС без ТВС от уровня посадки захвата ТВС на ТВС до уровня 200 мм выше головок установленных ТВС;

БИ37 - вертикальное перемещение захвата ТВС без ТВС от уровня на 200 мм выше головок установленных ТВС до транспортного положения.

Базовые интервалы технологического процесса ТП8:

БИ38 - установка на вилку крана траверсы;

БИ39 - перемещение крана с траверсой без ТУК на координаты извлечения контейнера из УГ;

БИ40 - вертикальное перемещение траверсы без ТУК от уровня транспортного положения до уровня сцепления траверсы с ТУК;

БИ41 - сцепление траверсы с ТУК в УГ;

БИ42 - вертикальное перемещение траверсы с ТУК от уровня сцепления траверсы с ТУК до уровня начала установки на ступеньку БВ;

БИ43 - перемещение крана с ТУК на координаты установки на ступеньку БВ;

БИ44 - вертикальное перемещение траверсы с ТУК от уровня начала установки ТУК на промежуточную площадку до уровня установки ТУК на ступеньку БВ;

БИ45 - установка крышки в ТУК;

БИ46 - вертикальное перемещение траверсы с ТУК от уровня установки ТУК на ступеньку БВ до уровня транспортного положения;

БИ47 - перемещение крана с ТУК на координаты мойки;

БИ48 - вертикальное перемещение траверсы с ТУК от уровня транспортного положения до уровня установки ТУК в мойку.

Базовые интервалы технологического процесса ТП9:

БИ49 - вертикальное перемещение траверсы с ТУК от уровня установки ТУК в мойке до уровня транспортного положения;

БИ50 - перемещение моста с ТУК на координаты установки ТУК в вагон;

БИ51 - вертикальное перемещение траверсы с ТУК от уровня транспортного положения до уровня установки ТУК в вагон;

БИ52 - расцепление траверсы с ТУК в вагоне;

БИ53 - вертикальное перемещение траверсы без ТУК от уровня расцепления траверсы с ТУК в вагоне до уровня транспортного положения;

БИ54 - снятие с вилки крана траверсы.

базовые интервалы технологического процесса ТП10:

БИ55 - вертикальное перемещение ЧСТ без ТВС;

БИ56 - горизонтальное перемещение ЧСТ без ТВС.

Базовые интервалы технологического процесса ТП11:

БИ57 - вертикальное перемещение ТУК без ТВС;

БИ58 - горизонтальное перемещение ТУК без ТВС.

6. Функции, выполняемые сложным технологическим комплексом.

Сложный технологический комплекс выполняет следующие требуемые функции:

функция 1 – осуществление комплекса операций с ТТО в соответствии с установленными номенклатурой ТТО и порядком осуществления перегрузки (перестановки, выгрузки, загрузки) ТВС. Номенклатура ТТО устанавливается индивидуально для каждой перегрузки (перестановки, выгрузки, загрузки) ТВС, вследствие чего количество и порядок следования технологических процессов ТП1-ТП11, выполняемых комплексом при осуществлении функции 1, также является индивидуальным;

функция 2 – предотвращение нарушений при проведении комплекса операций с ТТО требований нормативной и технологической документа-

ции, связанных с обеспечением безопасности при обращении с ядерным топливом. Поскольку, как отмечено выше, номенклатура ТТО устанавливается индивидуально для каждой перегрузки (перестановки, выгрузки, загрузки) ТВС, количество и порядок следования технологических процессов ТП1-ТП11, выполняемых комплексом при осуществлении функции 2, также является индивидуальным.

7. Критерии отказа сложного технологического комплекса.

Критерием отказа сложного технологического комплекса на выполнение функции 1 является отказ крана или МП или иной отказ (ошибка персонала), приводящий к невыполнению любого из технологических процессов ТП1-ТП11, подлежащих выполнению сложным технологическим комплексом.

Критерием отказа сложного технологического комплекса на выполнение функции 2 является наступление любого из событий нарушения требований нормативной и технологической документации, связанных с обеспечением безопасности при обращении с ядерным топливом, представленных в табл. № 1 настоящего приложения.

Таблица № 1

События, при наступлении которых сложный технологический комплекс отказывает на выполнение функции 2

Событие	Характеристика события	Основание для выбора
	События, связанные с ЧСТ	
Торцевой удар чехла со свежим топливом	Торцевой удар, который может вызвать повреждения или изменение геометрии ТВС и твэлов	Пункт 2.4.4 Правил безопасности при хранении и транспортировании ядерного топлива на объектах использования атомной энергии
Боковой удар чехла со свежим топливом	Боковой удар, который может вызвать повреждения или изменение геометрии ТВС и твэлов	Пункт 2.4.4 Правил безопасности при хранении и транспортировании ядерного топлива на объектах использования атомной энергии
	События, связанные с ТВС	
Избыточные механические нагрузки на ТВС при перегрузке	Превышение крутящего момента Превышение усилия сжатия Превышение усилия извлечения ТВС	Пункты 2.4.4, 4.6.1 Правил безопасности при хранении и транспортировании ядерного топлива на объектах использования атомной энергии
Усилие изгиба ТВС	Возникновение усилия изгиба	Пункты 2.4.4, 4.6.1 Правил безопасности при хранении и транспортировании ядерного топлива на объектах использования атомной энергии

Событие	Характеристика события	Основание для выбора
Боковой удар ТВС	Соударение штанги перегрузочной машины, транспортирующей ТВС, с конструкциями реактора или БВ не допускается	Пункты 2.4.4, 4.6.1 и 4.6.6 Правил безопасности при хранении и транспортировании ядерного топлива на объектах использования атомной энергии
Подъем ТВС выше допустимого уровня	Подъем ТВС в процессе ТТО выше максимально допустимого уровня	Пункты 4.6.3, 4.6.8 Правил безопасности при хранении и транспортировании ядерного топлива на объектах использования атомной энергии
События, связанные с ТУК		
Торцевой удар ТУК с ОТВС	Торцевой удар, который может вызвать повреждения или изменение геометрии ТВС и твэлов.	Пункт 2.4.4 Правил безопасности при хранении и транспортировании ядерного топлива на объектах использования атомной энергии
Боковой удар ТУК с ОТВС	Боковой удар, который может вызвать повреждения или изменение геометрии ТВС и твэлов.	Пункт. 2.4.4 Правил безопасности при хранении и транспортировании ядерного топлива на объектах использования атомной энергии

8. Анализ последствий нарушений ТП.

Для каждого базового интервала, перечисленного в разделе 5 настоящего приложения, определены характерные для него нарушения ТП, а также определены последствия нарушения.

Результаты определения последствий нарушений ТП представлены в табл. № 2 настоящего приложения (в связи с большим объемом таблицы представлен ее фрагмент – результаты анализа последствий нарушений технологического процесса ТП4 на базовом интервале БИ32 для функции 2).

Таблица № 2

Результаты определения последствий нарушений технологического процесса ТП 4 (фрагмент)

Базовый интервал	**Система, персонал**	**Нарушения технологического процесса**	**Предусмотренные защиты и блокировки (примечание 2)**	**Последствия при неработоспособности защит и блокировок**
БИ32 Вертикальное перемещение захвата ТВС с ТВС от положения хвостовика. ТВС	Машина перегрузочная	F012 Отказ силовой цепи привода перемещения захвата ТВС	L07(2), L07(3), L56(3), L82(2)	D01 Падение ТВС
		F018 Обрыв троса захвата ТВС	Защиты (блокировки) не предусмотрено	D01 Падение ТВС

Базовый интервал	Система, персонал	Нарушения технологического процесса	Предусмотренные защиты и блокировки (примечание 2)	Последствия при неработоспособности защит и блокировок
на 200 мм выше уровня головок установленных ТВС до транспортного положения		F001 Перерыв в энергоснабжении	Наложение тормозов привода захвата ТВС при снятии питания	D01 Падение ТВС
		F030 Ложное включение привода моста (примечание 1)	L03(2), L03(3), L01(4), L01(5)	D05 Боковой удар ТВС
		F040 Ложное включение привода тележки	L04(2), L04(3), L02(4), L02(5)	D05 Боковой удар ТВС
		F070 Ложное включение привода перемещения фиксатора в сторону расцепления	Конструкция захвата ТВС не позволят открыться фиксатору при наличии ТВС	D01 Падение ТВС

Примечание 1. Результаты определения причин возникновения нарушения ТП приведены в табл. № 3 настоящего приложения.

Примечание 2. Наименование защит и блокировок:

L01(4) - снижение скорости моста до заданного значения при наличии сигнала от ультразвуковых датчиков приближения к препятствию;

L01(5) - отключение питания моста при наличии сигнала датчика «Столкновение с препятствием»;

L02(4) - снижение скорости тележки до заданного значения при наличии сигнала от ультразвуковых датчиков приближения к препятствию;

L02(5) - отключение питания тележки при наличии сигнала датчика «Столкновение с препятствием»;

L07(2) - отключение питания электродвигателей всех механизмов МП при несанкционированном перемещении захвата ТВС;

L07(3) - отключение питания электродвигателей всех механизмов МП при несанкционированном перемещении захвата ТВС;

L03(3) - останов перемещения моста при нахождении РШ на расстоянии меньше минимально допустимого до границы зоны обслуживания;

L04(3) - останов перемещения тележки при нахождении РШ от границы зоны обслуживания на расстоянии меньше минимально допустимого;

L03(2) - останов перемещения моста при нахождении РШ на расстоянии меньше минимально допустимого до границы зоны обслуживания;

L56(3) - останов перемещения захвата ТВС при скорости большей, чем это установлено технологическими ограничениями;

L04(2) - останов перемещения тележки при нахождении РШ на расстоянии меньше минимально допустимого до границы зоны обслуживания;

L82(2) - останов захвата ТВС при превышении скорости перемещения.

9. Определение причин возникновения нарушений ТП.

Для каждого нарушения ТП, представленного в табл. № 2 настоящего приложения, определены причины его возникновения.

Результаты определения причин возникновения нарушений ТП представлены в табл. № 3 настоящего приложения (фрагмент – результаты анализа причин возникновения нарушения ТП «Ложное включение привода моста»).

Таблица № 3

Анализ причин возникновения нарушений ТП (фрагмент)

Нарушение технологического процесса	Отказы элементов систем, ошибки персонала, приводящие к нарушению	Предусмотренные защиты и блокировки (примечание 1)
F030 Ложное включение привода моста на БИ 32 Вертикальное перемещение захвата ТВС с ТВС от положения хвостовика ТВС на 200 мм выше уровня головок установленных ТВС до транспортного положения	IE 001 Ошибка оператора, приводящая к вводу несвоевременного задания на перемещение моста	P01(2), P01(3), P02(2), P02(3), P03(2)
	IE 201 Отказ пульта управления, приводящий к несвоевременному формированию задания на перемещение моста	
	IE 301 Отказ подсистемы управления, приводящий к несвоевременному формированию команды на перемещение моста	P01(3), P02(3)
	IE 401 Отказ преобразователя частоты привода перемещения моста, приводящий к несвоевременному запуску перемещения моста	L01(2), L01(3)

Примечание 1. Наименование защит и блокировок:

P01(2) - запрет на перемещение (блокировка) моста при перемещении захвата ТВС;

P01(3) - запрет на перемещение (блокировка) моста при перемещении захвата ТВС;

P02(2) - запрет на перемещение (блокировка) моста при нахождении захвата ТВС не в транспортном положении;

P02(3) - запрет на перемещение (блокировка) моста при нахождении захвата ТВС не в транспортном положении;

P03(2) - запрет на перемещение (блокировка) моста при нахождении ТВШ не в транспортном положении;

P01(3) - запрет на перемещение (блокировка) моста при перемещении захвата ТВС;

P02(3) - запрет на перемещение (блокировка) моста при нахождении захвата ТВС не в транспортном положении;

L01(2) - отключение питания электродвигателей (блокировка) всех механизмов МП при несанкционированном перемещении моста;

L01(3) - отключение питания электродвигателей (блокировка) всех механизмов МП при несанкционированном перемещении моста.

10. Построение структурно-логической модели надежности (функциональной безопасности) сложного технологического комплекса ТТО с ядерным топливом.

Для разработки структурно-логической модели надежности (функциональной безопасности) сложного технологического комплекса ТТО с ядерным топливом выбран метод деревьев отказов.

Деревья отказов технологического комплекса ТТО с ядерным топливом на выполнение функции 2 представлена на рис. 1-5 настоящего приложения (в связи с большой размерностью модели приведен ее фрагмент).

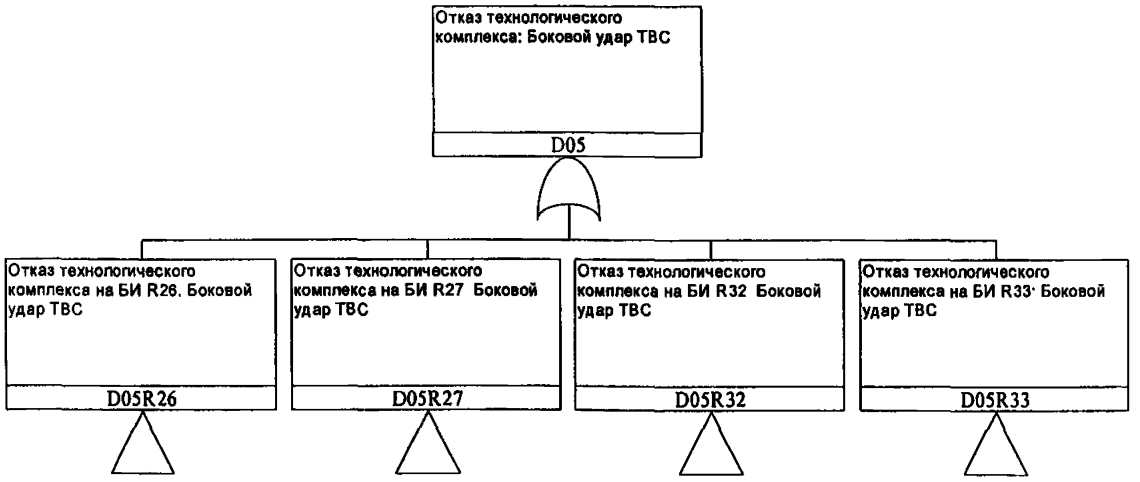


Рис. 1. Дерево отказов «Отказ сложного технологического комплекса вследствие бокового удара ТВС» (учтены все базовые интервалы)

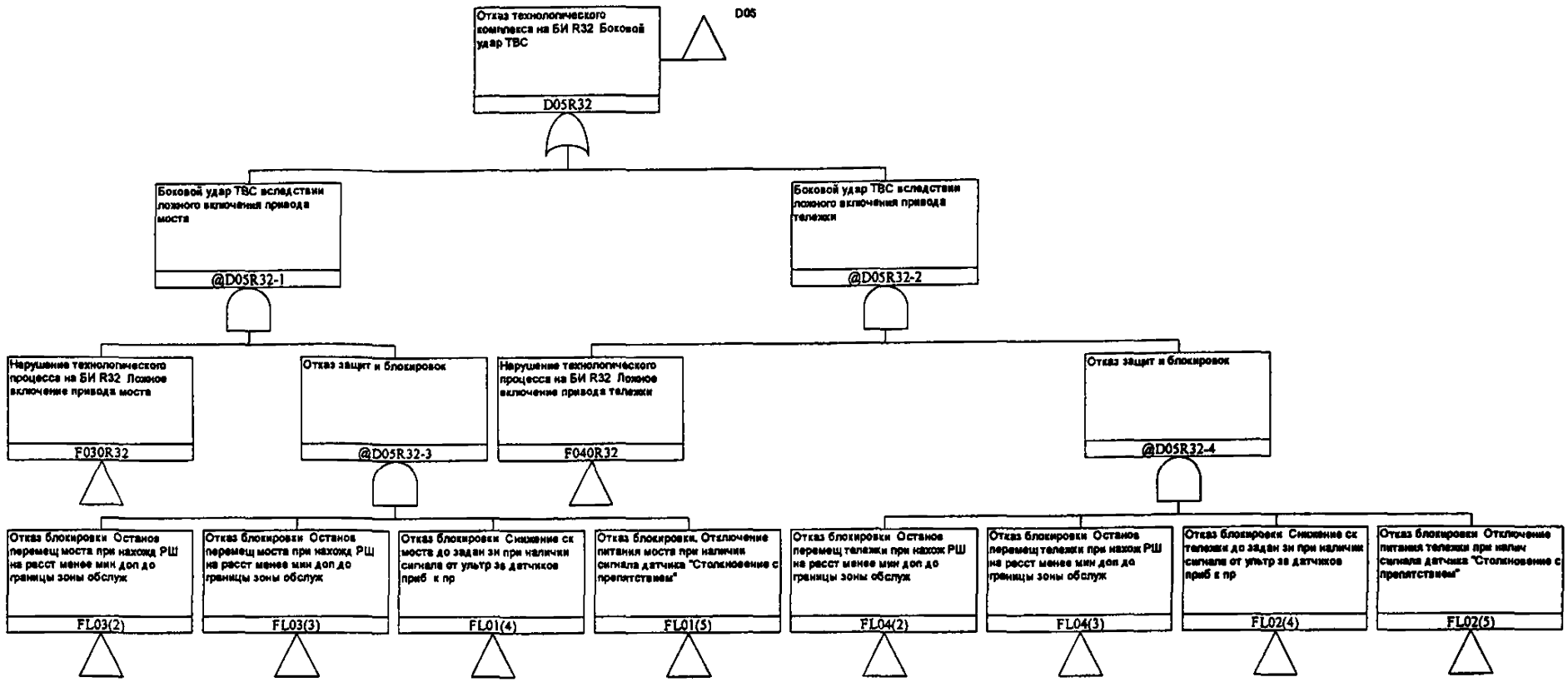


Рис. 2. Дерево отказов «Отказ сложного технологического комплекса вследствие бокового удара ТВС на базовом интервале БИ32» (разработано на основе данных таблицы № 2 настоящего приложения)

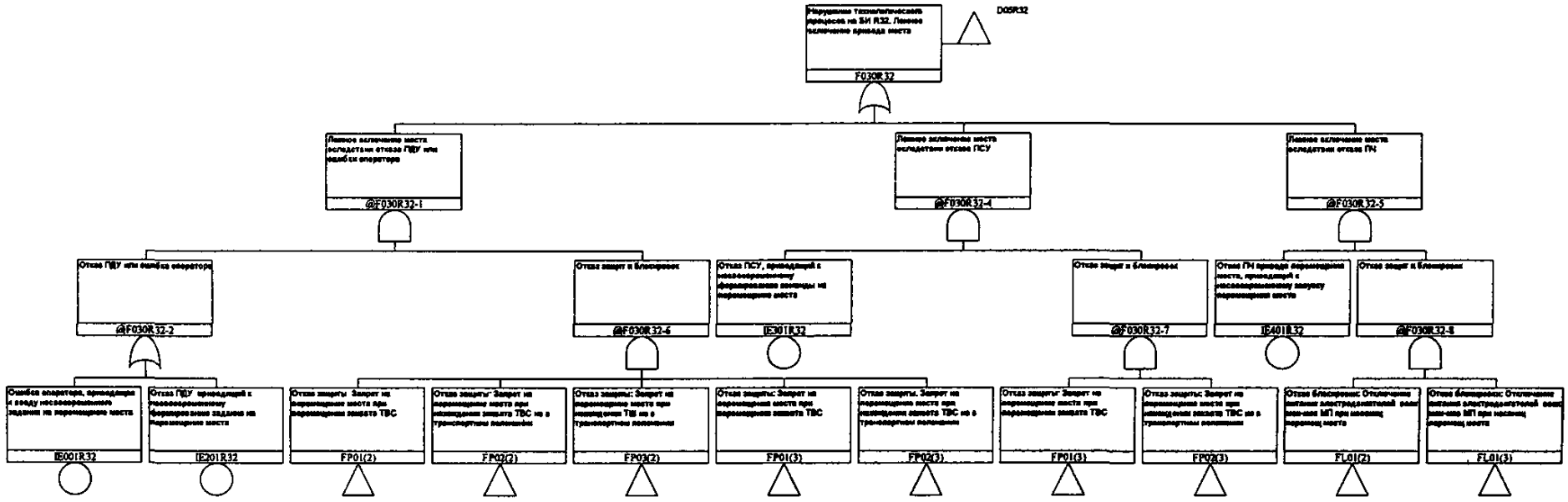


Рис. 3. Дерево отказов «Отказ сложного технологического комплекса вследствие ложного включения привода моста на базовом интервале БИ32» (разработано на основе данных таблицы № 3 настоящего приложения)

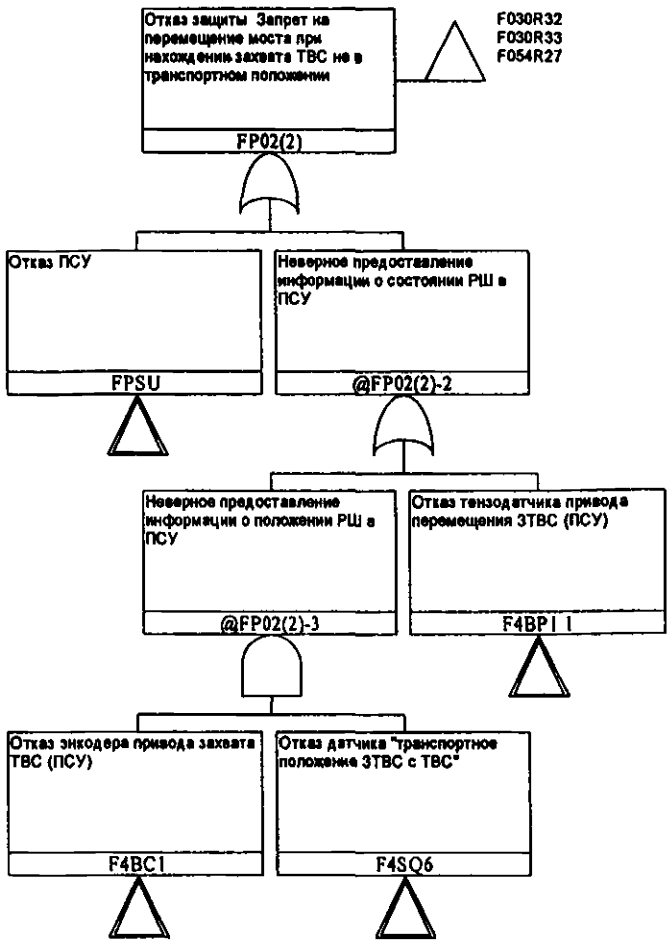


Рис. 4. Дерево отказов «Отказ защиты: Запрет на перемещение моста при нахождении захвата ТВС не в транспортном положении» (построено на основе анализа защит и блокировок МП)

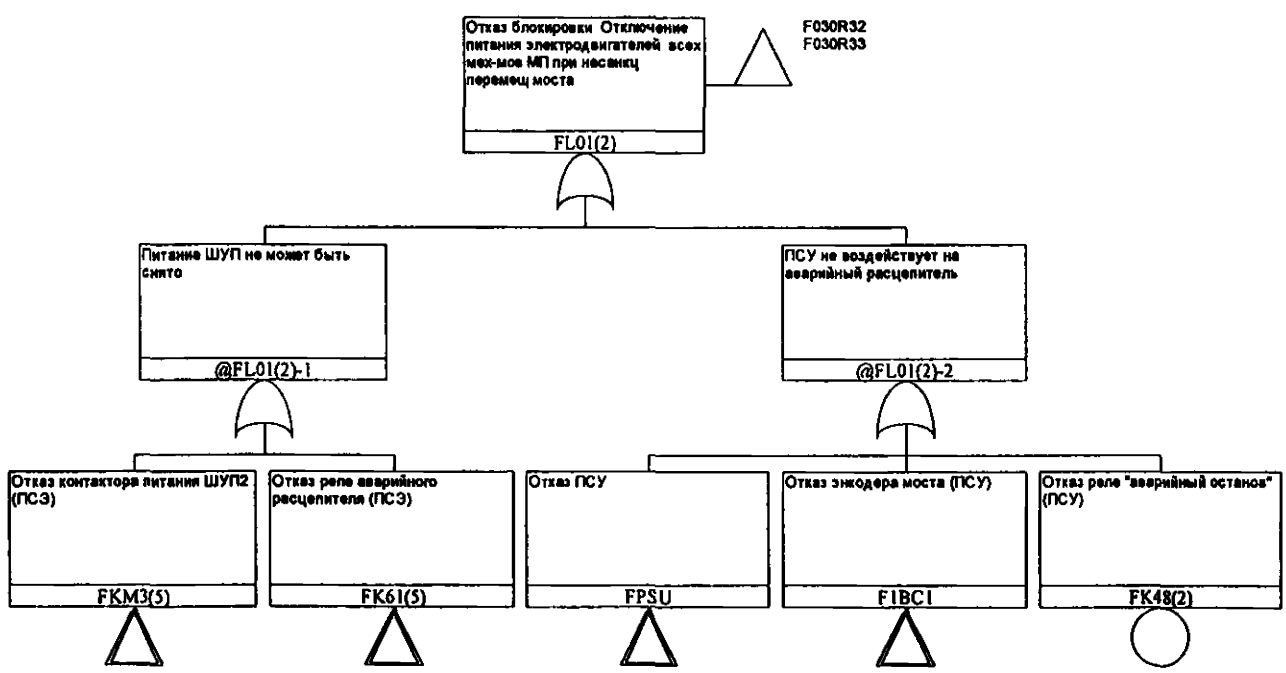


Рис. 5. Дерево отказов «Отказ блокировки: Отключение питания электродвигателей всех механизмов МП при несанкционированном перемещении моста» (построено на основе анализа защит и блокировок МП)

10. Параметры надежности элементов сложного технологического комплекса.

Результаты определения показателей надежности элементов технологического комплекса ТТО с ядерным топливом представлены в табл. № 4 настоящего приложения.

Таблица № 4

Параметры надежности элементов технологического комплекса ТТО с ядерным топливом (фрагмент)

Тип элемента	Интенсивность отказа, $1/ч \cdot 10^{-6}$
Электродвигатель DRS132S6BE5HR/FL/TF/EV7C/V/DH	0,41
Тормоз BE5B	0,41
Датчик положения 3RG40 23-0GB00	0,33
Датчик положения 3SE5122-0CD02	0,33
Мотор-редуктор KA37/TRS80S4BE1HR/TF/EV7C/DH	0,41
Преобразователь силоизмерительный	10,0
Мотор-редуктор KA107/T DRS132MBE5HR/TF/EV7C/DH	0,41
Тормоз NFF630	4,88
Мотор-редуктор KAF37/ DR63L4BR/HR/TF/EH1C/H	0,41
Выключатель поворотный	1,00
Тормоз NFF40	4,88
Мотор-редуктор KA47 R37 DR63M4BR/HR/TF/EH1C	0,41
Тормоз NFF4	0,57
Энкодер CEV 58M-00227	4,00
Ультразвуковой датчик	3,80
Реле в сборе LZS	0,13
Модуль интерфейсный IM151	0,82
Модуль ввода дискретных сигналов 8DI	0,43
Блок управления тормозом BMK	2,78
Блок управления тормозом GSSG	2,78
Контактор LC1D09	1,25
Модуль дискретных входов SM321	3,74
Модуль релейный PLC-RSC	0,03

Тип элемента	Интенсивность отказа, $1/ч \cdot 10^{-6}$
Модуль дискретных выходов SM 322	6,37
Модуль ввода аналоговых сигналов 4AI	1,11
Реле LR-2	0,28
Преобразователь MDX61B	
Модуль ввода дискретных сигналов 8DI	0,43
Выключатель концевой	1,00
Модуль вывода дискретных 8DO	0,29
Модуль ввода сигналов 2AI I 2/4	0,87

11. Учет зависимостей сложного технологического комплекса. Учет ООВ.

При выполнении анализа учитывались зависимости работы элементов и систем, составляющих сложный технологический комплекс от системы электроснабжения собственных нужд АС.

При анализе технологического комплекса ТТО с ядерным топливом были определены группы элементов, подверженных ООВ. Группы ООВ формировались для элементов, отвечающих критериям 1-3 в соответствии с пунктом 8 приложения № 5 к настоящему Руководству по безопасности, а также отвечающим одному из следующих требований:

элементы, входящие в группу ООВ, имеют общего изготовителя;

элементы, входящие в группу ООВ, имеют общую процедуру технического обслуживания и ремонта;

элементы, входящие в группу ООВ, характеризуются общностью расположения.

Описание групп элементов (фрагмент описания), подверженных ООВ, приведено в табл. № 5 настоящего приложения.

Таблица № 5

Группы элементов технологического комплекса ТТО с ядерным топливом, подверженных ООВ (фрагмент)

Обозначение и наименование группы	**Обозначение и наименование элементов, входящих в состав группы**	**Модель для определения вероятности ООВ**	**Значения параметров модели**
Оборудование машины перегрузочной			
1BC Энкодеры привода моста	1BC1 Энкодер привода моста (ПСУ) 1BC2 Энкодер привода моста (ПСЗБ)	Модель β-фактора	0,1

Обозначение и наименование группы	Обозначение и наименование элементов, входящих в состав группы	Модель для определения вероятности ООВ	Значения параметров модели
2BC Энкодеры привода тележки	2BC1 Энкодер привода тележки (ПСУ) 2BC2 Энкодер привода тележки (ПСЗБ)	Модель β-фактора	0,1
4BC Энкодеры привода захвата ТВС	4BC1 Энкодер привода захвата ТВС (ПСУ) 4BC2 Энкодер привода захвата ТВС (ПСЗБ)	Модель β-фактора	0,1
4BP Преобразователь силоизмерительный двухканальный. Контроль усилия на канате захвата ТВС	4BP1.1 Контроль усилия на канате захвата ТВС (канал датчика, подключаемый к ПСУ) 4BP1.2 Контроль усилия на канате захвата ТВС (канал датчика, подключаемый к ПСЗБ)	Модель β-фактора	0,1
3SQ(1,5) Датчики привода подрыва 1 «Крайнее верхнее положение»	3SQ1 Крайнее верхнее положение (ПСУ) 3SQ5 Крайнее верхнее положение (ПСЗБ)	Модель β-фактора	0,1
CPU Контроллеры	CPU_319-3 Модуль ЦПУ ПСУ CPU_319-3 Модуль ЦПУ ПСЗБ	Модель β-фактора	0,1
1YB Тормоза привода моста	1T1 Встроенный тормоз привода моста 1YB1 Внешний тормоз привода моста	Модель β-фактора	0,01
2YB Тормоза привода тележки	2T1 Встроенный тормоз привода тележки 2YB1 Внешний тормоз привода тележки	Модель β-фактора	0,01
4YB Тормоза привода захвата ТВС	4T1 Встроенный тормоз привода захвата ТВС 4YB1 Внешний тормоз привода захвата ТВС	Модель β-фактора	0,01
K4_K5 Реле ШУП разрешения движения тележки	K4 Реле разрешения движения тележки от шкафа управления K5 Реле разрешения движения тележки от подсистемы защит и блокировок	Модель β-фактора	0,1

Обозначение и наименование группы	Обозначение и наименование элементов, входящих в состав группы	Модель для определения вероятности ООВ	Значения параметров модели
К12_К13 Реле ШУП разрешения движения захвата ТВС	К12 Реле разрешения движения захвата ТВС от шкафа управления К13 Реле разрешения движения захвата ТВС от подсистемы защит и блокировок	Модель β-фактора	0,1
КМ11_КМ12 Контакторы включения внешнего и встроенного тормозов электродвигателя захвата ТВС	КМ11 Контактор включения внешнего тормоза электродвигателя захвата ТВС КМ12 Контактор включения встроенного тормоза электродвигателя захвата ТВС	Модель β-фактора	0,1

12. Учет влияния персонала.

Перечень возможных ошибок персонала был сформирован по результатам анализа причин возникновения нарушений ТП и условий отказа защит и блокировок.

При выполнении анализа причин возникновения нарушений ТП и условий отказа защит и блокировок были учтены действия, выполняемые персоналом при управлении, техническом обслуживании и тестировании оборудования технологического комплекса.

Общий перечень ошибок персонала при управлении был разбит на следующие группы:

1) для МП:

ошибки при управлении мостом;

ошибки при управлении тележкой;

ошибки при управлении механизмом подрыва;

ошибки при управлении захватом ТВС;

ошибки при управлении фиксатором захвата ТВС;

ошибки при управлении поворотом РШ;

ошибки при управлении захватом кластера;

2) для полярного крана:

ошибки при управлении мостом;

ошибки при управлении главной тележкой;

ошибки при управлении вспомогательной тележкой;

ошибки при управлении механизмом подъема 370 (200) т.;

ошибки при управлении механизмом подъема 160 (140) т.;

ошибки при управлении механизмом подъема 2х70 т.;

ошибки при управлении талями.

Ошибки персонала при техническом обслуживании и опробованиях были разбиты на следующие группы:

ошибки при вводе уставок срабатывания защит и блокировок;

ошибки при калибровке измерительных каналов;

ошибки при настройке циклограмм скоростей и нагрузок;

ошибки при подготовке и загрузке программы перегрузки (только для МП);

ошибки при подготовке и загрузке картограмм реактора и БВ (только для МП).

В табл. № 6 настоящего приложения приведен фрагмент перечня ошибок персонала с назначенными в результате скринингового и (при необходимости) детального анализа вероятностями.

По результатам анализа зависимостей между ошибками персонала значимые зависимости между вероятностями ошибок персонала не установлены.

Таблица № 6

Ошибки персонала (фрагмент)

Наименование ошибки персонала	**Вероятность ошибки персонала**
Ошибки при управлении машиной перегрузочной	
Ошибки при управлении мостом	
Ошибка оператора, приводящая к вводу несвоевременного задания на перемещение моста	$3 \cdot 10^{-3}$
Ошибка оператора, приводящая к вводу ошибочных координат останова моста в допустимой зоне (только для полуавтоматического режима)	$3 \cdot 10^{-3}$
Ошибка оператора, приводящая к вводу координат останова моста в недопустимой зоне (только для полуавтоматического режима)	$3 \cdot 10^{-3}$
Ошибки при управлении тележкой	
Ошибка оператора, приводящая к вводу несвоевременного задания на перемещение тележки	$3 \cdot 10^{-3}$
Ошибка оператора, приводящая к вводу ошибочных координат останова тележки в допустимой зоне (только для полуавтоматического режима)	$3 \cdot 10^{-3}$
Ошибка оператора, приводящая к вводу координат останова тележки в недопустимой зоне (только для полуавтоматического режима)	$3 \cdot 10^{-3}$
Ошибки при управлении захватом ТВС	
Ошибка оператора, приводящая к вводу несвоевременного задания на перемещение захвата ТВС вверх	$3 \cdot 10^{-3}$
Ошибка оператора, приводящая к вводу несвоевременного задания на перемещение захвата ТВС вниз	$3 \cdot 10^{-3}$
Ошибка оператора, приводящая к вводу координат останова захвата ТВС в недопустимой зоне (только для полуавтоматического режима)	$3 \cdot 10^{-3}$
Ошибки при вводе уставок срабатывания защит и блокировок	
Ошибка при введении параметра «Максимально допустимое усилие на двух канатах захвата ТВС»	$1 \cdot 10^{-3}$

Ошибка при введении параметра «Максимально допустимая скорость захвата ТВС»	$1 \cdot 10^{-3}$
Ошибки при калибровке каналов контроля	
Ошибка при калибровке канала контроля усилия на канате захвата ТВС	$2 \cdot 10^{-3}$
Ошибка при калибровке канала контроля усилия на канате захвата кластера	$2 \cdot 10^{-3}$
Ошибка при калибровке канала контроля положения моста	$2 \cdot 10^{-3}$

13. Результаты анализа надежности (функциональной безопасности) сложного технологического комплекса ТТО с ядерным топливом.

На основе разработанной логико-вероятностной модели сложного технологического комплекса ТТО с ядерным топливом на выполнение требуемой были сформированы минимальные сечения отказов, представленные в табл. № 7 настоящего приложения.

Таблица № 7

Минимальные сечения отказов сложного технологического комплекса ТТО с ядерным топливом (фрагмент для функции 2, результаты для функции 1 представляются аналогично)

№	Вероятность реализации в год	Вклад, %	Отказ элемента системы, ошибка персонала	Отказ защит и блокировок		
			событие 1	событие 2	событие 3	событие 4
Отказ сложного технологического комплекса: Боковой удар ТВС						
1	$3{,}60 \cdot 10^{-7}$	49,67	HE916R26	-	-	-
2	$3{,}60 \cdot 10^{-7}$	49,67	HE915R26	-	-	-
3	$1{,}08 \cdot 10^{-9}$	0,15	HE023R26	FUZ1(4.1)	KM-ALL	-
4	$1{,}08 \cdot 10^{-9}$	0,15	HE022R26	FUZ1(4.2)	KM-ALL	-
5	$5{,}40 \cdot 10^{-10}$	0,07	HE003R26	FUZ1(4.2)	KM-ALL	-
6	$5{,}40 \cdot 10^{-10}$	0,07	HE006R26	FUZ1(4.1)	KM-ALL	-
7	$1{,}24 \cdot 10^{-10}$	0,02	HE022R26	FPSZB	FUZ1(4.2)	FKM3(5)
8	$1{,}24 \cdot 10^{-10}$	0,02	HE023R26	FPSZB	FUZ1(4.1)	FKM2(5)
9	$1{,}12 \cdot 10^{-10}$	0,02	HE022R26	FUZ1(4.2)	K5-ALL	-
10	$1{,}12 \cdot 10^{-10}$	0,02	HE023R26	FUZ1(4.1)	K5-ALL	-
11	$6{,}19 \cdot 10^{-11}$	0,01	HE003R26	FPSZB	FUZ1(4.2)	FKM3(5)
12	$6{,}19 \cdot 10^{-11}$	0,01	HE006R26	FPSZB	FUZ1(4.1)	FKM2(5)
13	$5{,}62 \cdot 10^{-11}$	0,01	HE006R26	FUZ1(4.1)	K5-ALL	-

№	Вероятность реализации в год	Вклад, %	Отказ элемента системы, ошибка персонала	Отказ защит и блокировок		
			событие 1	событие 2	событие 3	событие 4
14	$5{,}62 \cdot 10^{-11}$	0,01	HE003R26	FUZ1(4.2)	K5-ALL	-
15	$3{,}27 \cdot 10^{-11}$	0,00	HE022R26	FPSZB	FUZ1(4.2)	F2SQ7
16	$3{,}27 \cdot 10^{-11}$	0,00	HE023R26	FPSZB	FUZ1(4.1)	F2SQ8
17	$1{,}88 \cdot 10^{-11}$	0,00	HE022R26	CPU-ALL	F2BQ1	FKM3(5)
18	$1{,}88 \cdot 10^{-11}$	0,00	HE023R26	CPU-ALL	F2BQ2	FKM2(5)
19	$1{,}88 \cdot 10^{-11}$	0,00	HE023R26	FPSU	F2BQ2	KM-ALL
20	$1{,}88 \cdot 10^{-11}$	0,00	HE022R26	FPSU	F2BQ1	KM-ALL
21	$1{,}63 \cdot 10^{-11}$	0,00	HE003R26	FPSZB	FUZ1(4.2)	F2SQ7
22	$1{,}63 \cdot 10^{-11}$	0,00	HE006R26	FPSZB	FUZ1(4.1)	F2SQ8
23	$1{,}38 \cdot 10^{-11}$	0,00	HE023R26	CPU-ALL	FUZ1(4.1)	FKM2(5)
24	$1{,}38 \cdot 10^{-11}$	0,00	HE022R26	CPU-ALL	FUZ1(4.2)	FKM3(5)
25	$1{,}29 \cdot 10^{-11}$	0,00	HE023R26	FPSZB	FUZ1(4.1)	FK27(5)
26	$1{,}29 \cdot 10^{-11}$	0,00	HE022R26	FPSZB	FUZ1(4.2)	FK27(5)
27	$1{,}07 \cdot 10^{-11}$	0,00	HE306R26	FUZ1(4.1)	KM-ALL	-
28	$1{,}07 \cdot 10^{-11}$	0,00	HE302R26	FUZ1(4.2)	KM-ALL	-
29	$9{,}39 \cdot 10^{-12}$	0,00	HE004R33	CPU-ALL	F2BQ2	FKM2(5)
30	$9{,}39 \cdot 10^{-12}$	0,00	HE001R33	CPU-ALL	F2BQ1	FKM3(5)
31	$9{,}39 \cdot 10^{-12}$	0,00	HE003R26	F2BQ1	VAR	KM-ALL
32	$9{,}39 \cdot 10^{-12}$	0,00	HE001R32	F2BQ1	VAR	FKM3(5)
33	$9{,}39 \cdot 10^{-12}$	0,00	HE003R26	NEM	CPU-ALL	FKM2(5)
34	$9{,}39 \cdot 10^{-12}$	0,00	HE004R27	CPU-ALL	F2BQ2	OVA(5)
35	$9{,}39 \cdot 10^{-12}$	0,00	HE006R26	FPSU	F2BQ2	KM-ALL
36	$9{,}39 \cdot 10^{-12}$	0,00	HE004R32	CPU-ALL	F2BQ2	FKM2(5)
37	$9{,}39 \cdot 10^{-12}$	0,00	HE006R26	CPU-ALL	F2BQ2	FKM2(5)
38	$9{,}39 \cdot 10^{-12}$	0,00	HE005R27	CPU-ALL	F2BQ1	FKM3(5)
39	$7{,}87 \cdot 10^{-12}$	0,00	HE023R26	FUZ1(4.1)	FKM2(5)	FKM9(5)
40	$7{,}87 \cdot 10^{-12}$	0,00	HE023R26	FUZ1(4.1)	FKM2(5)	FKM10(5)
…	…	…	…	…	…	…

Результаты количественного анализа надежности (функциональной безопасности) технологического комплекса ТТО с ядерным топливом на выполнение требуемой функции 2 приведены в табл. № 8 настоящего приложения.

Таблица № 8

Результаты анализа надежности (функциональной безопасности) технологического комплекса ТТО с ядерным топливом на выполнение требуемой функции 2

Отказ сложного технологического комплекса	**Вероятность отказа в течение года**
Отказы сложного технологического комплекса, связанные с ЧСТ	
Падение ЧСТ	$7{,}49 \cdot 10^{-8}$
Торцевой удар ЧСТ	$5{,}75 \cdot 10^{-8}$
Боковой удар ЧСТ	$4{,}67 \cdot 10^{-5}$
Отказы сложного технологического комплекса, связанные с ТВС	
Падение ТВС	$5{,}40 \cdot 10^{-8}$
Сжатие ТВС	$2{,}38 \cdot 10^{-7}$
Усилие изгиба ТВС	$5{,}29 \cdot 10^{-7}$
Боковой удар ТВС	$3{,}62 \cdot 10^{-6}$
Недопустимое верхнее положение ТВС	$1{,}36 \cdot 10^{-12}$
Растяжение ТВС	$4{,}16 \cdot 10^{-7}$
Скручивание ТВС	$1{,}36 \cdot 10^{-9}$
Отказы сложного технологического комплекса, связанные с ТУК	
Падение ТУК с ОТВС	$2{,}25 \cdot 10^{-8}$
Торцевой удар ТУК с ОТВС	$6{,}34 \cdot 10^{-8}$
Боковой удар ТУК с ОТВС	$2{,}49 \cdot 10^{-5}$
Отказ сложного технологического комплекса по любой причине	
Суммарная вероятность отказа сложного технологического комплекса на выполнение функции 2	$7{,}67 \cdot 10^{-5}$

14. Выводы и рекомендации по результатам анализа надежности.

Для сложного технологического комплекса не установлены нормативные нормируемые показатели надежности, в связи с чем сравнение с ними результатов анализа надежности не осуществляется.

Для сложного технологического комплекса установлены проектные требования к показателям надежности (представлены в техническом задании). Выполненный анализ показывает соответствие сложного технологи-

ческого комплекса требованиям к показателям надежности как при выполнении функции 1, так и при выполнении функции 2.

По результатам анализа следует рекомендовать рассмотрение дополнения МП блокировками, защищающими от реализации доминирующих минимальных сечений (приводится список блокировок, рекомендуемых дополнительно к реализации), а также дополнительные меры по снижению вероятности ошибок персонала, входящих в доминирующие минимальные сечения (приводится перечень ошибок персонала и рекомендуемых мер по снижению их вероятностей, к которым могут относиться, например, корректировка эксплуатационной документации, дополнение программ подготовки персонала).

15. Список литературы.

Приводится список использованной литературы.

ПРИЛОЖЕНИЕ № 11
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому и атомному надзору
от 28 января 2015 г. № 26

Рекомендации по применению вероятностных методов механики разрушения к оценке надежности пассивных элементов

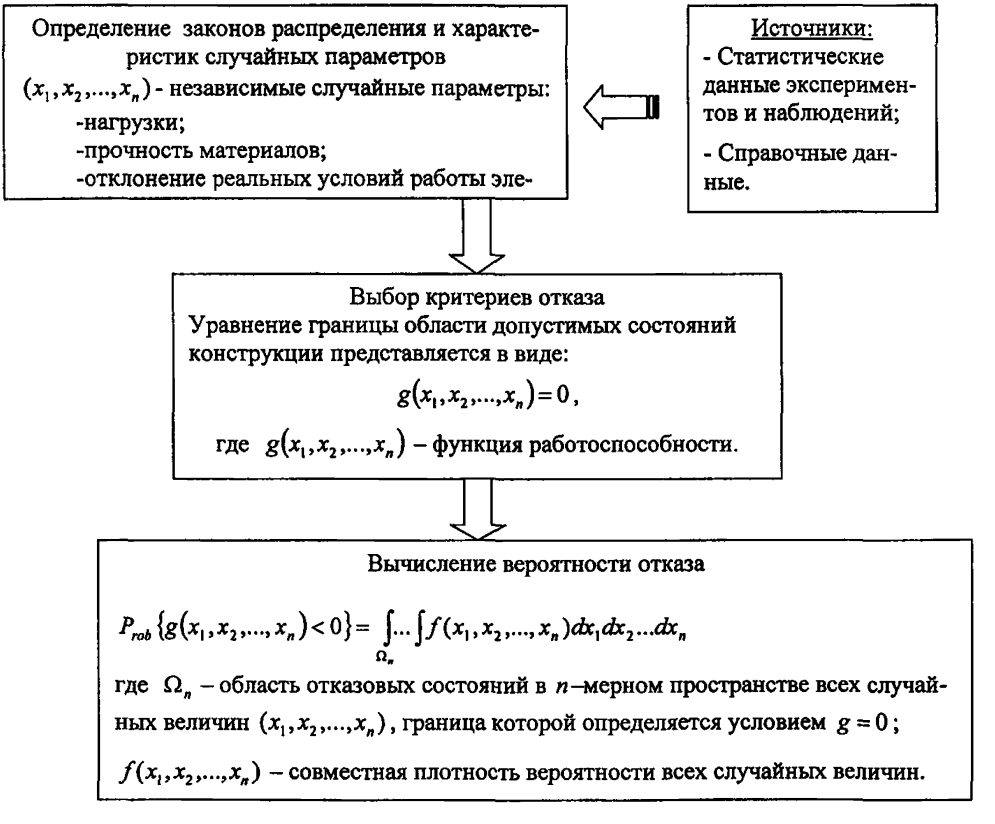


Рис. 1. Схема определения вероятности отказа пассивного элемента

Если все расчетные величины можно разделить на две группы, где первая включает характеристики, относящиеся к свойствам самой конструкции, а вторая характеризует внешние воздействия, то в приложении к задачам расчета на прочность условие отказа математически будет выражаться неравенством:

$$g(x_1, x_2, ..., x_n) = R(x_1, x_2, ..., x_m) - Q(x_{m+1}, x_{m+2}, ..., x_n) < 0$$

или

$$g = R - Q < 0, \qquad (1)$$

где:

g – функция работоспособности или резерв прочности;

R – несущая способность, выраженная в тех же единицах что и нагрузочный эффект Q;

Q – нагрузочный эффект.

При любых законах распределения R и Q математическое ожидание и стандартное отклонение резерва прочности соответственно равны:

$$m_g = m_R - m_Q, \quad s_g = \sqrt{s_R^2 + s_Q^2}, \qquad (2)$$

где m_R и s_R – математическое ожидание и стандарт распределения несущей способности;

m_Q и s_Q – математическое ожидание и стандарт распределения нагрузочного эффекта.

Для нормального распределения случайных величин вероятность отказа P_f определяется по формуле:

$$P_f = 1 - \Phi(\beta), \qquad (3)$$

где:

$\Phi(\beta)$ – табулированный интеграл Гаусса,

$\beta = \frac{m_g}{s_g} = \frac{m_R - m_Q}{\sqrt{s_R^2 + s_Q^2}}$ – характеристика безопасности (число стандартов s_g, укладывающихся в интервале от $g = 0$ до $g = m_g$).

Выражение для определения характеристики безопасности можно записать в виде:

$$\beta = \frac{n-1}{\sqrt{n^2 \cdot \nu_R^2 + \nu_Q^2}}, \qquad (4)$$

где:

$n = \frac{m_R}{m_Q}$ – коэффициент безопасности;

ν_R – коэффициент вариации несущей способности;

ν_Q – коэффициент вариации нагрузочного эффекта.

Для определения моментов (математического ожидания и стандартного отклонения) несущей способности и нагрузочного эффекта может быть использован следующий подход. В нормах расчета на прочность приведены нормативные значения характеристик прочности материалов R_n, определенные экспериментальным путем из предположения нормального закона распределения с доверительной вероятностью превышения 0,95. Полагая, что расчетные значения характеристик прочности материалов R имеют доверительную вероятность превышения 0,99865, математическое ожидание и стандарт могут быть определены из системы:

$$\begin{cases} R_n = m_R - 1{,}64 \cdot s_R \\ R = m_R - 3 \cdot s_R \end{cases}, \qquad (5)$$

Тогда

$$m_R = R_n + 1{,}64 \cdot \frac{R_n - R}{1{,}36} = R_n \cdot \left(1 + 1{,}64 \cdot \frac{1 - 1/\gamma_m}{1{,}36}\right),$$

$$s_R = \frac{R_n - R}{1{,}36} = R_n \cdot \left(\frac{1 - 1/\gamma_m}{1{,}36}\right),$$

где $\gamma_m = \frac{R_n}{R}$ - коэффициент надежности (запаса) по материалу.

Аналогичный подход может быть использован для определения математического ожидания и стандартного отклонения ряда статических нагрузок.

Другой приближенный метод - метод надежности первого порядка (FORM) основан на разложении функции работоспособности в ряд Тейлора в окрестности математического ожидания случайных величин и сохранении только линейных членов разложения. Для нелинейной функции работоспособности $g=g(x_1, x_2,..., x_n)$ разложение в ряд Тейлора примет вид:

$$g \approx g\left(m_{x_1}, m_{x_2}, \ldots, m_{x_n}\right) + \sum_{i=1}^{n} \frac{\partial g}{\partial x_i}\left(m_{x_1}, m_{x_2}, \ldots, m_{x_n}\right)\left(x_i - m_{x_i}\right) + \tilde{W}, \qquad (6)$$

где $\tilde{W}$ – нелинейные члены разложения.

Разложение производится в окрестности центра распределения, при этом нелинейными членами можно пренебречь. Связано это с тем, что при незначительном удалении от центра распределения вклад нелинейных членов несущественный, а при значительном удалении значения функции распределения быстро затухают. Тогда исходную функцию работоспособности можно заменить линейной зависимостью:

$$g = g\left(m_{x_1}, m_{x_2}, \ldots, m_{x_n}\right) + \sum_{i=1}^{n} \frac{\partial g}{\partial x_i}\left(m_{x_1}, m_{x_2}, \ldots, m_{x_n}\right)\left(x_i - m_{x_i}\right) \qquad (7)$$

Числовые характеристики для линейной функции работоспособности будут определяться по формулам:

$$m_g = g\left(m_{x_1}, m_{x_2}, \ldots, m_{x_n}\right), \quad S_g{}^2 = \sum_{i=1}^{n}\left(\frac{\partial g}{\partial x_i}\left(m_{x_1}, m_{x_2}, \ldots, m_{x_n}\right)\right)^2 S_{x_i}^2. \qquad (8)$$

После нахождения числовых характеристик вычисляется вероятность отказа по формуле (3) настоящего приложения.

В некоторых практических задачах диапазон изменений случайных аргументов не настолько мал, чтобы в его пределах функция могла быть с достаточной точностью линеаризована. В этих случаях для проверки применимости метода и для уточнения полученных результатов может быть применен метод, основанный на сохранении в разложении функции не только линейных членов, но и некоторых последующих членов более высоких порядков и оценке погрешностей, связанных с этими членами.

Наиболее универсальными являются методы статистического моделирования, которые позволяет моделировать любой процесс, на протекание которого влияют случайные факторы. Основная идея методов – связь между вероятностными характеристиками различных случайных процессов и величинами, являющимися решениями задач математического анализа (например, значениями интегралов, решениями дифференциальных уравнений). Вместо вычисления ряда сложных аналитических выражений можно экспериментально определить значение соответствующих вероятностей или математических ожиданий. Необходимо отметить особенность методов, состоящую в том, что оценка погрешности вычислений носит вероятностный характер. В этом методе нельзя утверждать, что ошибка превысит какое-либо значение, а можно только указать границы, за которые ошибка не выйдет с вероятностью близкой к единице.

ПРИЛОЖЕНИЕ № 12
к руководству по безопасности
при использовании атомной энергии
«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций», утвержденному приказом Федеральной службы по экологическому, технологическому и атомному надзору
от 28 января 2015 г. № 26

Дополнительная информация по выполнению анализа надежности программного обеспечения

1. К числу основных факторов, влияющих на надежность ПО, относятся:

взаимодействие ПО с внешней средой (программно-технические средства, трансляторы, операционная система);

взаимодействие с человеком (разработчиком или пользователем);

организация ПО (проектирование, постановка задачи и способы их достижения и реализации) и качество его разработки. Этот фактор оказывает наибольшее влияние на надежность ПО;

тестирование.

2. Причинами отказов ПО могут являться ошибки в определении технических спецификаций для ПО, ошибки в программе, ошибки в вычислении, логические ошибки, ошибки ввода/вывода, ошибки компиляции, ошибки пользователей, дефекты загруженного в память модуля ПО, вызываемые физическими причинами, некорректное использование ПО, конфликт с операционной системой и другие.

Ошибки в ПО. При создании ПО далеко не всегда удается обнаружить и устранить все ошибки на стадии отладки. Поэтому ПО, несмотря на выполняемые процедуры обеспечения качества, может отказывать, если при эксплуатации возникают сочетания входных данных или режимов, не предусмотренных при отладке. Например, синтаксическая несовместимость может быть вызвана несоответствиями в способах задания данных на уровне языка программирования;

К ошибкам вычислений относятся, например, неправильные кодировки форм, ошибки в знаках (арифметических), непрерывное преобразование. В результате ошибок вычислений появляется отказ ПО в виде неверно рассчитанного результата.

К логическим ошибкам относится, например, неправильная передача управления, ошибки при формировании условия поиска. Логические ошибки приводят к искажению алгоритма обработки данных. К ним также относится семантическая несовместимость модулей используемого ПО, которая возникает, когда идентичные, синтаксически корректные символы используются для обозначения различных понятий.

К ошибкам ввода-вывода относятся, например, недопустимые форматы данных, неправильное указание размещения на экране или бумаге, неверное задание числа разрядов.

Ошибки компиляции могут быть вызваны дефектом компилятора.

К ошибкам пользователей относятся, например, неправильное понимание выводимых указаний, ввод недопустимых данных.

Дефекты загруженного в память модуля ПО, вызываемые физическими причинами, могут быть связаны, например, со сбоями в работе ячеек памяти, искажением информации в каналах связи.

Некорректное использование ПО может произойти, если ранее разработанное ПО применяется, например, после модификации технических средств.

Конфликт с операционной системой может возникнуть из-за ограничений параллельной работы и доступа к внешним ресурсам или нарушения требований к синхронизации, определяемых возможностями аппаратной части системы и пользовательского интерфейса. Так как управляемые процессы на АС имеют сложную многоуровневую природу, то ПО систем управления является многозадачным, когда необходимо одновременно реализовать сложные алгоритмы управления различными объектами, установленными на АС. При одновременном выполнении нескольких задач необходимо разделить ресурсы вычислительной системы в зависимости от их приоритета и различных событий, связанных с конкретными задачами. Это и может быть причиной конфликта.

3. Модели надежности ПО.

Модели надежности ПО принято разделять на аналитические и эмпирические.

Аналитические модели надежности ПО дают возможность рассчитывать количественные показатели надежности, основываясь на данных о поведении программы в процессе тестирования. Аналитические модели представлены двумя группами: динамические модели и статические модели. В динамических моделях поведение ПО (появление отказов) рассматривается во времени. В статических моделях появление отказов не связывают со временем, а учитывают только зависимость количества ошибок от числа тестовых прогонов (по области ошибок) или зависимость количества ошибок от характеристики входных данных (по области данных). К динамическим моделям относятся, в частности, модель надежности Шумана [10, 11, 12], модели роста надежности ПО или SGRM-модели [13]. К ста-

тическим моделям относятся, в частности, модель надежности Миллса [10, 14], модель надежности Липова [9, 10, 15], модель последовательности испытаний Бернулли [10, 11, 16].

Обе группы аналитических моделей являются экстраполяцией процесса тестирования на условия реальной эксплуатации ПО. Модели могут быть адекватны, только если условия тестирования и работы сравнимы, так как надежность ПО может достаточно сильно меняться в зависимости от этих условий.

Модели роста надежности ПО (наиболее популярные) базируются на результатах тестирования версий ПО в процессе его отладки (с исправлением выявленных ошибок) вплоть до окончательной проверки ПО. После выявления отказа ПО обычно корректируется, и поэтому его надежность меняется. Выявленный тренд изменения (обычно повышения) надежности экстраполируется для предсказания текущего уровня надежности и его изменения в будущем (наработки до следующего отказа и времени, требуемого для выявления всех ошибок в ПО). Модели роста надежности ПО основаны на двух основных предположениях: отказы фиксируются в хронологическом порядке, и все ошибки, обнаруженные в ПО, исправляются. При использовании этих моделей обычно не учитывается тяжесть выявленного отказа ПО, то есть не различаются реальные отказы и небольшие дефекты. Эти модели достаточно субъективны, а определяемые тренды надежности зависят от изменений в процессе отладки (например, возможно изменение состава группы специалистов, участвующих в отладке ПО, или интегрирование в ПО новых функциональных возможностей). Момент выявления последнего отказа ПО также оказывает достаточно большое влияние на характер тренда. В моделях может приниматься как допущение, что кривая повышения надежности стремится к уровню абсолютной надежности, так и допущение, что всегда будет оставаться некое остаточное количество отказов, которое вызывается дополнительными ошибками, вносимыми при исправлении ранее выявленных отказов ПО.

Эмпирические модели надежности ПО базируются на анализе структурных особенностей ПО. Они рассматривают зависимость показателей надёжности от числа межмодульных связей, количества циклов в модулях и т.д. Часто эмпирические модели не дают конечных результатов показателей надёжности, однако использование этих моделей позволяет выявлять взаимосвязь между сложностью ПО и его надежностью. Эти модели можно использовать на этапе проектирования ПО, когда осуществляется разбивка на модули и известна его структура.

Нормативный документ

Руководство по безопасности
при использовании атомной энергии

«Рекомендации по порядку выполнения анализа надежности систем и элементов атомных станций, важных для безопасности, и их функций»

РБ-100-15

Официальное издание
Ответственный за выпуск Синицына Т.В.
Верстка выполнена в ФБУ «НТЦ ЯРБ» в полном соответствии с приложением к приказу Федеральной службы по экологическому, технологическому и атомному надзору от 28 января 2015 г. № 26

Подписано в печать 05.02.2015.

ФБУ «Научно-технический центр
по ядерной и радиационной безопасности» (ФБУ «НТЦ ЯРБ»)
является официальным издателем и распространителем
нормативных актов Федеральной службы по экологическому, технологическому и атомному надзору (Приказ Федеральной службы по экологическому, технологическому и атомному надзору от 20.04.06 № 384)

Тираж 100 экз.
Отпечатано в ФБУ «НТЦ ЯРБ».
Москва, ул. Малая Красносельская, д. 2/8, корп. 5
Телефон редакции: 8-499-264-28-53

gost.e-ecolog.ru