ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
РОССИЙСКАЯ АКАДЕМИЯ РАКЕТНЫХ
И АРТИЛЛЕРИЙСКИХ НАУК

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ И БЕЗОПАСНОСТИ

ТЕХНИЧЕСКИЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ

Труды XX Всероссийской
научно-практической конференции

Том 2

НПО СПЕЦИАЛЬНЫХ МАТЕРИАЛОВ

Санкт-Петербург
2017

Актуальные проблемы защиты и безопасности: Труды XX Всероссийской научно-практической конференции РАРАН (3–6 апреля 2017 г.).

Издание ФГБУ «Российской академии ракетных и артиллерийских наук». Москва – 2017.

Составители и редакторы:
академик РАРАН, д.т.н., профессор В.А. Петров,
член-корреспондент РАН, академик РАРАН, д.т.н., профессор М.В. Сильников,
академический советник РАРАН, к.т.н., доцент А.М. Сазыкин,
к.т.н. А.С. Алешин.

Санкт-Петербург, 2017.

В девяти томах трудов конференции представлен широкий спектр концептуальных вопросов проблем защиты и безопасности: вооружение и военная техника, оружие, в том числе нелетального действия, системы обнаружения, наведения, связи, навигации и управления подразделениями, борьба с терроризмом, обнаружение и обезвреживание ВВ и радиоактивных веществ, безопасность особо важных объектов, ядерных центров, проблемы Военно-Морского Флота России, боевая экипировка и средства индивидуальной защиты, современные защитные материалы и конструкции, технологии их производства.

Том 1. «Вооружение, военная и специальная техника» 448 стр., 85 докладов, 193 автора.
Том 2. «Технические средства противодействия терроризму» 310 стр., 55 докладов, 114 авторов.
Том 3. «Бронетанковая техника и вооружение» 184 стр., 28 докладов, 70 авторов.
Том 4. «Проблемы Военно-Морского Флота России» 392 стр., 60 докладов, 87 авторов.
Том 5. «Направления совершенствования теории и практики боевого применения РВиА в операции (бою)» 294 стр., 79 докладов, 117 авторов.
Том 6. «Проблемы организации материально-технического обеспечения военной безопасности» 308 стр., 56 докладов, 97 авторов.
Том 7. «Комплексная безопасность на транспорте» 282 стр., 44 доклада, 72 автора.
Том 8. «Гуманитарные проблемы модернизации ВС РФ» 314 стр., 74 доклада, 95 авторов.
Том 9. «Специальный сборник»

Решением президиума ВАК Минобрнауки России от 26 октября 2007 г. в соответствии с Решением президиума ВАК от 22.06.2007 №27/55а (п. 3) изданиям Российской академии ракетных и артиллерийских наук предоставлено право опубликования научных результатов соискателей ученой степени доктора и кандидата наук.

Содержание (фрагмент)

УДК 51-74

ПРОГРАММНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОЕКТНОЙ ОЦЕНКИ ПОКАЗАТЕЛЕЙ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ ОПАСНЫХ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ

И.А. Можаева (ООО «НТЦ СЗМА»), **А.В. Струков** (АО «СПИК СЗМА»)

Введение

Основой для разработки программно-методического обеспечения проектной оценки показателей функциональной безопасности систем противоаварийной защиты (ПАЗ) опасных производственных объектов (ОПО) являются рекомендации нормативных документов Федеральной службы по экологическому, технологическому и атомному надзору (Ростехнадзор) при анализе опасностей, связанных с отказами технических устройств, использовать соответствующие методы теории надежности [1].

Выявление опасностей, оценка риска, определение необходимого снижения риска для современных технических систем представляет собой сложную комплексную задачу системного анализа, выполнение которого даже при наличии разработанного методического обеспечения невозможно или крайне затруднено без использования соответствующих программных средств. К таким программным средствам относится отечественный программный комплекс (ПК) «АРБИТР» [2], разработанный в «Специализированной инжиниринговой компании «Севзапмонтажавтоматика» и аттестованный Ростехнадзором РФ, аттестационный паспорт № 222 от 21 февраля 2007 г. Реализованный в ПК АРБИТР автоматизированный структурно-логический метод моделирования надежности, безопасности и технического риска позволяет на одном экранном интерфейсе использовать методики построения блок-схем, деревьев неисправностей, деревьев событий, а также методику «галстук-бабочка» [5], совмещающую на одном экранном интерфейсе перечисленные выше графические построения. Важным достоинством ПК АРБИТР является возможность оперативной адаптации алгоритмов и процедур для решения современных задач анализа функциональной безопасности.

1. Нормативные требования в области функциональной безопасности

Для современных промышленных процессов характерны возрастающие доля и значимость применения приборных систем безопасности (ПСБ), обычно называемых программируемыми электронными системами безопасности или системами противоаварийной защиты (ПАЗ). Общие подходы к вопросам обеспечения безопасности на всех стадиях жизненного цикла ПАЗ подробно изложены в серии стандартов ГОСТ Р МЭК 61508 [4].

Стандарты серии ГОСТ Р МЭК 61511 [3] устанавливают необходимость проведения анализа опасностей и риска ПСБ, применяемых в промышленных процессах и разработанных в соответствии с требованиями МЭК 61508. Указанные стандарты в целях реализации рациональной и последовательной технической политики устанавливают подход, минимизирующий стандартизацию для всех этапов жизненного цикла безопасности. Концепция жизненного цикла безопасности предполагает, что для каждой стадии этого процесса должны быть определены входы, выходы, а также действия по верификации правильности их определения.

Для этапа разработки и проектирования ПАЗ основной задачей (выходом) является проектирование систем ПАЗ, отвечающих требованиям к функциям безопасности и

соответствующих заданному уровню полноты безопасности (УПБ). Под полнотой безопасности понимается средняя вероятность того, что ПАЗ удовлетворительно выполняет требуемые функции безопасности при всех заданных условиях и в течение заданного периода времени [3,4].

Уровень полноты безопасности – УПБ (safety integrity level; SIL) – это дискретный уровень, принимающий одно из четырех возможных значений, определяющий требования к полноте безопасности для функций безопасности ПАЗ. Уровень полноты безопасности, равный 4, характеризует наибольшую полноту безопасности, уровень, равный 1, отвечает наименьшей полноте безопасности.

Входными данными для этапа разработки и проектирования ПАЗ являются требования по безопасности и УПБ, установленные в спецификации на основе распределения требований к безопасности. Эти входные требования являются выходами начальной стадии жизненного цикла безопасности – анализа опасностей и риска (рис.1).

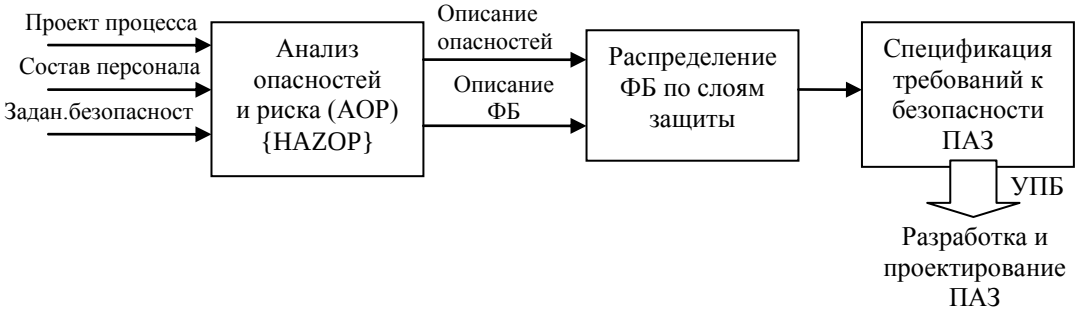

Рисунок 1 – Фрагмент жизненного цикла безопасности

Одним из методов верификации ПАЗ на стадии разработки и проектирования ПАЗ является оценка уровня полноты безопасности.

Первым шагом в оценке УПБ является определение минимально необходимых требований к архитектуре канала ПАЗ, определяемых требованиями к аппаратной отказоустойчивости. Аппаратная отказоустойчивость характеризует способность компонента (элемента, подсистемы) выполнять заданную функцию безопасности при наличии одного или более опасного отказа. Требования отказоустойчивости аппаратных средств представлены с минимальной избыточностью. В зависимости от интенсивности запросов на обслуживание, интервала между контрольными проверками для обеспечения заданного значения УПБ может возникнуть необходимость в дополнительной избыточности. В таблице 1 представлено минимально допустимое число отказов устройств.

Таблица 1 – Минимально допустимое число отказов [ГОСТ Р МЭК 61511-1, табл.5]

УПБ	Минимально допустимое число отказов		
	SFF (ДБО) < 60%	60% ≤ SFF (ДБО) ≤ 90%	SFF (ДБО) > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Специальные требования		

Из таблицы 1 видно, что минимальные требования к архитектуре канала ПАЗ главным образом определяются долей безопасных отказов (ДБО, SFF в английской аббревиатуре). При этом следует помнить, что методика расчета показателей безопасности ПАЗ, представленная в ГОСТ Р МЭК 61508-6, предполагает, что элемент ПАЗ имеет интенсивность опасных отказов менее 10^{-5} (1/час).

В качестве примеров архитектуры с отказоустойчивостью, равной 0, можно привести архитектуры 1oo1, 2oo2, 3oo3, с отказоустойчивостью 1 – архитектуры 1oo2, 1oo2D, 2oo3, с отказоустойчивостью 2 – архитектуру 1oo3.

Одним из разделов спецификации требований при проектировании системы ПАЗ являются требования к значению вероятности отказа при наличии запроса на выполнение функции безопасности. Эти требования должны быть проверены расчетом, при этом значение вероятности отказа должно быть не более целевой меры отказов, установленной в спецификациях требований к безопасности.

Для функций безопасности ПАЗ, выполняемых в режиме по запросу, целевая мера отказов выражается в терминах средней вероятности отказа (*PFDavg*) выполнения по запросу предусмотренной функции безопасности для режима низкой интенсивности запросов или в терминах средней частоты опасных отказов (*PFH*) для режима с высокой интенсивностью запросов или режима с непрерывным запросом (табл.2).

Таблица 2 – Уровни полноты безопасности [3]

Уровень безопасности (SIL)	**Режим с низким уровнем требований по требованию функции безопасности** (средняя вероятность отказа в выполнении заданной функции безопасности по требованию)	**Режим с высоким уровнем требований по требованию функции безопасности** (вероятность опасного отказа в течение одного часа в режиме непрерывной работы)
4	$\geq 10^{-5}$ PFD $<10^{-4}$	$\geq 10^{-9}$ PFH $<10^{-8}$
3	$\geq 10^{-4}$ PFD $<10^{-3}$	$\geq 10^{-8}$ PFH $<10^{-7}$
2	$\geq 10^{-3}$ PFD $<10^{-2}$	$\geq 10^{-7}$ PFH $<10^{-6}$
1	$\geq 10^{-2}$ PFD $<10^{-1}$	$\geq 10^{-6}$ PFH $<10^{-5}$

Количественная оценка вероятности отказа *PFDavg* выполняется для каждой функции безопасности ПАЗ, так как им могут быть свойственны различные виды отказов компонентов и архитектур ПАЗ в части резервирования.

2. Методологическая и алгоритмическая основы оценки вероятности отказа на запрос

По физическому смыслу *PFDavg* есть средняя неготовность системы на интервале между контрольными проверками. Расчет *PFDavg* основан на учете двух типов неготовности канала:

1 – неизвестная, когда простой ПАЗ вызван DD (опасными необнаруженными) или DU (опасными обнаруженными) отказами;

2 – неизвестная, когда простой вызван тестовыми проверками, плановыми ремонтами и т.п., когда можно включить другие слои защиты.

Для понимания сущности процесса рассмотрим три типичных вида функционирования ПАЗ:

1. В межконтрольный период (период между контрольными проверками) не было опасных отказов (рис.1).

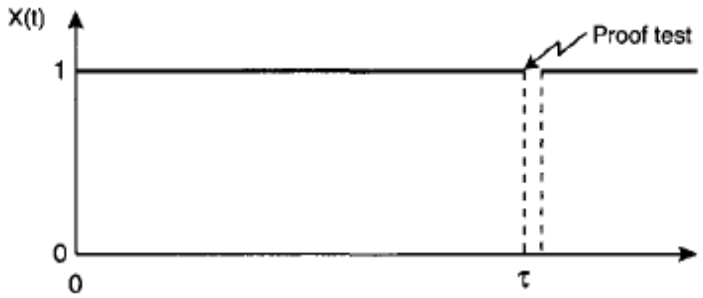

Рисунок 1 – В межконтрольный период (0,τ) опасных отказов не было [6]

После проведения контрольных проверок (1-2 часа) система ПАЗ снова готова к работе.

2. В межконтрольный период произошел опасный обнаруживаемый отказ (DD-отказ) (рис.2).

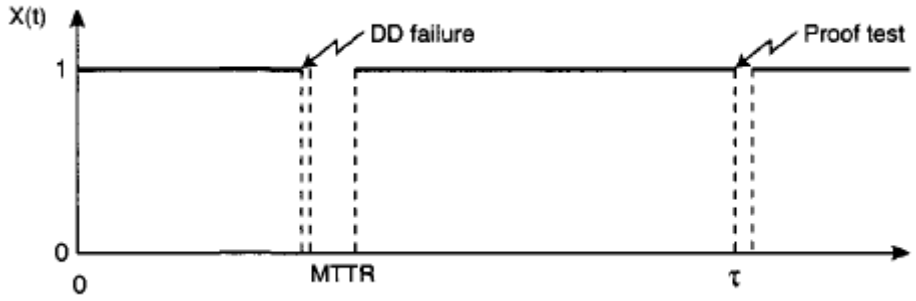

Рисунок 2 – В межконтрольный период (0,τ) обнаружен опасный отказ [6]

При DD-отказе ПАЗ переходит в состояние 0, теряет возможность выполнять функции безопасности (ФБ). Восстановление работоспособности происходит за среднее время восстановления MTTR, после чего ПАЗ работает как новая система. Обычно MTTR=5-10час.

3. В межконтрольный период произошел опасный необнаруживаемый отказ (DU-отказ) (рис.3).

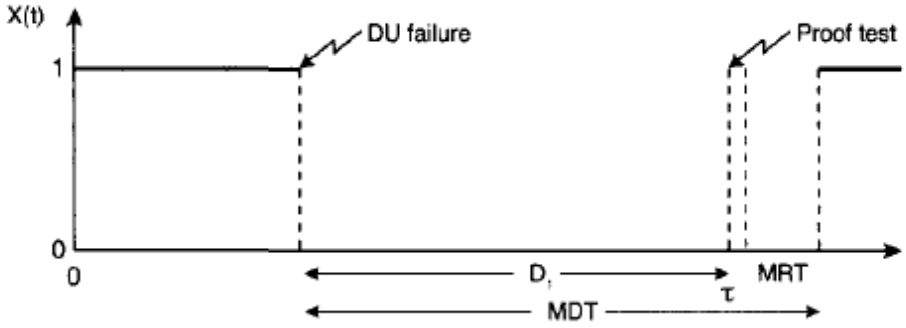

Рисунок 3 – В межконтрольный период (0,τ) опасный отказ не обнаружен [6]

Так как опасный отказ является необнаруженным, то с момента его появления до времени начала тест-проверок ПАЗ находится в состоянии скрытого отказа. Время простоя относительно возможности выполнения ФБ равно D_t. При обнаружении отказа тест-проверками осуществляется восстановление работоспособности ПАЗ за среднее время ремонта MRT. Общее (среднее) время простоя MDT=D_t+MRT.

Будем считать, что за время тест-проверок вероятность возникновения двух или более опасных отказов пренебрежительно мало.

При периодических контрольных проверках *PFD(t)* как функция времени и ее среднее значение *PFDavg* имеют вид, показанный на рис.4

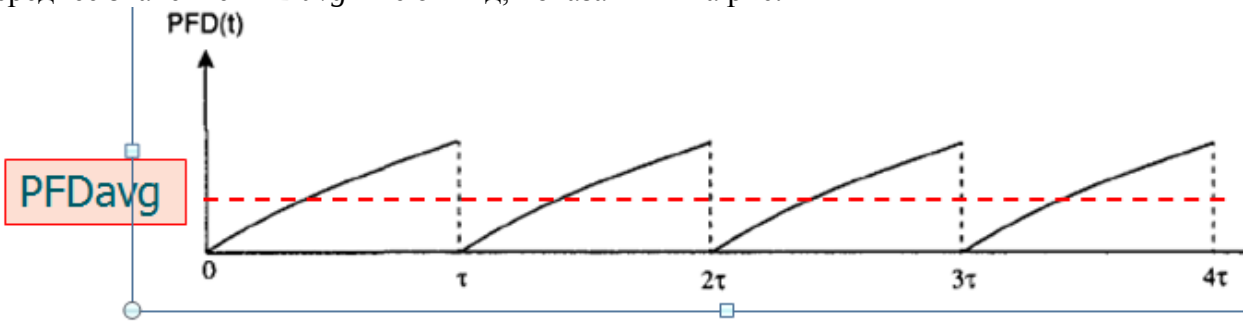

Рисунок 4– Вероятность отказа на запрос PFD(t) в межконтрольные периоды и ее среднее значение PFDavg []

Возможны две интерпретации PFDavg:

- Если запрос на ФБ происходит в случайное время, то PFDavg есть средняя вероятность того, что ПАЗ не готов реагировать и реализовывать ФБ.
- PFDavg равно среднему относительному времени, когда ПАЗ не готов выполнять ФБ. Количественно эта вероятность (неготовность) есть отношение среднего времени простоя $E[D(0,\tau)]$ к величине межпроверочного интервала τ, то есть

$$E[D(0,t)] = PFD_{avg} \cdot t \quad PFD_{avg} = \frac{E[D(0,\tau)]}{\tau}, \tag{1}$$

Среднее время простоя на межпроверочном интервале определяется коэффициентом простоя *F(t)* и вычисляется как

$$E(D_1) = \int_0^\tau F(t)dt, \tag{2}$$

Тогда

$$PFD_{avg} = \frac{1}{\tau}\int_0^\tau PFD(t)dt = \frac{1}{\tau}\int_0^\tau F(t)dt = 1 - \frac{1}{\tau}\int_0^\tau R(t)dt, \tag{3}$$

где, $R(t) = 1 - F(t)$ – коэффициент готовности канала.

Для иллюстрации метода расчета *PFDavg* для каналов с различной архитектурой с учетом того, что на практике часто $MTTR \ll \tau$ и $MRT \ll \tau$, вместо коэффициента готовности канала будем использовать вероятность безотказной работы (ВБР) канала.

Архитектура 1oo1

При экспоненциальном законе распределения времени до отказа ВБР $R(t) = \exp(-\lambda_{DU}t)$, где λ_{DU} – интенсивность опасных (D) необнаруженных (U) отказов.

Тогда PFD_{avg} канала рассчитывается по формуле

$$PFD_{avg}^{1oo1} = 1 - \frac{1}{\tau}\int_0^\tau R(t)dt = 1 - \frac{1}{\tau}\int_0^\tau e^{-\lambda_{DU}t}dt = 1 - \frac{1}{\lambda_{DU}t}(1 - e^{-\lambda_{DU}t}) \tag{4}$$

При разложении в ряд Тейлора показательной функции имеем

$$\begin{aligned} PFD_{avg}^{(1oo1)} &= 1 - \frac{1}{\lambda_{DU}t}\left(\lambda_{DU}t - \frac{(\lambda_{DU}t)^2}{2} + \frac{(\lambda_{DU}t)^3}{3!} - \frac{(\lambda_{DU}t)^4}{4!} + \ldots\right) = \\ &= 1 - \left(1 - \frac{\lambda_{DU}t}{2} + \frac{(\lambda_{DU}t)^2}{3!} - \frac{(\lambda_{DU}t)^3}{4!} + \ldots\right) \end{aligned} \tag{5}$$

При малых значениях вероятности отказа, т.е. $F(t) \approx \lambda_{DU}t \ll 0.1$ имеем

$$PFD_{avg}^{(1oo1)} \approx \frac{\lambda_{DU}t}{2} \tag{6}$$

Архитектура 1oo2

Оба канала характеризуются интенсивностями опасных необнаруживаемых отказов λ_{DU}. Оба канала имеют одинаковый межпроверочный интервал τ. Полагается, что функция безопасности выполняется, если работоспособен хотя бы один канал. ВБР такой структуры

$$R(t) = 2e^{-\lambda_{DU}t} - e^{-2\lambda_{DU}t}. \tag{7}$$

Тогда средняя вероятность отказа на запрос для архитектуры 1oo2 рассчитывается по формуле

$$\begin{aligned} PFD_{avg}^{(1oo2)} &= 1 - \frac{1}{\tau}\int_0^\tau (2e^{-\lambda_{DU}t} - e^{-2\lambda_{DU}t})dt = 1 - \frac{2}{\lambda_{DU}\tau}(1 - e^{-\lambda_{DU}\tau}) + \\ &+ \frac{1}{2\lambda_{DU}\tau}(1 - e^{-2\lambda_{DU}\tau}) \end{aligned}. \tag{8}$$

При малых значениях вероятности отказа, а также используя разложение в ряд Тейлора показательной функции, выражение для приближенных (8) можно записать в виде

$$PFD_{avg}(1oo2) \approx \frac{(\lambda_{DU}t)^2}{3}. \quad (9)$$

Архитектура 2oo3

Все каналы характеризуются идентичными интенсивностями опасных необнаруживаемых отказов λ_{DU} и имеют одинаковый межпроверочный интервал τ. Полагается, что функция безопасности выполняется, если работоспособны два любых канала. ВБР такой структуры

$$R(t) = 3e^{-2\lambda_{DU}t} - 2e^{-3\lambda_{DU}t}. \quad (10)$$

Тогда средняя вероятность отказа на запрос для архитектуры 2oo3 рассчитывается по формуле

$$PFD_{avg}^{(2oo3)} = 1 - \frac{1}{\tau}\int_0^{\tau}(3e^{-2\lambda_{DU}t} - 2e^{-3\lambda_{DU}t})dt = 1 - \frac{3}{2\lambda_{DU}\tau}(1 - e^{-2\lambda_{DU}\tau}) + \\ + \frac{2}{3\lambda_{DU}\tau}(1 - e^{-3\lambda_{DU}\tau}). \quad (11)$$

Для приближенных расчетов используется формула

$$PFD_{avg}^{(2oo3)} \approx (\lambda_{DU}\tau)^2. \quad (12)$$

Алгоритмическая основа методики оценки *PFDavg* различных архитектур – приближенные формулы стандарта IEC 61508-6 для расчета *PFDavg* простых типовых архитектур 1oo1 и 1oo2D.

Основные допущения методики расчета *PFDavg*:

- все каналы имею постоянную интенсивность отказов в течение срока службы системы;
- все резервированные каналы имеют одинаковые интенсивности отказов и диагностический охват DC;
- интервал времени между тестовыми испытаниями должен быть, по крайней мере, на порядок больше времени ремонта MRT;
- ожидаемый интервал между запросами на выполнение ФБ должен быть, по крайней мере, на порядок больше интервала времени между тестовыми испытаниями;
- подсистема датчиков (ввода) включает фактические датчики и все другие элементы и кабели, вплоть до (но не включая) элементов, где сигналы впервые комбинируются при помощи голосования или другого процесса обработки (например, конфигурация для двух каналов датчиков приведена на рис.5);

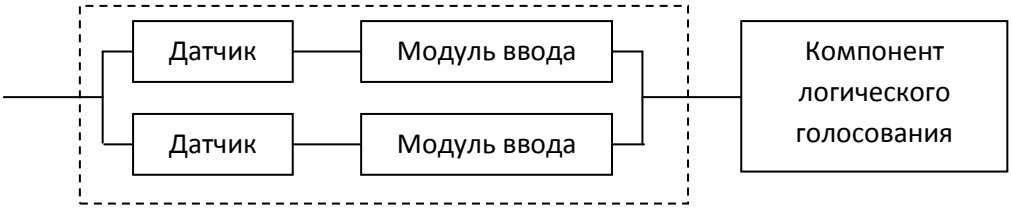

Рисунок 5 – Пример конфигурации для двух каналов датчиков [4]

- логическая подсистема включает компоненты, на которых происходит первое комбинирование сигналов, и все остальные компоненты вплоть до (и включая) компонентов, на которых окончательные сигналы выдаются на подсистему конечных элементов;

- подсистема конечных элементов (вывода) включает все компоненты и кабели, которые связаны с обработкой окончательных сигналов от логической подсистемы, включая компоненты окончательного исполнения;
- интервал на проведение проверочного испытания должен быть как минимум на порядок больше, чем среднее время ремонта;
- для каждой подсистемы существует свой интервал проверочного испытания и среднее время на проведение ремонта;
- ожидаемый интервал между запросами на выполнение функции безопасности должен быть как минимум на порядок больше, чем среднее время ремонта;
- если отказ блока питания к обесточиванию системы безопасности и инициирует переход системы в безопасное состояние, то блок питания не влияет на среднюю вероятность отказа по запросу системы безопасности; если для перехода в безопасное состояние на систему подается питание или блок питания имеет режимы неисправности, которые могут вызвать небезопасную работу системы безопасности, то блок питания должен учитываться при расчетах;
- при использовании терминального канала он ограничивается только той частью рассматриваемой системы, которая обычно представляет собой подсистему датчиков, логики или конечных элементов.

Основная идея IEC 61508-6 состоит в расчете *PFDavg* канала, представленного как один элемент, характеризуемый средней групповой частотой опасных отказов λ_{DG} и эквивалентным групповым временем простоя t_{GE}

$$PFD_{avg}^{(G)} = F(\lambda_{DG}, t_{GE}, MTTR, MRT).$$

Как отмечалось выше, по физическому смыслу PFD есть средняя неготовность системы на интервале между контрольными проверками.

Анализ построения формул (5), (8), (11) позволяет по аналогии с алгоритмом оценки показателей надежности восстанавливаемых систем, реализованном в ПК АРБИТР [2], обосновать следующий подход к оценке системных показателей функциональной безопасности *PFDsys*.

Так как состояние системы безопасности полностью определяется состоянием ее элементов, тогда системный показатель функциональной безопасности рассчитывается с использованием структурной функции системы, то есть

$$PFD_{sys} = P\{ PFD_1, ..., PFD_i, ..., PFD_n \},$$
$$PFH_{sys} = P\{ PFH_1, ..., PFH_i, ..., PFH_n \},$$

где *PFDsys, PFHsys* – системные показатели функциональной безопасности;
PFDi, PFHi – показатели функциональной безопасности *i-го* компонента;
P{...} – структурная функция системы.

3. Методика расчета средней вероятности отказа на запрос

В общем виде методика расчета *PFDavg* канала включает в себя следующие шаги:

I. Формирование исходных данных, необходимых для расчета вероятностей отказа на запрос для всех элементов системы.

II. Расчет с помощью утилиты вероятностей отказа на запрос структур с архитектурой 1oo1 и 1oo2D по формулам стандарта ГОСТ Р МЭК 51508-6.

III. Построение схемы функциональной целостности (СФЦ) в виде структурной схемы надежности или дерева неисправностей системы безопасности и моделирование надежности системы безопасности с учетом особенностей построения голосующих групп в программной среде ПК АРБИТР.

Формирование исходных данных, необходимых для расчета показателей функциональной безопасности, осуществляется на основе анализа документации производителей компонентов.

Для расчета показателей функциональной безопасности архитектур 1oo1 и 1oo2D в программной среде ПК АРБИТР разработана утилита «Расчет вероятности отказа на запрос *PFDavg*». Экранный интерфейс утилиты представлен на рис.6.

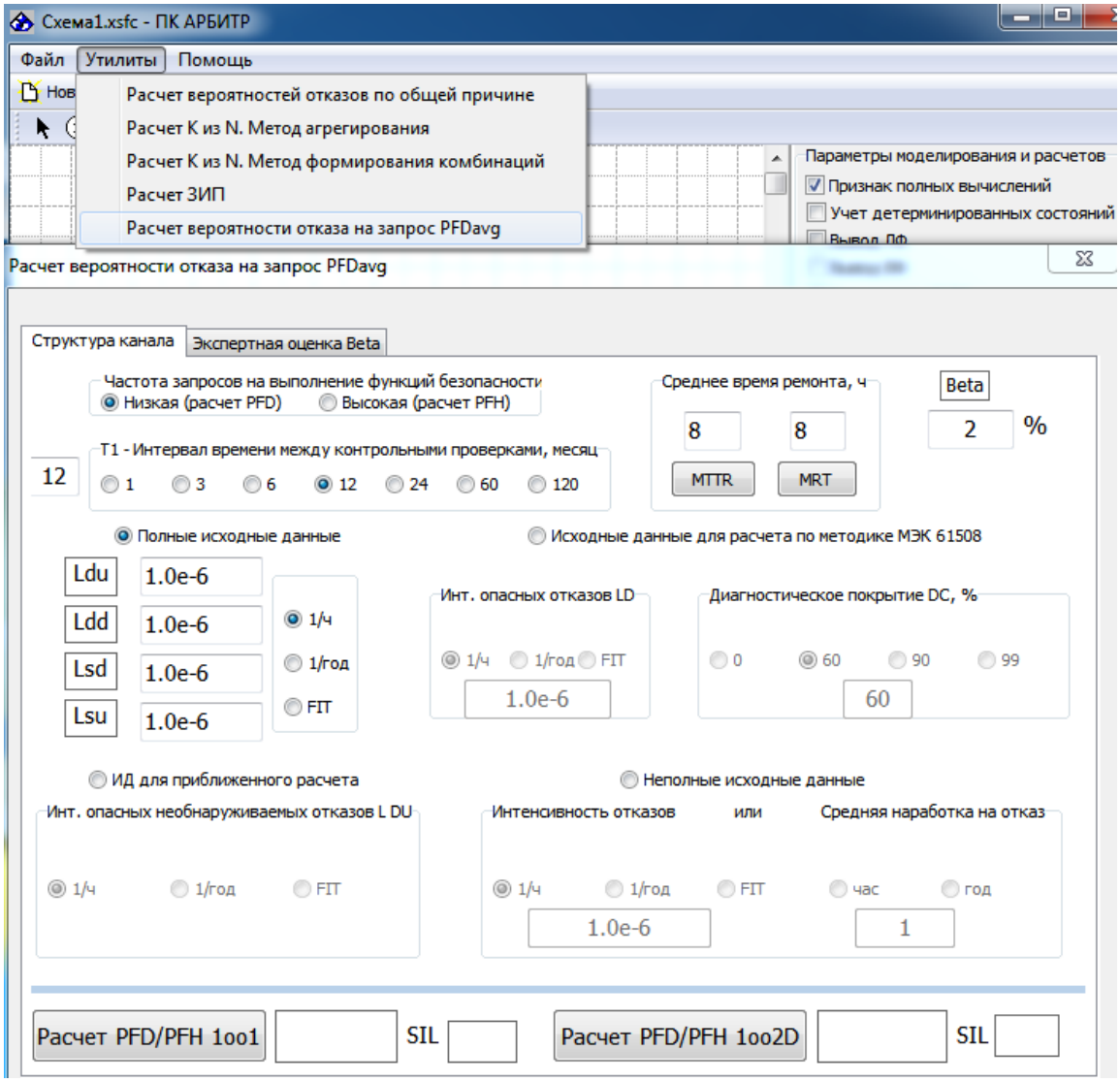

Рисунок 6 – Утилита «Расчет вероятности отказа на запрос *PFDavg*»

Для ввода исходных данных и расчета показателей на странице «Структура канала» выбираются следующие режимы и вводятся исходные данные:

- частота запросов на выполнение функций безопасности: низкая (расчет *PFD*), если частота запросов не выше 1 раза в год, высокая (расчет *PFH*) – если частота запросов выше 1 раза в год.

- интервал времени между контрольными проверками (в тексте стандартов серии МЭК 61508 обозначен через T_1 , в месяцах). Для высокой частоты запросов интервал T_1 обычно выбирается из дискретного ряда 1, 3, 6, 12 месяцев, для низкой частоты запросов – из ряда 6, 12, 24 и 120 месяцев. По умолчанию задается 12 месяцев.

- среднее время восстановления (MTTR) и средняя продолжительность ремонта (MRT). Обычно по умолчанию задается MTTR= MRT=8ч.

Исходные данные об интенсивностях отказов для отдельных компонентов систем ПАЗ обычно приводятся производителями компонент в «Руководстве по функциональной безопасности». Учитывая, что разные производители и вендеры по-разному формируют данные по надежности и безопасности, в утилите предусмотрены четыре режима ввода исходных данных об интенсивностях отказов компонент.

Полные исходные данные включают в себя следующие данные об интенсивностях отказов:

- опасных необнаруженных – *Ldu*;
- опасных обнаруженных– *Ldd*;
- безопасных необнаруженных – *Lsu*;
- безопасных обнаруженных – *Lsd*.

Значения интенсивностей отказов могут иметь размерности «1/час», «1/год» или FIT (10^{-9} 1/час).

Исходные данные для расчета по методике МЭК 61508 включают в себя:

- данные об интенсивностях опасных отказов *Ld*;
- значение диагностического охвата, в %.

Значения интенсивности опасных отказов могут иметь размерности «1/час», «1/год» или FIT.

Исходные данные для приближенного расчета включают в себя данные об интенсивностях опасных необнаруженных отказов *Ldu*.

В этом случае для структуры 1oo1 $PFD_{1oo1} \approx \frac{L_{du}T_1}{2}$, для структуры 1oo2D с учетом отказов по общей причине $PFD_{1oo2D} \approx \frac{\beta L_{du}T_1}{2}$, где β – параметр бета-модели ООП.

Неполные исходные данные предполагают использование следующих допущений:

- при задании интенсивности отказов

Ldu = Ldd = Lsu = Lsd = L/4, где *L* – общая (суммарная) интенсивность отказов.

Значения интенсивности отказов могут иметь размерности «1/час», «1/год» или FIT.

- при задании средней наработки на отказ To $L = 1/To$.

Пересчет размерности производится с условием 1 год = 8760 час.

Формирование исходных данных состоит в оценке показателей безопасности каналов с архитектурами 1oo1 и 1oo2D по формулам, приведенным в табл.3 и 4.

Таблица 3 – Показатели безопасности канала с архитектурой 1oo1

Частота запросов	Формула расчета [2]
Низкая	$PFD_{1oo1} = \lambda_{DU} \cdot (\frac{T_1}{2} + MTTR) + \lambda_{DD} \cdot MRT$, $PFD_{1oo1} \approx Ldu \cdot \frac{T1}{2}$.
Высокая	$PFH_{1oo1} = \lambda_{DU}$

Таблица 4 – Показатели безопасности канала с архитектурой 1oo2D

Частота запросов	Формула расчета [2]
Низкая	$PFD_{1oo2D} = 2(1-\beta)L_{DU}((1-\beta)L_{DU} + (1-\beta_D)L_{DD} + L_{SD})t_{CE'}t_{GE'} + 2(1-K)L_{DD}t_{CE'} + \beta L_{DU}(\frac{T_1}{2} + MRT)$
Высокая	$PFH_{1oo2D} = 2(1-\beta)L_{DU}((1-\beta)L_{DU} + (1-\beta_D)L_{DD} + L_{SD})t_{CE'} + 2(1-K)L_{DD} + \beta L_{DU}$

где $t_{CE'} = \dfrac{\lambda_{DU}(\frac{T_1}{2} + MRT) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + (\lambda_{DD} + \lambda_{SD})}$;

$t_{GE'} = \dfrac{T_1}{3} + MRT$;

$\beta_D = \dfrac{\beta}{2}$ – параметр β-модели учета влияния ООП, равный доле обнаруженных диагностическими тестами ООП. Обычно полагают, что доля необнаруженных ООП $\beta = 2 \cdot \beta_D$; K = 0.98.

После построения схемы функциональной целостности (СФЦ) в виде структурной схемы надежности или дерева неисправностей системы безопасности рассчитанные с помощью утилиты вероятности отказов на запрос вводятся как вероятностные параметры функциональных вершин.

4. Пример. Решение задачи из стандарта МЭК 61508-6

На рис.7 приведена архитектура системы безопасности для режима низкой интенсивности запросов из стандарта МЭК 61508-6.

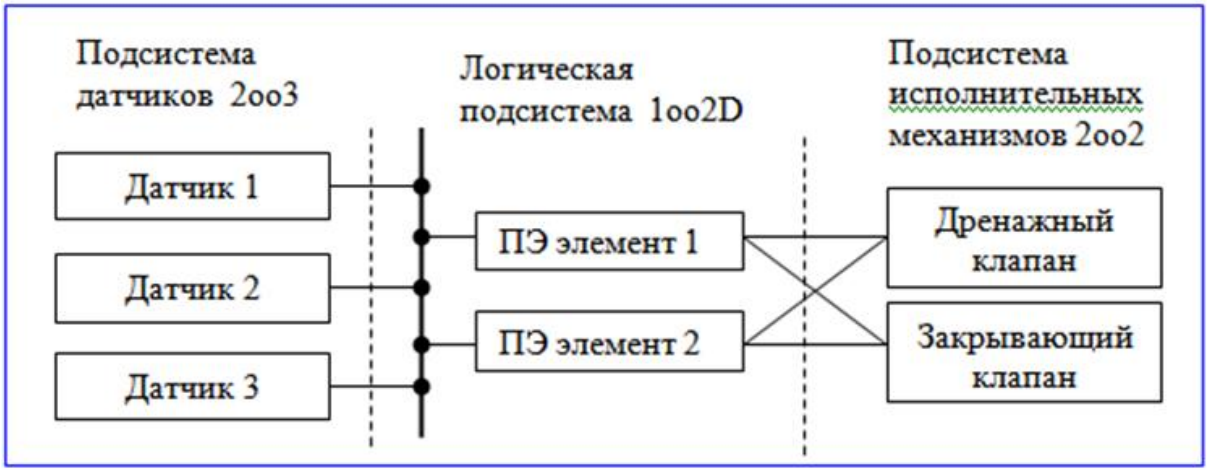

Рисунок 7 – Система безопасности из стандарта 61508-6

Анализируемая система безопасности включает в себя голосующую группу аналоговых датчиков давления (датчики 1-3) с архитектурой 2oo3 на выходе. Логическая подсистема состоит из двух программируемых электронных элементов с архитектурой 1oo2D, управляющие сигналы которых поступают на дренажный и закрывающий клапаны. Для обеспечения функции безопасности необходима работа обоих клапанов.

Согласно методики расчета, описанной выше в п.3, решение примера содержит три шага.

Шаг 1. Формирование исходных данных, необходимых для расчета вероятностей отказа на запрос для всех элементов системы.

Исходные данные по компонентам системы безопасности приведены в табл.4.

Таблица 4 – Исходные данные по компонентам для примера 1

Наименование элементов	λ_D, 1\ч	DC,%	β,%	β_D,%	T_1, мес	MTR, ч
Датчики	2.5E-6	90	20	10	12	8
ПЭ логические элементы	5.0-6	99	2	1	12	8
Дренажный клапан	2.5E-6	60	-	-	12	8
Закрывающий клапан	5.0-6	60	-	-	12	8

Шаг 2. Расчет с помощью утилиты вероятностей отказа на запрос структур с архитектурой 1oo1 и 1oo2D.

Для расчета используется утилита «Расчет вероятности отказа на запрос». Экранный интерфейс страницы утилиты после ввода исходных данных и расчета *PFDavg* аналоговых датчиков давления представлен на рис.8.

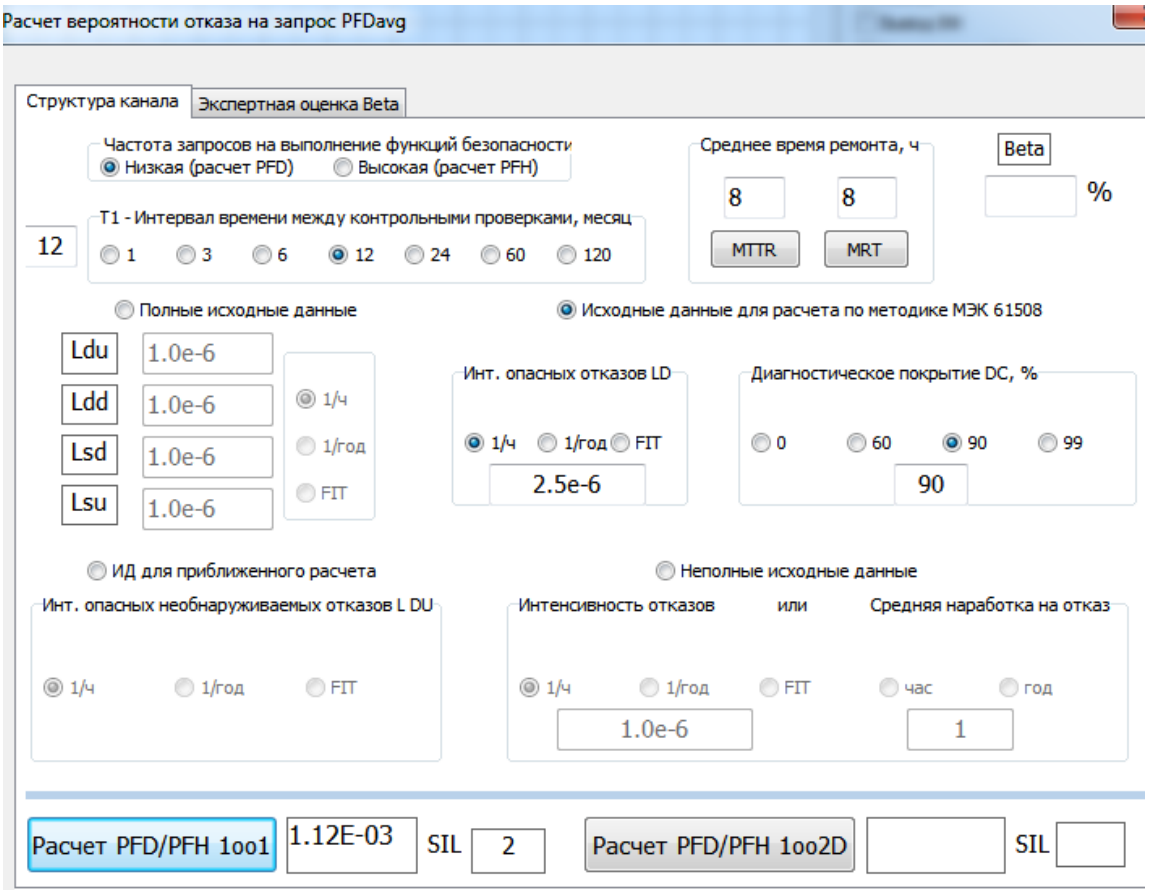

Рисунок 8 – Экранный интерфейс утилиты для расчета *PDFavg* датчика

На рис.8 показано, что для расчета *PFDavg* датчика в утилиту введены следующие исходные данные:

- частота запросов на выполнение функций безопасности – низкая;
- интервал времени между контрольными проверками T_1 – 12 месяцев;
- среднее время ремонта и восстановления (MTTR, MRT) – 8ч;
- исходные данные об интенсивностях отказов (по методике МЭК 61508): интенсивность опасных отказов λ_D=2.5E-06 (1/ч) и охват диагностикой DC=90%.

Результатом расчета *PFDavg* датчика с помощью утилиты является получение значения вероятности 1.12E-03, что указывает на возможность использования датчика в системах, отвечающих требованию уровня SIL2.

В табл.5 представлены результаты расчетов для всех элементов системы безопасности.

Таблица 5 – Результаты расчетов *PDFavg* элементов системы безопасности

Наименование элементов	Архитектура	*PFDavg*
Датчики	1oo1	1.115·E-03
ПЭ логические элементы	1oo2D	1.042·E-05
Дренажный клапан	1oo1	4.40·E-03
Закрывающий клапан	1oo1	8.80·E-03

Шаг 3. Построение схемы функциональной целостности.

Схема функциональной целостности (СФЦ) системы безопасности состоит из СФЦ подсистемы датчиков, СФЦ логической подсистемы и СФЦ подсистемы конечных (исполнительных) механизмов.

На рис.9 представлены фрагменты экранного интерфейса построения СФЦ подсистемы датчиков.

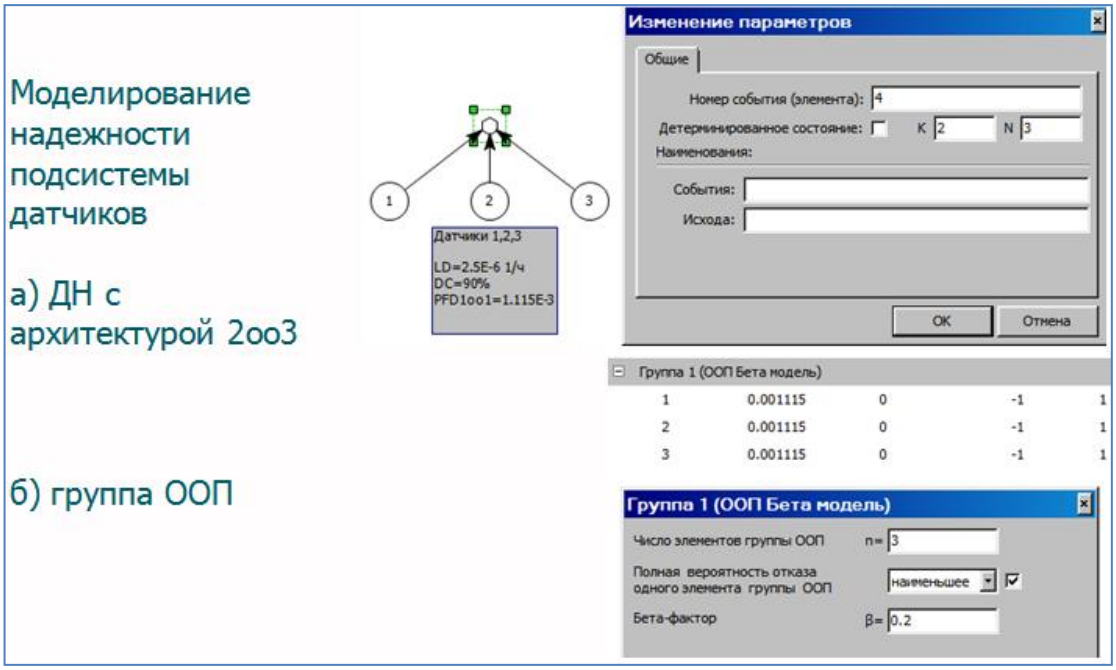

Рисунок 9 – Построения СФЦ подсистемы датчиков

На рис.9 показано, что для формирования дерева неисправностей (ДН) структуры «2oo3» используется вкладка «Изменение параметров», позволяющая задать параметры структуры «К из N» (в нашем случае – «2oo3»). Учет отказов по общей причине (ООП) и ввод параметров бета-модели осуществляется с помощью вкладок «Изменение группы» и «Параметры модели». В качестве парметров функциональных вершин №1, 2 и 3 используются значения вероятностей *PFDavg*, указанных в табл.5.

Фрагмент экранного интерфейса построения СФЦ ДН подсистемы исполнительных механизмов показан на рис.10.

Так как для нормальной работы системы безопасности требуется работоспособность дренажного и закрывающего клапанов, то функциональные вершины № 6 и 7 соединены по логике «ИЛИ».

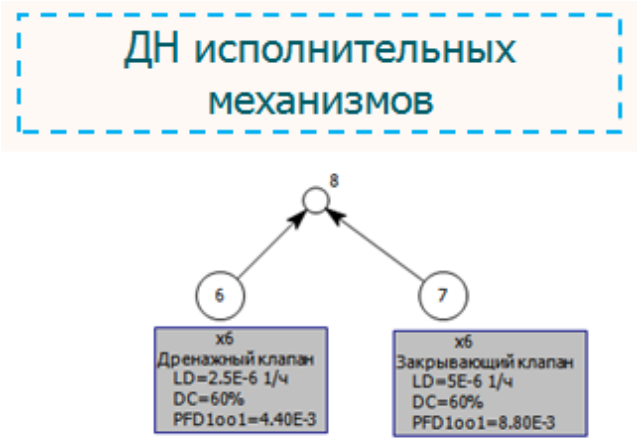

Рисунок 10 – Построение СФЦ ДН подсистемы исполнительных механизмов

На рис.10 вероятностные параметры вершин № 6 и 7 (*PFDavg* клапанов) рассчитаны с помощью утилиты (табл.5).

На рис.11 показана окончательная СФЦ системы безопасности и результаты моделирования.

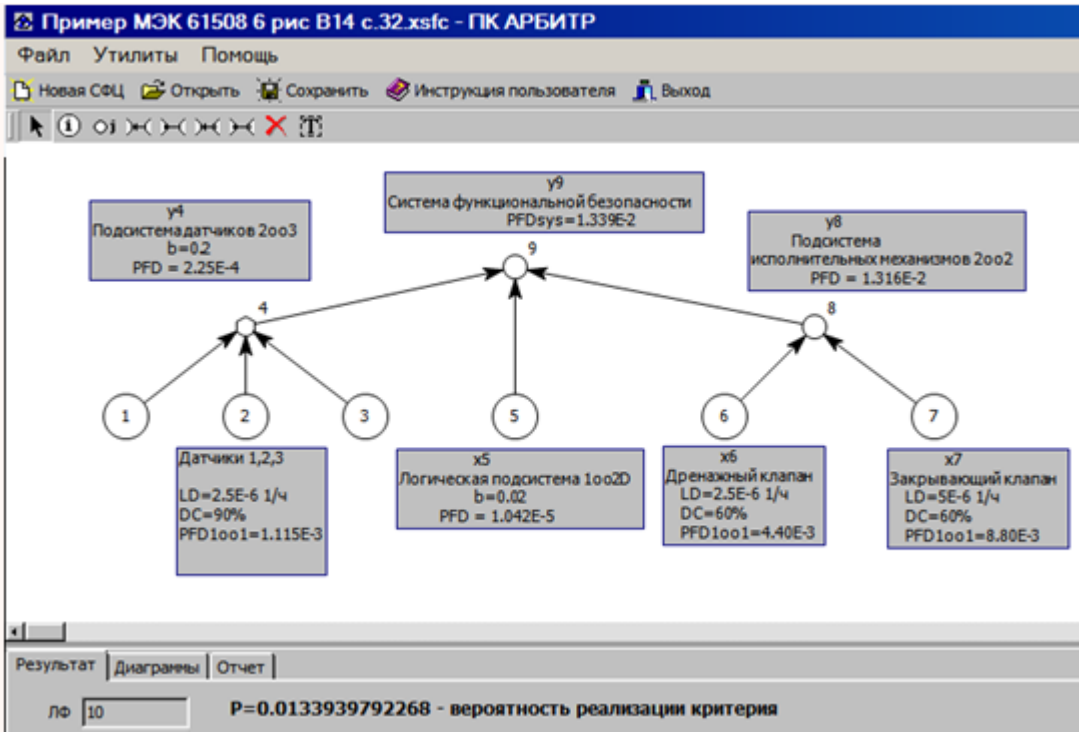

Рисунок 11 – СФЦ системы безопасности

Как видно из рис.11, *PFDavg* системы безопасности составляет 1.33E-2, что соответствует уровню полноты безопасности SIL1 и совпадает с решением, приведенным в [61508-6].

Для решения задачи обеспечения более высокого уровня полноты безопасности следует воспользоваться результатами анализа значимости элементов системы безопасности, которые представлены в табл.6.

Таблица 6 – Анализ элементов системы безопасности. Таблица характеристик элементов

Номер эл-та	**P эл-та**	**Значимость эл-та**	**Отрицательн. вклад**	**Положительн. вклад**	**Наименование**
1	0.000892	0.0017585	1.5686E-6	0.001757	ДД1
2	0.000892	0.0017585	1.5686E-6	0.001757	ДД2
5	1.042E-5	0.98662	1.0281E-5	0.98661	ЛП
6	0.0044	0.99097	0.0043603	0.98661	Клапан дренажн.
7	0.0088	0.99537	0.0087592	0.98661	Клапан закрыв.
3	0.000892	0.0017585	1.5686E-6	0.001757	X3 (ДД3)
13	0.000223	0.98683	0.00022006	0.98661	CCF1[X1,X2,X3]

Как видно из табл.6 наибольшую значимость имеют элементы № 6, 7 и 13. С точки зрения снижения величины *PFDavg* системы безопасности важным показателем является отрицательный вклад элементов, то есть влияние снижения их собственной вероятности отказа на системный показатель. Здесь также следует обратить внимание на элементы № 6, 7 и 13, обеспечивающие максимальный отрицательный вклад. Таким образом, для повышения уровня полноты безопасности анализируемой структуры следует либо подобрать исполнительные механизмы с более низкой вероятностью *PFDavg*, либо

реализовать организационные или инженерные методы снижения влияния отказов по общей причине в подсистеме датчиков (элемент №13).

ЛИТЕРАТУРА

1. Руководство по безопасности «Методические основы по проведению анализа опасностей и оценки риска аварий на опасных производственных объектах». Серия 27. Выпуск 16.– М.: ЗАО «Научно-технический центр исследований проблем промышленной безопасности, 2016. 56 с.
2. Можаев А.С. Аннотация программного средства «АРБИТР» (ПК АСМ СЗМА) // Вопросы атомной науки и техники. Серия «Физика ядерных реакторов». Раздел «Аннотации программных средств, аттестованных Ростехнадзором РФ»: науч.-техн. сб.– М. : РНЦ «Курчатовский институт», 2008. – Вып. 2/2008. – С.105-116.
3. ГОСТ Р МЭК 61511. Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1-3. 2013.
4. ГОСТ Р МЭК 61508. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1-7. 2012.
5. Можаев И.А., Нозик А.А., Струков А.В. Программная реализация методов количественного анализа риска аварий опасных производственных объектов на основе логико-вероятностного и логико-детерминированного подходов // Наука и безопасность. 2016. №2/20. С.26–36.
6. Rausand M. Reliability of Safety-Critical Systems: Theory and Applications. Wlley. 2014. 448 p.