**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» МАИ**

На правах рукописи

УДК: 519.873+519.81+519.248:681.51] (043)

Савельев Артем Сергеевич

РАЗРАБОТКА МЕТОДИКИ СНИЖЕНИЯ ВЕРОЯТНОСТИ ПРЕЖДЕВРЕМЕННОГО ПЕРЕХОДА НА РЕЗЕРВНЫЙ РЕЖИМ КОМПЛЕКСНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ГРАЖДАНСКОГО САМОЛЕТА ПО ПРИЧИНЕ ОТКАЗОВ СОПРЯГАЕМОГО ОБОРУДОВАНИЯ

Специальность 2.3.1. Системный анализ, управление и обработка информации (авиационная и ракетно-космическая техника)

**Диссертация на соискание учёной степени
кандидата технических наук**

Научный руководитель: кандидат технических наук, доцент
Неретин Евгений Сергеевич

Москва – 2023

Оглавление

Перечень сокращений

АВПО – Анализ видов и последствий отказов

АО – Аппаратное обеспечение

АП-25 – Авиационный правила, ч.25

АС – Аварийная ситуация

БИНС – Бесплатформенная инерциальная навигационная система

БС – Без ситуации

БРУД – Блок рычагов управления двигателями

БРУС – Боковая ручка управления самолетом

ВАК – Высшая аттестационная комиссия

ВОИЧ – Воздействие одиночных ионизирующих частиц

ВПП – Взлетно-посадочная полоса

ВС – Воздушное судно

ГС – Гидравлические системы

ИУ – Исполнительные устройства

ИС – Интегральная схема

КМОП – Комплементарная структура металл-оксид-полупроводник

КС – Катастрофическая ситуация

КСУ – Комплексная система управления

КТ – Квалификационные требования

МАИ – Московский авиационный институт (национальный исследовательский университет)

МОП – Модельно-ориентированный подход

МОПОБ – Модельно-ориентированный подход к оценке безопасности

НЛГС – Нормы летной годности самолетов

НФФБ – Нарушение функции функционального блока

ОБ – Оценка безопасности

ОУ – Органы управления

ОФО – Оценка функциональных опасностей

ПК – Персональный компьютер

ПО – Программное обеспечение

ПОБ – Предварительная оценка безопасности

ППСПП – Поперечное сечение полупроводника

ПУ САУ – Пульт управления режимами САУ

Р – Руководство

РДПВ – Располагаемая дистанция прерванного взлета

РДВ – Располагаемая дистанция взлета

РДР – Располагаемая дистанция разбега

РПД – Располагаемая посадочная дистанция

РУВТ – Ручка управления воздушными тормозами

РУМК – Ручка управления механизацией крыла

САУ – Система автоматического управления

СДУ – Система дистанционного управления

СВС – Система воздушных сигналов

СС – Сложная ситуация

ТУ – Технические условия

УУП – Усложнение условий полета

ФБ – Функциональный блок

ЭРИ – электрорадиоизделия

AADL – Architecture Analysis & Design Language

ARP – Aerospace Recommended Practice

MEL – Minimum Equipment List

UDP – Universal Datagram Protocol

Введение

Актуальность работы. Безопасность – качественный интегральный показатель, имеющий множество определений и трактований. В мире гражданской авиации основным определением безопасности служит представленное в Руководстве P-4754A [1]:

Безопасность – состояние, в котором риск приемлем.

Основным показателем *безопасности* становится сведение к минимуму неприемлемых рисков. Для достижения *безопасности* предусмотрены различные методы: резервирование, обнаружение и изоляция отказов и т.д.

Современные комплексные системы управления имеют не менее двух режимов: основной и резервный. В обоих режимах реализуются все функции, связанные непосредственно с управлением аэродинамическими поверхностями самолета. Ключевым отличием основного режима управления является наличие дополнительных защитных функций, препятствующих возникновению аварийных и катастрофических ситуаций. К защитным функциям относятся, например, предупреждение о приближении к эксплуатационным ограничениям скоростей, углов и перегрузок, ограничения отклонения поверхностей на разных режимах полета, парирование возмущений и др. Переход между режимами может быть не резким с постепенной деградацией отдельных функций [2]. Таким образом, стоит задача сохранять функции основного режима управления как можно дольше или, иначе говоря, минимизировать вероятность перехода не резервный режим управления.

Структурно-функционально можно представить основной режим управления как комплекс взаимодействующих систем, представленных на Рисунке 1: 6 основные вычислители КСУ (расположенные в независимых блоках: левом и правом), *n*-канально резервированных БИНС и СВС, пульт с кнопкой перехода на резервный режим (реализующей возможность инициации экипажем перехода на резервный режим в случае неконтролируемых отказов основного режима).

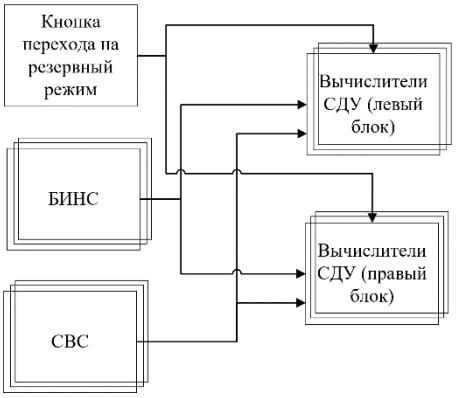

Рисунок 1 – Структурно-функциональная схема основного режима

Очевидно, в представленной структуре ключевыми источниками угроз для основного режима управления являются взаимодействующие системы, т.к. вычислители КСУ имеют высокий показатель избыточности и независимости. При этом отказы простых электромеханических устройств, таких как кнопки, имеют достаточно низкую интенсивность по сравнению со сложной радиоэлектронной аппаратурой, входящей в состав БИНС и СВС. Из этого следует, что основными потенциальными источниками проблем являются отказы БИНС и СВС. Под отказами будем понимать скачкообразные и постепенные изменения сигнала как в одном, так и в нескольких каналах системы в одно и то же или разное время. В задачи КСУ в таком случае входит контроль данных сигналов и определение исправных.

Отказы подразделяются на мгновенные, при которых выходной сигнал меняет свое значение с истинного на некорректное за крайне малый промежуток времени (например, обрыв цепи), и постепенные, при которых выходной сигнал меняет свое значение за продолжительное время (от нескольких тактов работы встроенных средств контроля). Примерами постепенных отказов могут служить ухудшения характеристик сопротивления в резисторах или износ механических узлов. Если мгновенные отказы алгоритмически легко обнаруживаемы даже в случае исправности всего двух каналов сигнала, то при постепенном отказе, т.е. при обработке встроенными средства контроля двух сигналов с различными характеристиками, очевидного решения в широко применяющихся алгоритмах нет. Таким образом, широко применяющиеся алгоритмы применимы вплоть до второго отказа.

Однако, практика показывает, что такие события не являются практически невероятными (т.е. имеют вероятность возникновения более, чем $1*10^{-9}$/л.ч.). Соответственно, и переход с основного режима систем управления на резервный не является практически невероятным событием, что негативно влияет на безопасность эксплуатации. Актуальность проблемы подтверждается тем, что каждый отказ влечет за собой необходимость проведения регламентных работ по ремонту и техническому обслуживанию. Зная о том, что есть отказ, но не зная в каком именно из блоков, увеличивается время ремонта и количество досрочных съемов исправного оборудования.

Данная проблема может быть решена пересмотром подхода к методике контроля систем. Известны различные перспективные методы контроля, включая искусственный интеллект [3] и включение в контур дополнительного эталонного наземного источника информации [4]. Каждый из методов показывает положительные результаты для некоторых групп видов отказов, но следует отметить, что часть из них сложна в практической реализации на борту или для сертификации. Таким образом актуальным остается разработка методики, не требующей значительного изменения программно-аппаратного комплекса, и вместе с тем логика работы которой очевидна и может быть верифицирована.

Основание для выполнения работы – Грант Российского фонда фундаментальных исследований № 20-31-90028 «Применение модельно-ориентированного подхода к оценке безопасности гражданских воздушных судов на примере комплекса бортового оборудования».

Цель диссертационной работы – повышение безопасности полётов за счет снижения вероятности преждевременного перехода на резервный режим комплексной системы управления.

Объект исследования – комплексная система управления перспективного гражданского самолета.

Предмет исследования – встроенные средства контроля комплекса сопрягаемого с комплексной системой управления бортового оборудования гражданского самолета.

Задачи диссертационной работы:

1. Сформировать требования к встроенным средствам контроля по результатам анализа функциональных недостатков использующихся средств контроля сигналов сопрягаемого с КСУ оборудования;
2. Разработать методику, обеспечивающую выбор исправных сигналов сопрягаемого оборудования вплоть до третьего отказа;
3. Разработать методику оценки безопасности системы в соответствии с отраслевыми стандартами Р-4754А, Р-4761;
4. Разработать стенд полунатурного моделирования отказных состояний;
5. Провести имитационное моделирование работы встроенных средств контроля в составе основного режима системы управления.

Методы исследования, примененные в работе: методы системного анализа, методы экспериментальных исследований, численные методы компьютерного моделирования, методы прогнозирования и оценки надежности сложных систем.

Научная новизна диссертационной работы заключается в следующем:

- разработана методика контроля сигналов в основном режиме комплексной системы управления, обеспечивающая на основе комбинации метода Лорцзака и неравенства Чебышева функционирование сопрягаемого оборудования вплоть до последнего отказа;
- разработаны алгоритмы, реализующие предложенную методику контроля сигналов сопрягаемого оборудования на основе комбинации метода Лорцзака и неравенства Чебышева в среде MATLAB;
- разработана методика выполнения мероприятий оценки безопасности на основе нотации SysML, с учетом повышения точности расчетов показателей надежности и безопасности при использовании предложенной методики контроля сигналов сопрягаемого оборудования.

Результаты, выносимые на защиту:

- методика контроля сигналов в основном режиме комплексной системы управления, обеспечивающая на основе комбинации метода Лорцзака и

неравенства Чебышева функционирование сопрягаемого оборудования вплоть до последнего отказа;

- алгоритмы, реализующие предложенную методику контроля сигналов сопрягаемого оборудования на основе комбинации метода Лорцзака и неравенства Чебышева в среде MATLAB;
- стенд полунатурного моделирования, включающий физические имитаторы оперативных органов управления в кабине экипажа;
- методика выполнения мероприятий оценки безопасности на основе нотации SysML, с учетом повышения точности расчетов показателей надежности и безопасности при использовании предложенной методики контроля сигналов сопрягаемого оборудования.

Практическая значимость полученных в диссертационной работе результатов состоит в следующем:

- разработана методика контроля сигналов сопрягаемого оборудования в основном режиме комплексной системы управления, позволяющая определить исправные сигналы в случае их фактического меньшинства;
- разработан программно-аппаратный комплекс (стенд полунатурного моделирования), обеспечивающий валидацию степени опасности функциональных отказов;
- полученные методики упрощают процесс взаимодействия инженеров разного уровня иерархии (самолет / система / компонент) и авиационных властей.

Достоверность полученных результатов обеспечивается корректным применением математического аппарата и их экспериментальной проверкой.

Внедрение и реализация. Основные результаты диссертационной работы внедрены при выполнении научно-исследовательских работ в ПАО «Корпорация «Иркут» и учебный процесс на кафедре 703 «Системное проектирование авиакомплексов» Института №7 «Робототехнические и интеллектуальные системы» МАИ, что подтверждается соответствующими актами о внедрении.

Апробация работы. Основные положения диссертационной работы представлены и обсуждены на 17-й, 18-й, 19-й и 20-й Международных конференциях «Авиация и космонавтика» (г. Москва, 2018, 2019, 2020, 2021 гг.), III и IV Конкурсе научно-технических работ ПАО «Корпорация «Иркут» (г. Москва, 2018, 2019 гг.), 11-м и 12-м Всероссийских межотраслевых молодёжных конкурсах научно-технических работ и проектов «Молодёжь и будущее авиации и космонавтики» (г. Москва, 2019, 2020 гг.), XLV, XLVI и XLVII Международных молодёжных научных конференциях «Гагаринские чтения» (г. Москва, 2019, 2020, 2021 гг.), 3-ей Международной конференции «3rd International Conference on Control, Artificial Intelligence, Robotics & Optimization ICCAIRO» (Греция, г. Афины, 2019 г.), XII и научно-практических конференций студентов и аспирантов «Актуальные проблемы развития авиационной техники и методов ее эксплуатации» (г. Иркутск, 2019, 2020 гг.), XV Международной конференции по электромеханике и робототехнике «Завалишинские чтения» (г. Санкт-Петербург, 2020 г.), XV Международной научно-технической конференции «Автоматизация и энергосбережение в машиностроении, энергетике и на транспорте» (г. Вологда, 2020 г.), XI-й международной научно-технической конференции «Проблемы совершенствования робототехнических и интеллектуальных систем летательных аппаратов» (г. Москва, 2020 г.), IV Международной научно-практической конференции «Производственные технологии будущего: от создания к внедрению» (г. Комсомольск-на-Амуре, 2021 г.), научных семинарах института №7 «Робототехнические и интеллектуальные системы» МАИ.

Публикации. Основные результаты диссертационной работы полностью отражены в 7 статьях (4 из которых – в журналах, рекомендованных Перечнем ведущих периодических изданий ВАК при Министерстве науки и высшего образования РФ), 22 трудах и тезисах докладов международных и всероссийских конференций и семинаров.

Структура и объем диссертационной работы. Диссертация включает в себя введение, четыре главы, заключение и список использованной литературы. Общий объем работы составляет 136 страниц, включая 54 рисунка и 15 таблиц. Список использованных источников содержит 77 наименований.

Во *введении* представлена общая характеристика работы, сформулированы основная цель и вытекающие из нее задачи исследования, указаны объект, предмет и методы исследования, приведен обзор исследований по рассматриваемой тематике, отражены актуальность, научная новизна и практическая значимость диссертационной работы. Кратко излагается содержание работы по главам.

В *главе 1* диссертационной работы проведен анализ современных и перспективных подходов к методам контроля бортового оборудования. Классические методы были оценены с точки зрения их подверженности воздействию различных видов отказов, как мгновенных, так и постепенных, а также их комбинаций. По результатам оценена вероятность перехода на резервный режим КСУ при каждой из методик контроля.

В *главе 2* поставлена и решена задача разработки методики контроля сопрягаемого с КСУ оборудования:

- разработаны требования к разрабатываемой методике контроля;
- реализован алгоритмическое обеспечение, реализующее требования к методике контроля;
- Проведено моделирование и оценено достижение заданных требований к методике контроля.

В *главе 3* представлен реализованный программно-аппаратный комплекс, позволяющий обеспечить полунатурное моделирование отказных состояний, проведены полунатурные испытания в различных конфигурациях самолета.

В *главе 4* предложена методика модельно-ориентированного подхода к оценке безопасности. В соответствии с данной методикой проведена оценка безопасности предлагаемой методики контроля, сопрягаемого с КСУ оборудования в соответствии с требованиями отраслевого стандарта Р-4761.

В *заключении* представлены ключевые результаты работы и сформулированы выводы о достижении поставленной цели.

ГЛАВА 1. СОВРЕМЕННЫЕ ПОДХОДЫ К МЕТОДАМ КОНТРОЛЯ БОРТОВОГО ОБОРУДОВАНИЯ

1.1 Общие положения

Метод определения кворумного значения для трижды резервированных систем, к которым относятся БИНС и СВС, с учетом норм MEL (допускается вылет с одним отказавшим вычислителем БИНС или СВС) можно представить как мажоритарный элемент с выходом u и входами x_1, x_2, x_3, как представлено на рисунке 2. При этом один из параметров x_i может отсутствовать, что не влияет на общую схему представления мажоритарного элемента.

Рисунок 2 – Представление мажоритарного элемента

1.1.1 Методы контроля, выносимые на сравнение

Далее рассмотрены три типа мажоритарных элементов, работающих согласно: методу выбора арифметического значения (раздел 1.2), методу выбора медианного значения (раздел 1.3) и методу контроля по предыстории (раздел 1.4). Не будут рассматриваться методы с использованием искусственного интеллекта, т.к. настоящие алгоритмы не использовались в авиационных проектах, а также не имеют возможности быть сертифицированными из-за аспектов верификации и подверженности кибератакам.

1.1.2 Виды отказов, стойкость к которым будет анализироваться

Известно, что существуют два типа отказов сложного электронного оборудования: параметрические отказы (постепенные, т.е. деградирующие со временем) и внезапные (мгновенно изменяющие свое значение) [5].

В ходе выполнения диссертационного исследования будут рассматриваться оба варианта, т.к. статистические данные показывают, что оба они являются вероятными [6, 7].

1.2 Методика выбора арифметического значения

1.2.1 Описание методики

В общем виде методика расчета среднего арифметического значения может быть представлена как показано в формуле (1).

$$u = \frac{1}{n}\sum_{1}^{n} x_i \qquad (1);$$

Очевидная проблема метода вычисления среднего арифметического значения заключается в том, что независимо от количества исправных каналов, любой отказ приводит к незамедлительному влиянию на результирующий сигнал u.

1.2.2 Результаты методики выбора арифметического значения

В данном разделе представлены результаты моделирования постепенных и внезапных отказов БИНС. Дополнительно учитывались погрешности измерений.

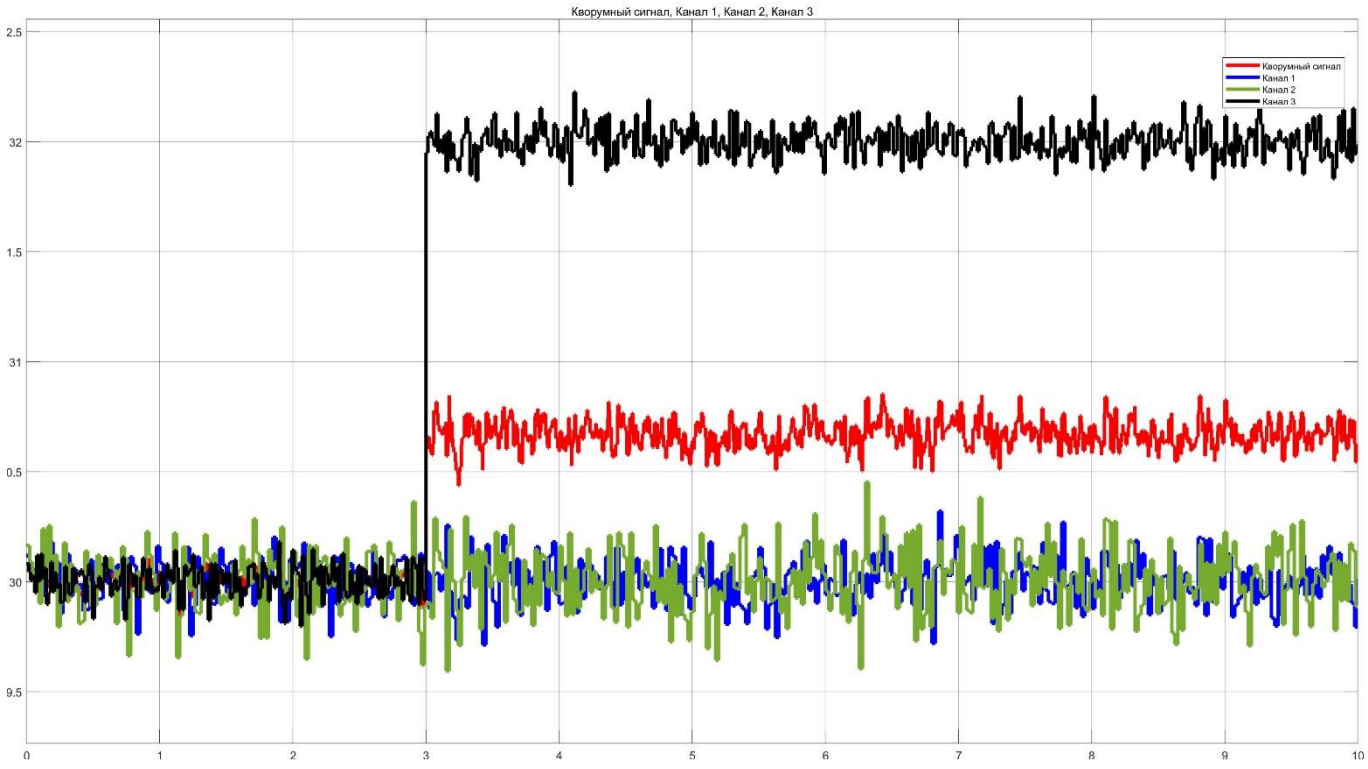

Рисунок 3. Результаты моделирования метода выбора среднего арифметического при мгновенном отказе в одном канале с учетом помех

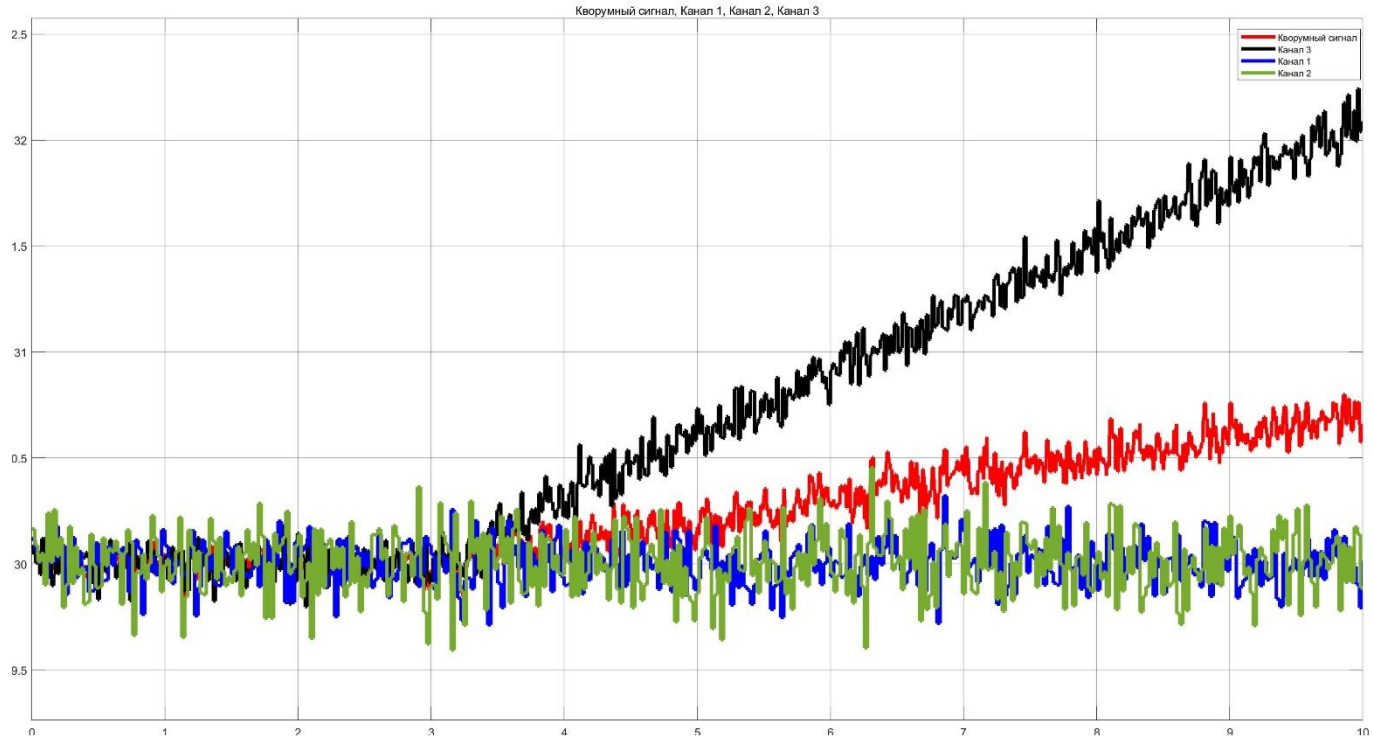

Рисунок 4. Результаты моделирования метода выбора среднего арифметического при постепенном отказе в одном канале с учетом помех

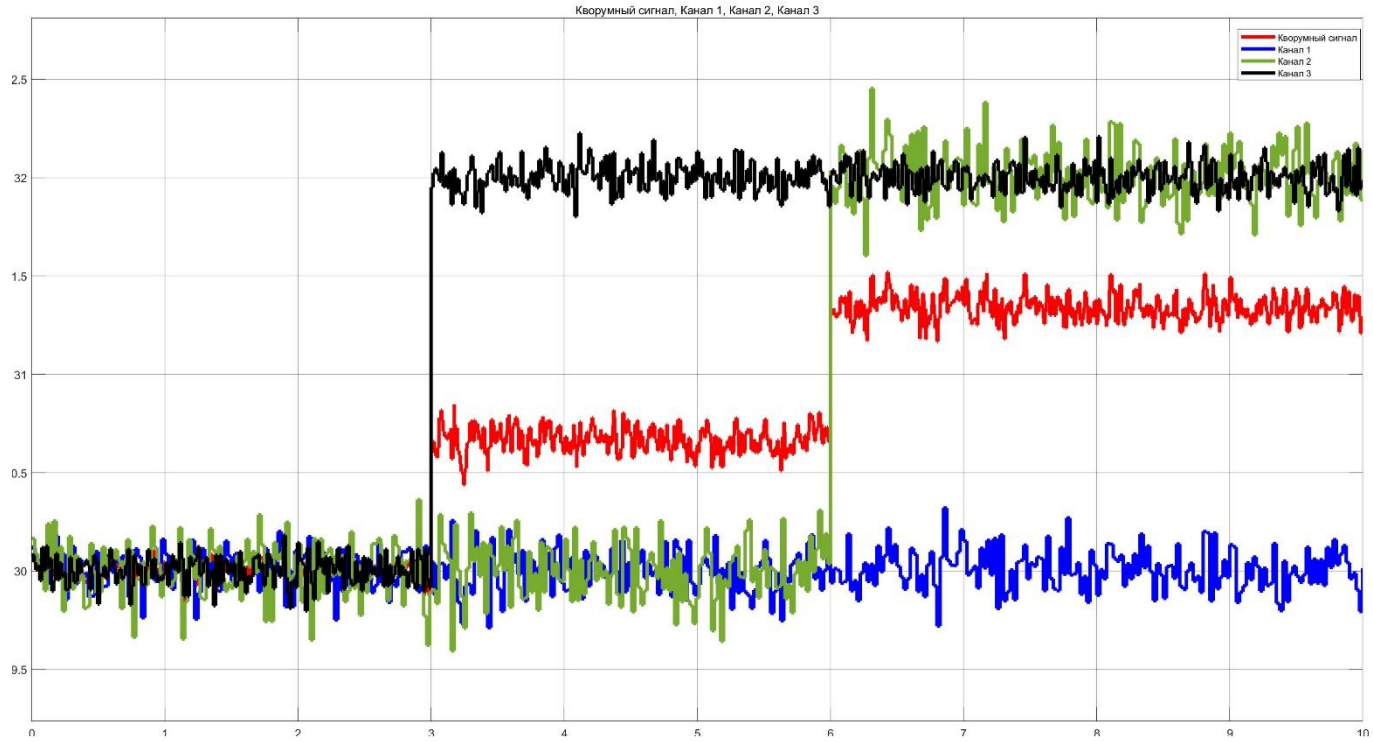

Рисунок 5. Результаты моделирования метода выбора среднего арифметического при мгновенном отказе в двух каналах с учетом помех

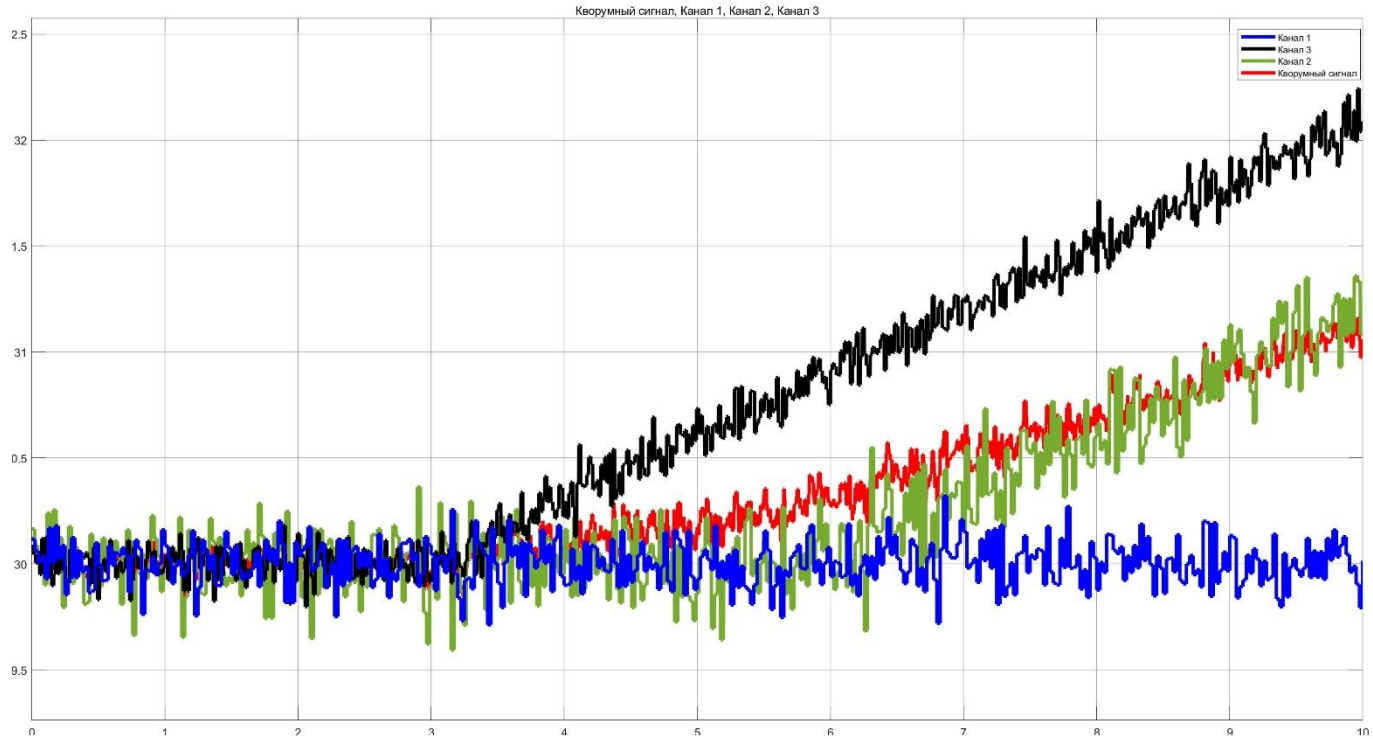

Рисунок 6. Результаты моделирования метода выбора среднего арифметического при постепенном отказе в двух каналах с учетом помех

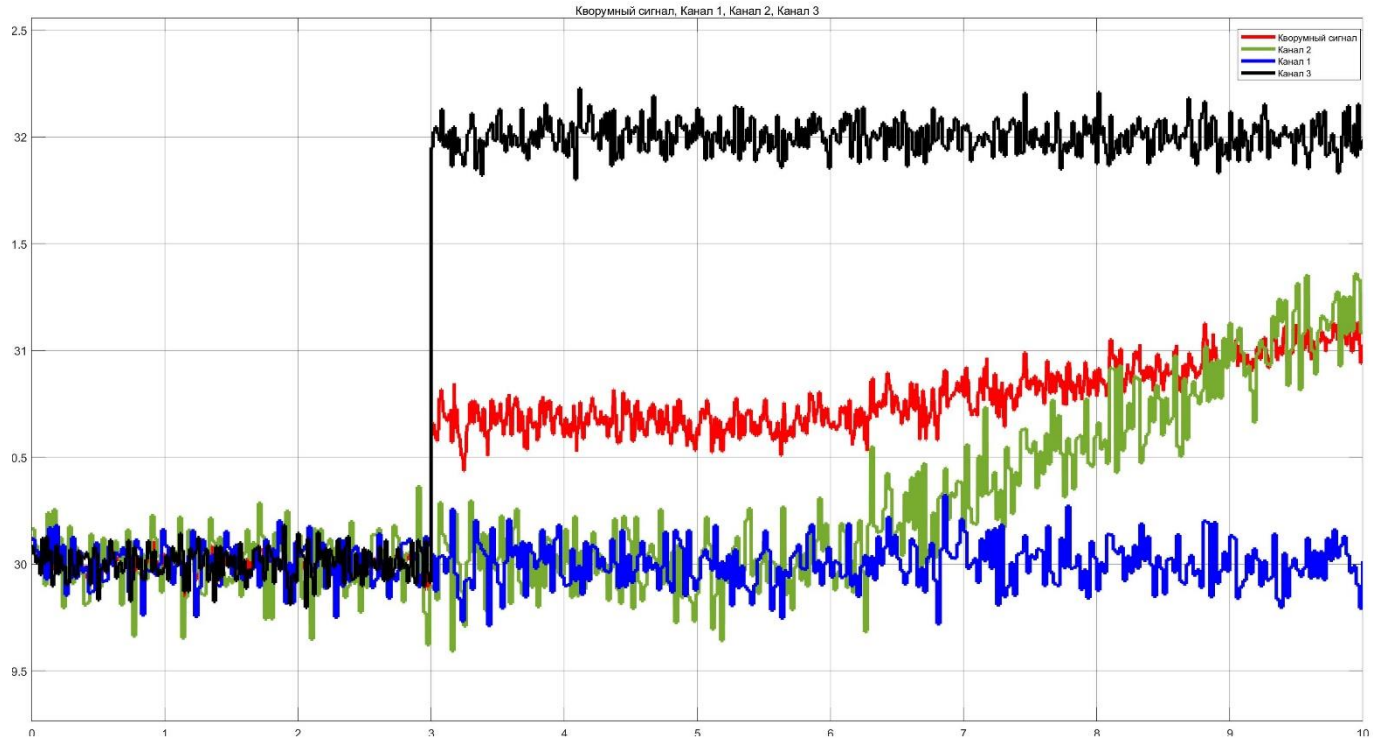

Рисунок 7. Результаты моделирования метода выбора среднего арифметического при мгновенном отказе в одном канале и последующем постепенном отказе в другом канале с учетом помех

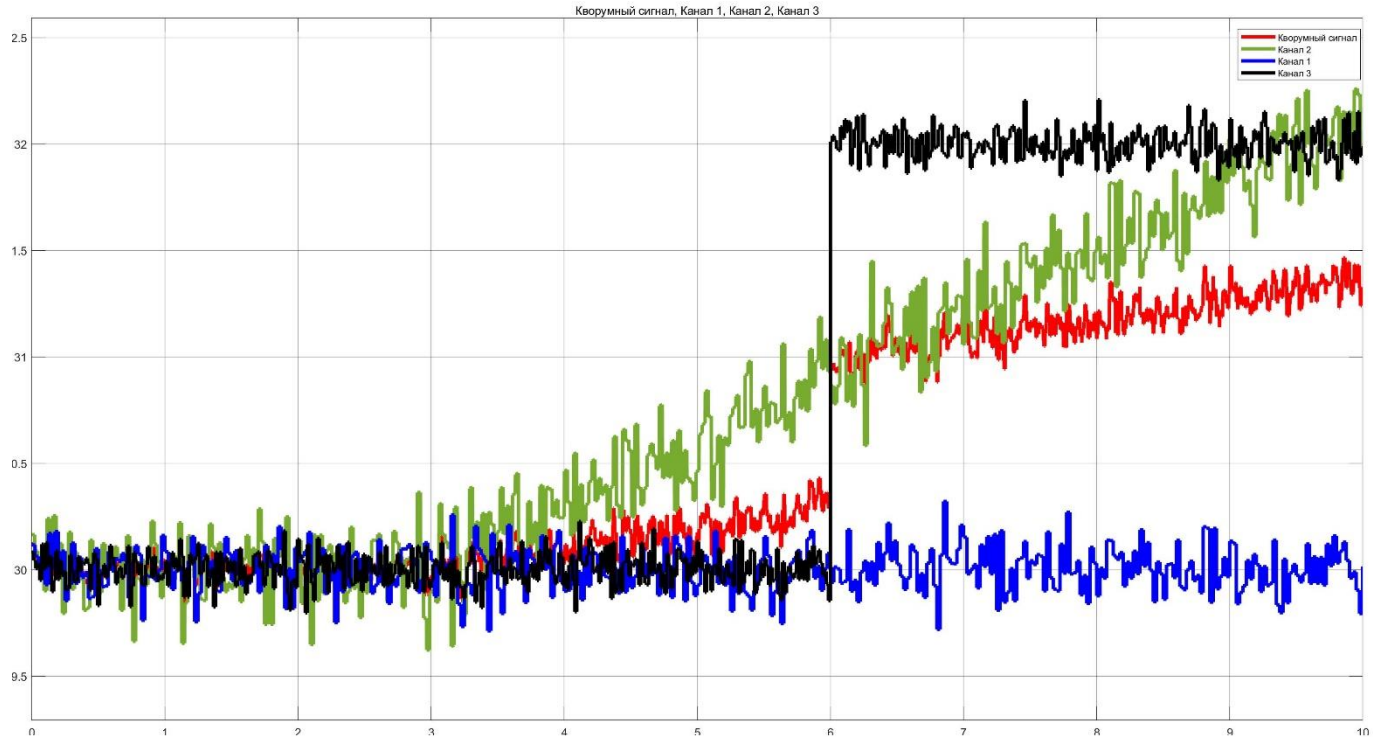

Рисунок 8. Результаты моделирования метода выбора среднего арифметического при постепенном отказе в одном канале и мгновенном в другом канале с учетом помех

Контроль среднего значения корректно функционирует вплоть до второго отказа. Найдем вероятность перехода на резервный режим КСУ.

$$P_{\text{РР}}(t) = P_{\text{кпрр}}(t) + (P_{\text{БИНС1}}(t) + P_{\text{БИНС2}}(t) + P_{\text{БИНС3}}(t)) + (P_{\text{СВС1}}(t) + P_{\text{СВС2}}(t) + P_{\text{СВС3}}(t)) + (P_{\text{КСУЛ1}}(t) * P_{\text{КСУЛ2}}(t) + P_{\text{КСУЛ1}}(t) * P_{\text{КСУЛ3}}(t) + P_{\text{КСУЛ2}}(t) * P_{\text{КСУЛ3}}(t)) * (P_{\text{КСУП1}}(t) * P_{\text{КСУП2}}(t) + P_{\text{КСУП1}}(t) * P_{\text{КСУП3}}(t) + P_{\text{КСУП2}}(t) * P_{\text{КСУП3}}(t))$$

Здесь $P_{PP}(t)$ – вероятность перехода на резервный режим КСУ, $P_{кпрр}(t)$ – вероятность отказа кнопки перехода на резервный режим, $P_{БИНСi}(t)$ – вероятность отказа i-го БИНС, $P_{СВСi}(t)$ – вероятность отказа i-го СВС, $P_{КСУЛi}(t)$ – вероятность отказа i-го левого вычислителя КСУ, $P_{КСУПi}(t)$ – вероятность отказа i-го правого вычислителя КСУ. Значением вероятности отказов КСУ можем пренебречь для простоты расчетов, т.к. параметр интенсивности отказов электронного оборудования КСУ, БИНС и СВС примерно равен. Требования АП-25 нормируют вероятность возникновения отказных состояний за 1 час полета. Тогда можем представить расчет вероятности в виде следующего выражения:

$$P_{\text{РР}}(t = 1\text{ч}) = \left(1 - e^{-\lambda_{\text{кпрр}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{БИНС1}}t}\right) + \left(1 - e^{-\lambda_{\text{БИНС2}}t}\right) + \left(1 - e^{-\lambda_{\text{БИНС3}}t}\right) + \left(1 - e^{-\lambda_{\text{СВС1}}t}\right) + \left(1 - e^{-\lambda_{\text{СВС2}}t}\right) + \left(1 - e^{-\lambda_{\text{СВС3}}t}\right).$$

Здесь параметр λ – интенсивность отказа соответствующих компонентов основного режима КСУ. Примем следующие значения: $\lambda_{\text{кпрр}} = 5{,}2 * 10^{-10}/\text{ч}$, $\lambda_{\text{БИНС1}} = \lambda_{\text{БИНС2}} = \lambda_{\text{БИНС3}} = 1{,}17 * 10^{-5}/\text{ч}$, $\lambda_{\text{СВС1}} = \lambda_{\text{СВС2}} = \lambda_{\text{СВС3}} = 6{,}72 * 10^{-5}/\text{ч}$. Тогда расчетное значение составит $P_{\text{РР}}(t = 1\text{ч}) = 2{,}53 * 10^{-4}$, что не является событием практически невероятным (то есть, имеющим вероятность менее 10^{-9} на один час).

Таким образом, контроль среднего значения хоть и является достаточно простым алгоритмически, оставляет проблему снижения вероятности перехода на резервный режим КСУ до практически невероятной нерешенной. Более того, не обеспечивается корректная работа при постепенных видах отказов даже в одном канале. Таким образом, безопасность использования данного метода не может быть продемонстрирована.

1.3 Методика выбора медианного значения

1.3.1 Описание методики

В общем виде методика расчета среднего арифметического значения может быть представлена как показано в формуле (2).

$$u = median(x) \qquad (2);$$

Здесь функция *median(x)* возвращает значение x_i, соответствующее:

- середине ранжированного по возрастанию ряда принятых показаний $\{x_1, x_2, \dots, x_n\}$, если n – нечетное, или
- среднему арифметическому значений, ранжированного по возрастанию, $\frac{x_{\left(\frac{n}{2}-1\right)} + x_{\left(\frac{n}{2}+1\right)}}{2}$ принятых показаний $\{x_1, x_2, \dots, x_n\}$, если n – четное.

Данный метод является наиболее распространенным в гражданской авиации, т.к. не требует значительных вычислительных мощностей, очевиден в работе (и, соответственно, в процессе верификации). Также из математического смысла следует, что отказ в одном из каналов не должен влиять на результирующий сигнал.

1.3.2 Результаты методики выбора медианного значения

В данном разделе представлены результаты моделирования постепенных и внезапных отказов БИНС. Дополнительно учитывались погрешности измерений.

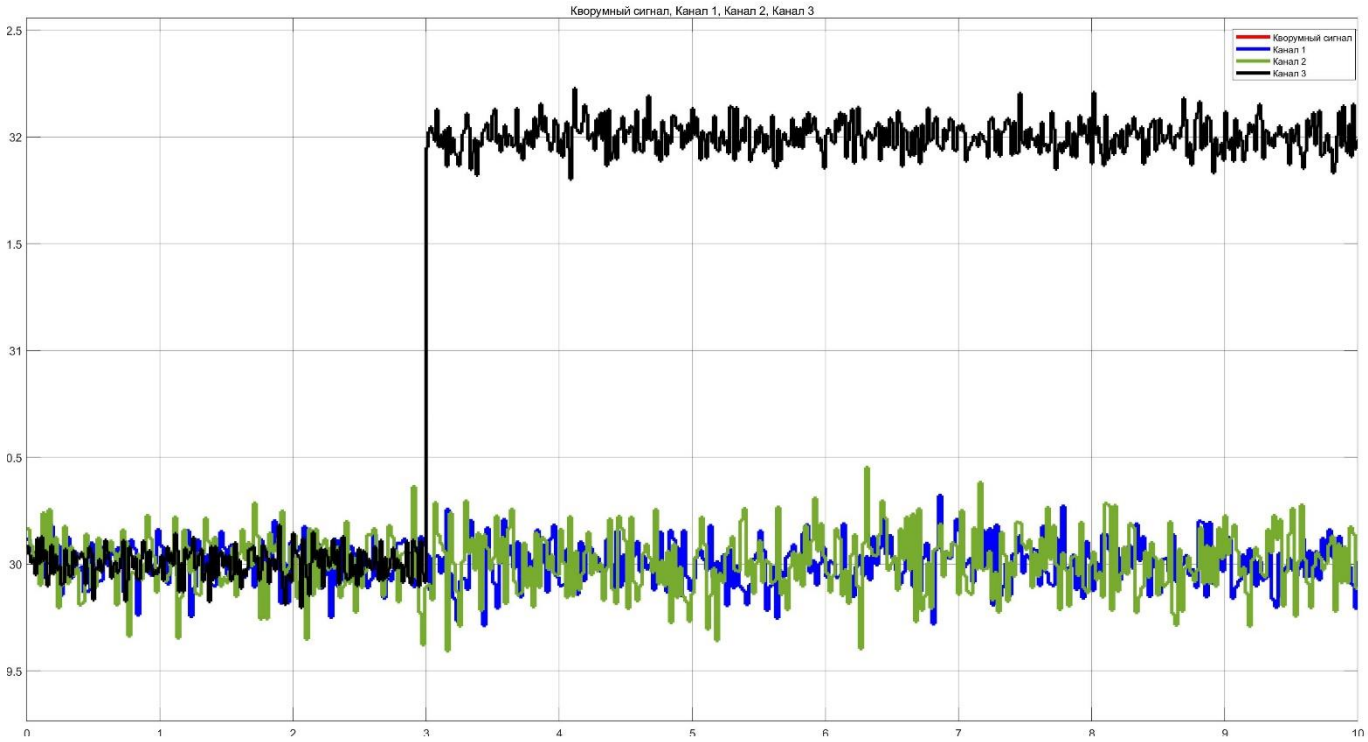

Рисунок 9. Результаты моделирования метода выбора медианного значения при мгновенном отказе в одном канале с учетом помех

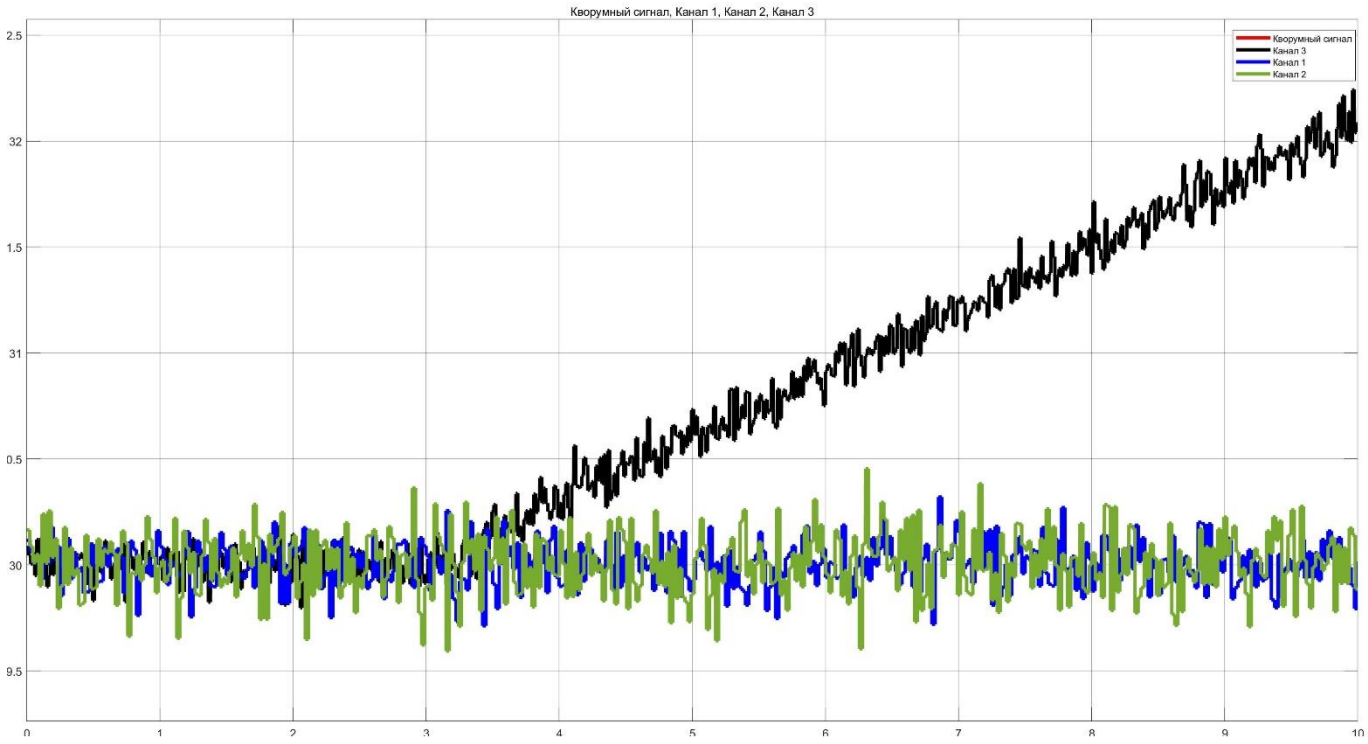

Рисунок 10. Результаты моделирования метода выбора медианного значения при постепенном отказе в одном канале с учетом помех

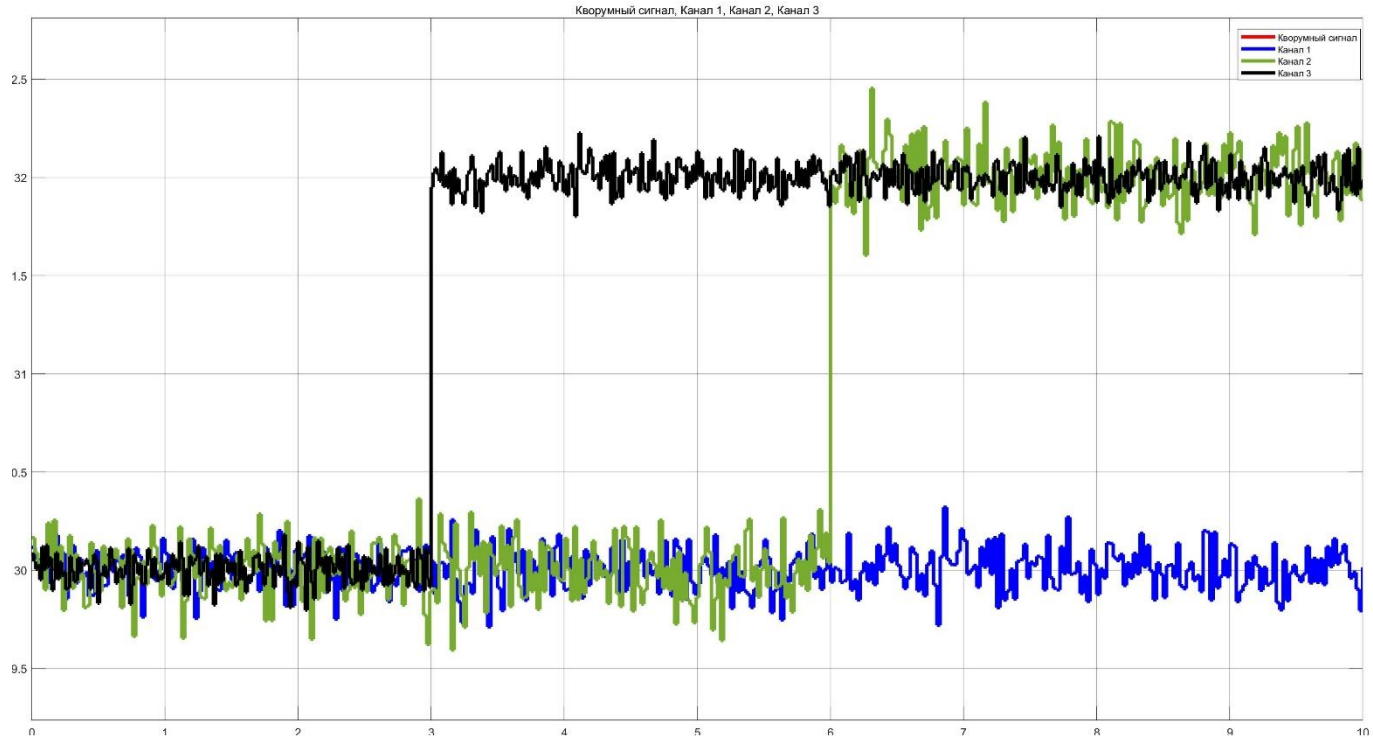

Рисунок 11. Результаты моделирования метода выбора медианного значения при мгновенном отказе в двух каналах с учетом помех

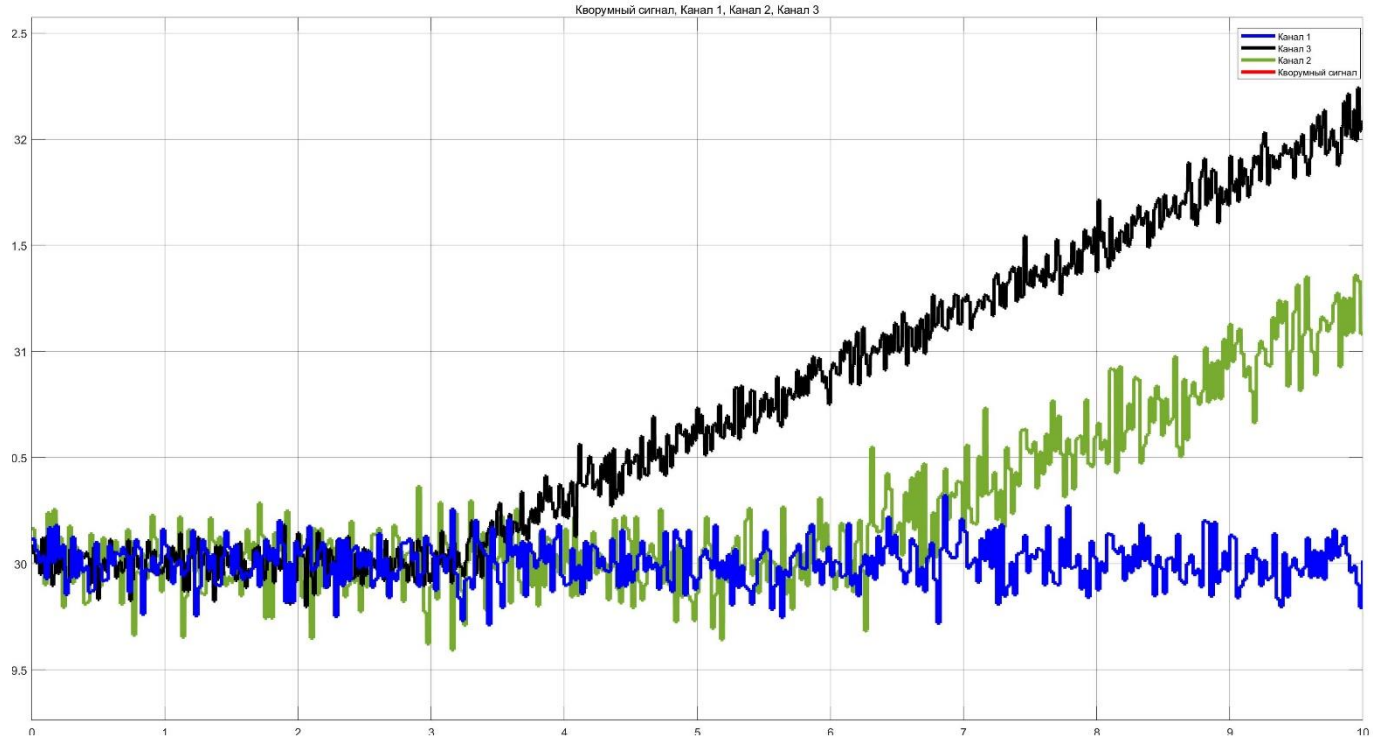

Рисунок 12. Результаты моделирования метода выбора медианного значения при постепенном отказе в двух каналах с учетом помех

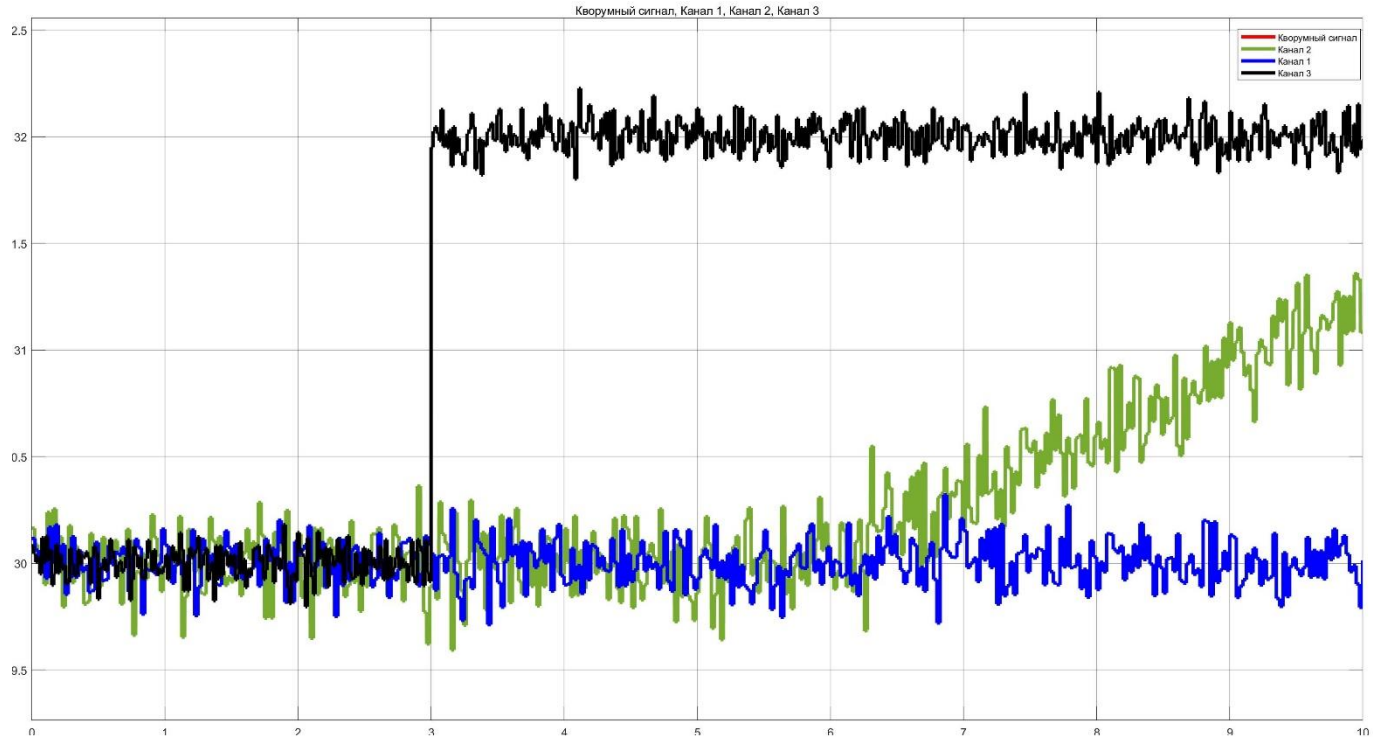

Рисунок 13. Результаты моделирования метода выбора медианного значения при мгновенном отказе в одном канале и последующем постепенном отказе в другом канале с учетом помех

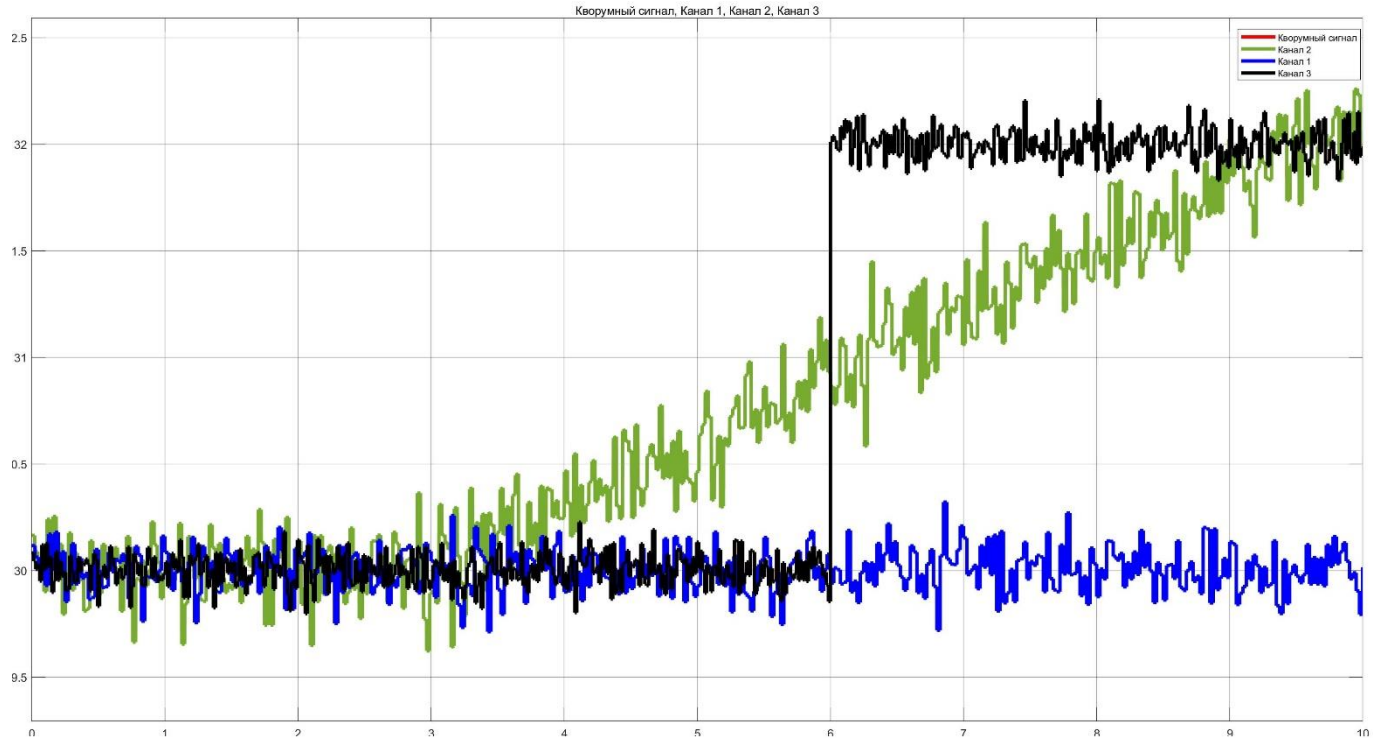

Рисунок 14. Результаты моделирования метода выбора медианного значения при постепенном отказе в одном канале и мгновенном в другом канале с учетом помех

Контроль по вычислению медианного значения корректно функционирует до второго отказа. Найдем вероятность перехода на резервный режим КСУ.

$$P_{\text{РР}}(t) = P_{\text{кпрр}}(t) + (P_{\text{БИНС1}}(t) * P_{\text{БИНС2}}(t) + P_{\text{БИНС1}}(t) * P_{\text{БИНС3}}(t) + P_{\text{БИНС2}}(t) * P_{\text{БИНС3}}(t)) + (P_{\text{СВС1}}(t) * P_{\text{СВС2}}(t) + P_{\text{СВС1}}(t) * P_{\text{СВС3}}(t) + P_{\text{СВС2}}(t) * P_{\text{СВС3}}(t)) + (P_{\text{КСУЛ1}}(t) * P_{\text{КСУЛ2}}(t) + P_{\text{КСУЛ1}}(t) * P_{\text{КСУЛ3}}(t) + P_{\text{КСУЛ2}}(t) * P_{\text{КСУЛ3}}(t)) * (P_{\text{КСУП1}}(t) * P_{\text{КСУП2}}(t) + P_{\text{КСУП1}}(t) * P_{\text{КСУП3}}(t) + P_{\text{КСУП2}}(t) * P_{\text{КСУП3}}(t))$$

Здесь $P_{PP}(t)$ – вероятность перехода на резервный режим КСУ, $P_{кпрр}(t)$ – вероятность отказа кнопки перехода на резервный режим, $P_{БИНСi}(t)$ – вероятность отказа i-го БИНС, $P_{СВСi}(t)$ – вероятность отказа i-го СВС, $P_{КСУЛi}(t)$ – вероятность отказа i-го левого вычислителя КСУ, $P_{КСУПi}(t)$ – вероятность отказа i-го правого вычислителя КСУ. Значением вероятности отказов КСУ можем пренебречь для простоты расчетов, т.к. параметр интенсивности отказов электронного оборудования КСУ, БИНС и СВС примерно равен. Требования АП-25 нормируют вероятность возникновения отказных состояний за 1 час полета. Тогда можем представить расчет вероятности в виде следующего выражения:

$$P_{\text{РР}}(t = 1\text{ч}) = \left(1 - e^{-\lambda_{\text{кпрр}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{БИНС1}}t}\right) * \left(1 - e^{-\lambda_{\text{БИНС2}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{БИНС1}}t}\right) * \left(1 - e^{-\lambda_{\text{БИНС3}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{БИНС2}}t}\right) * \left(1 - e^{-\lambda_{\text{БИНС3}}t}\right)\right) + \left(\left(1 - e^{-\lambda_{\text{СВС1}}t}\right) * \left(1 - e^{-\lambda_{\text{СВС2}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{СВС1}}t}\right) * \left(1 - e^{-\lambda_{\text{СВС3}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{СВС2}}t}\right) * \left(1 - e^{-\lambda_{\text{СВС3}}t}\right)\right)$$

Здесь параметр λ – интенсивность отказа соответствующих компонентов основного режима КСУ. Примем следующие значения: $\lambda_{\text{кпрр}} = 5{,}2 * 10^{-10}/\text{ч}$, $\lambda_{\text{БИНС1}} = \lambda_{\text{БИНС2}} = \lambda_{\text{БИНС3}} = 1{,}17 * 10^{-5}/\text{ч}$, $\lambda_{\text{СВС1}} = \lambda_{\text{СВС2}} = \lambda_{\text{СВС3}} = 6{,}72 * 10^{-5}/\text{ч}$. Тогда расчетное значение составит $P_{\text{РР}}(t = 1\text{ч}) = 1{,}49 * 10^{-8}$, что не является событием практически невероятным (то есть, имеющим вероятность менее 10^{-9} на один час).

Таким образом, контроль по вычислению медианного значения хоть и является достаточно простым алгоритмически и распространен на практике, оставляет проблему снижения вероятности перехода на резервный режим КСУ до практически

невероятной нерешенной. Неисправный результирующий сигнал возникает при любых отказах в двух каналах.

1.4 Методика контроля по предыстории

1.4.1 Описание методики

Под контролем по предыстории понимается введение весового коэффициента для каждого из сигналов, увеличивающегося со временем, если сигнал не отличается больше доверительного порога от предыдущего значения.

Для каждого датчика вводится параметр предыстории – достоверность V_i, изначально равный 1. Каждую секунду V_i увеличивается, если $|u–x_i| < \varepsilon$, где ε – пороговая величина сравнения. На k-ом цикле весовые коэффициенты вычисляются по формуле: $w_i=1/k * V_i$ [8].

Тогда параметр u можно представить, как представлено ниже:

$u = \frac{\sum_1^3 w_i v_i x_i}{\sum_1^3 w_i v_i}$, где весовые коэффициенты w_i вычисляются по формуле Лорцзака [9], а параметр предыстории v_i по формуле:

$$w_i = \frac{1}{1+\prod_{j=1,j\neq i}^{3} \frac{(x_i-x_j)^2}{\beta^2}}, \quad \text{где } \beta = \min_{i=1,j=1,i\neq j}(x_i - x_j)$$

$$v_i(k) = \begin{cases} (v_i^{k-1} + \delta) \in [0.1; 1.0], \text{если } \left|x_i^{k-1} - u\right| < \varepsilon \\ (v_i^{k-1} - \delta) \in [0; 0.9], \text{если } \left|x_i^{k-1} - u\right| \geq \varepsilon \end{cases}$$

Здесь k – такт вычислений, δ – параметр скорости изменения функции предыстории v_i, ε – допустимый порог сравнения одноименных сигналов.

1.4.2 Результаты методики контроля по предыстории

В данном разделе представлены результаты моделирования постепенных и внезапных отказов БИНС. Дополнительно учитывались погрешности измерений.

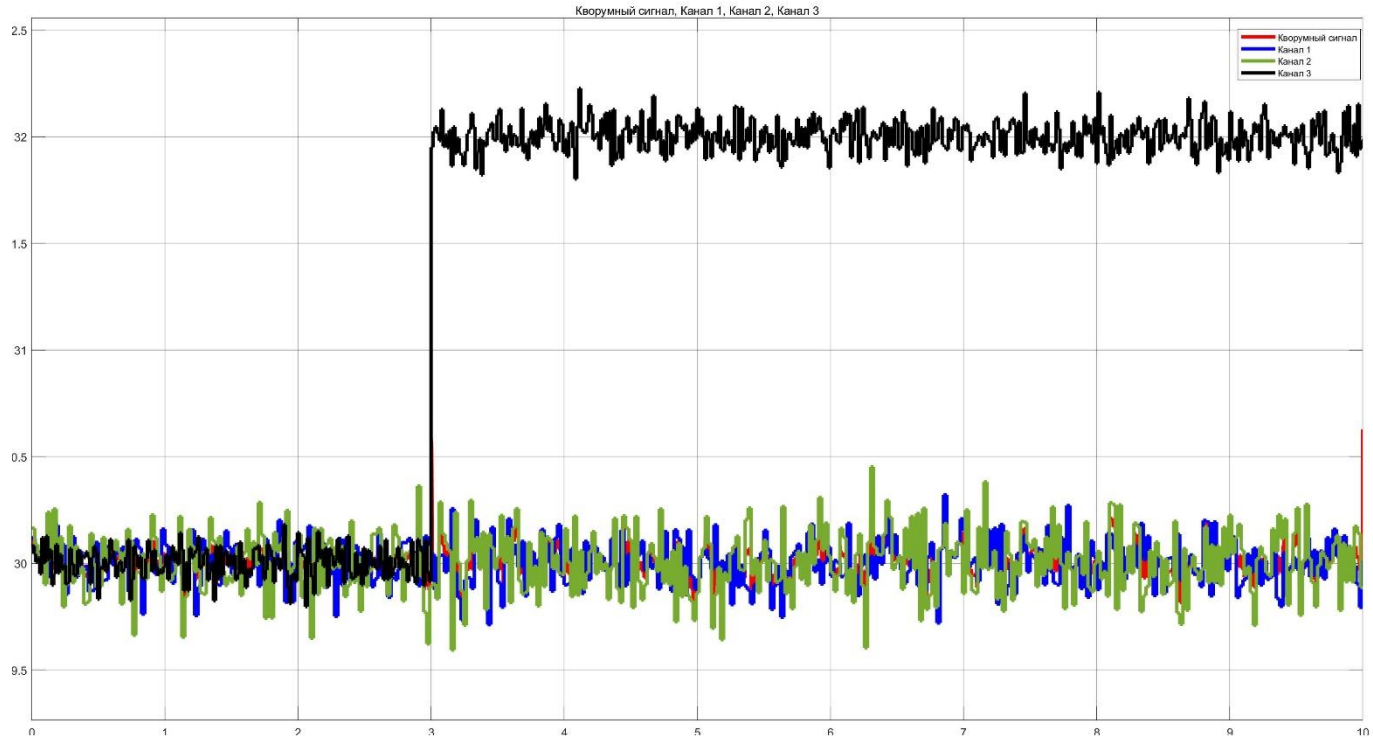

Рисунок 15. Результаты моделирования метода контроля по предыстории при мгновенном отказе в одном канале с учетом помех

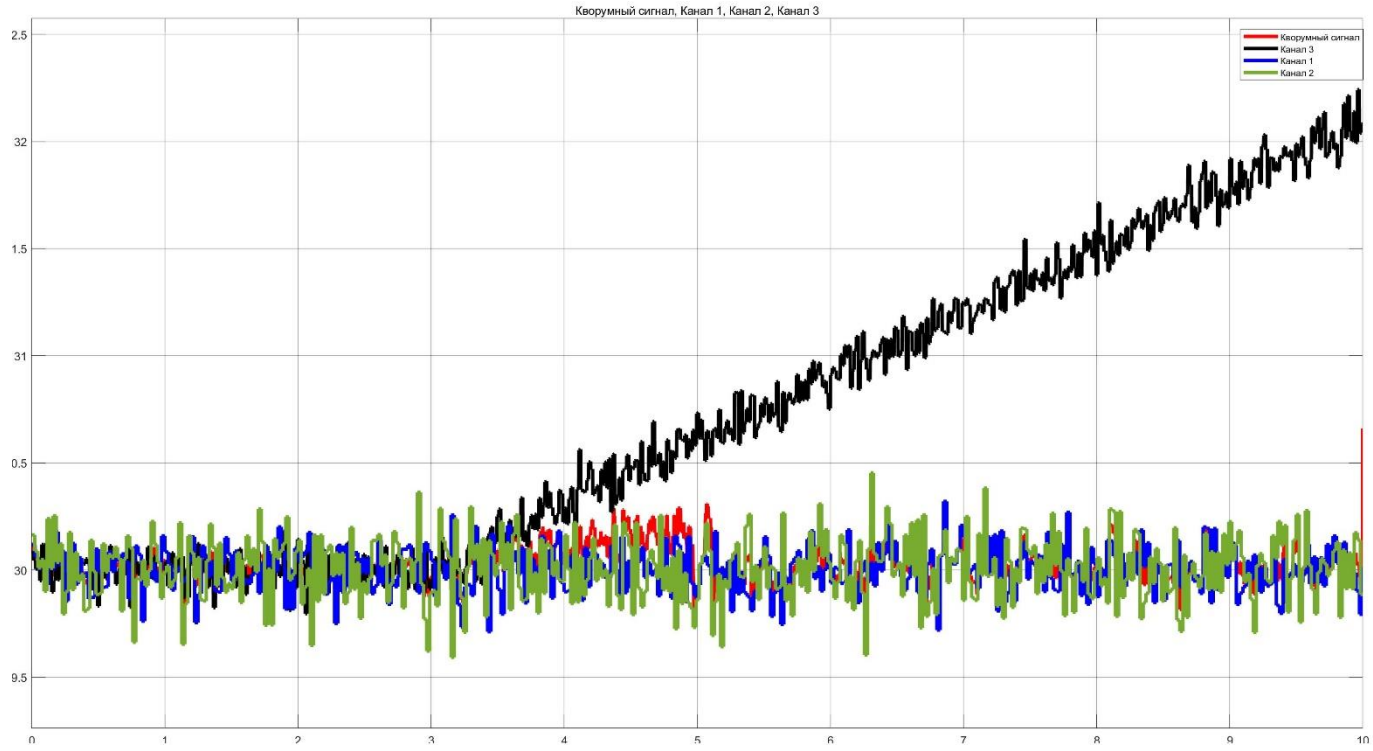

Рисунок 16. Результаты моделирования метода контроля по предыстории при постепенном отказе в одном канале с учетом помех

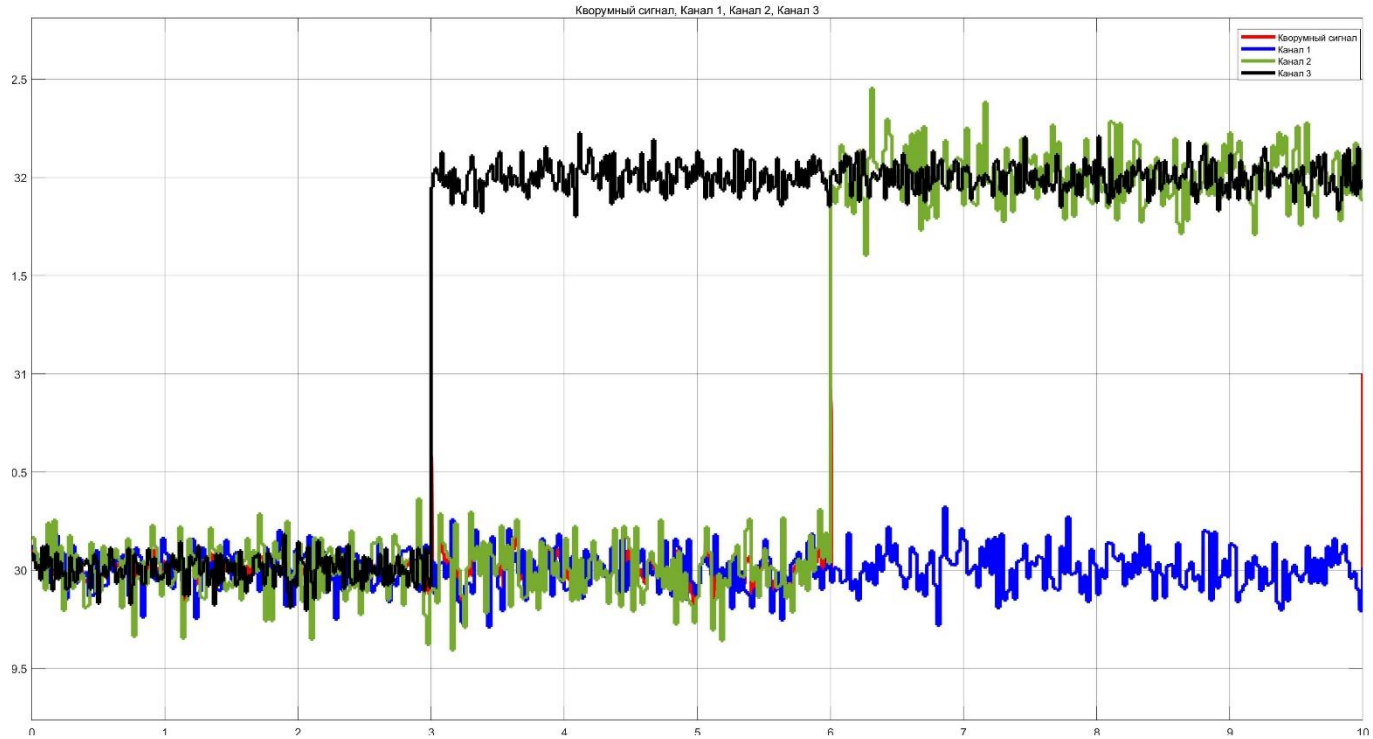

Рисунок 17. Результаты моделирования метода контроля по предыстории при мгновенном отказе в двух каналах с учетом помех

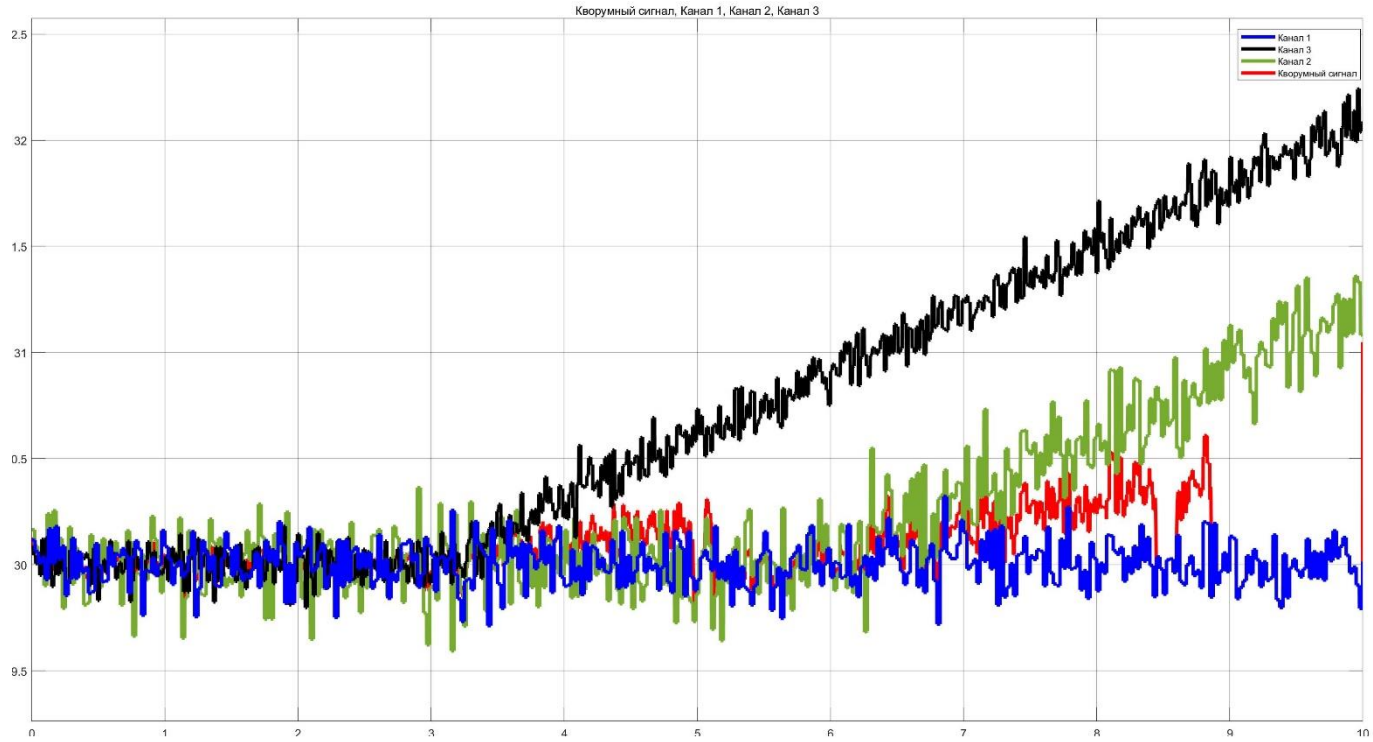

Рисунок 18. Результаты моделирования метода контроля по предыстории при постепенном отказе в двух каналах с учетом помех

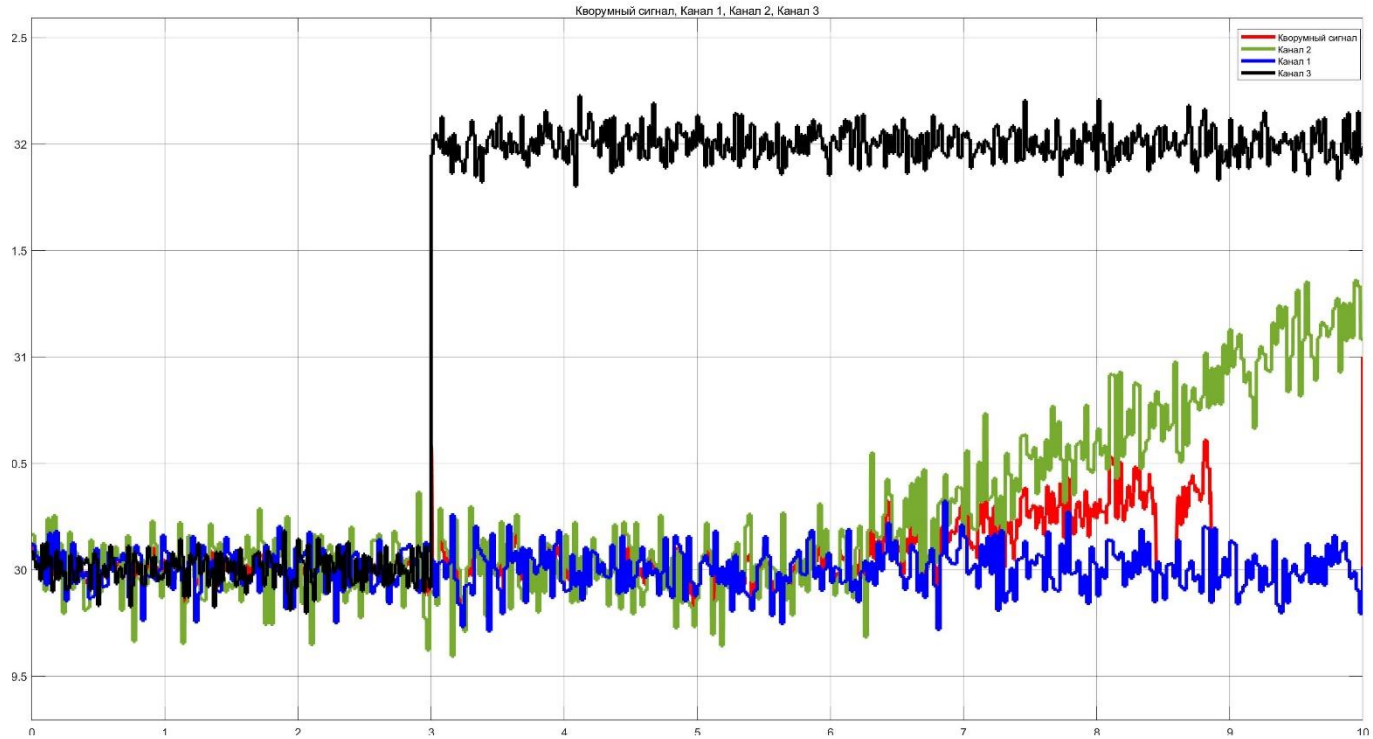

Рисунок 19. Результаты моделирования метода контроля по предыстории при мгновенном отказе в одном канале и последующем постепенном отказе в другом канале с учетом помех

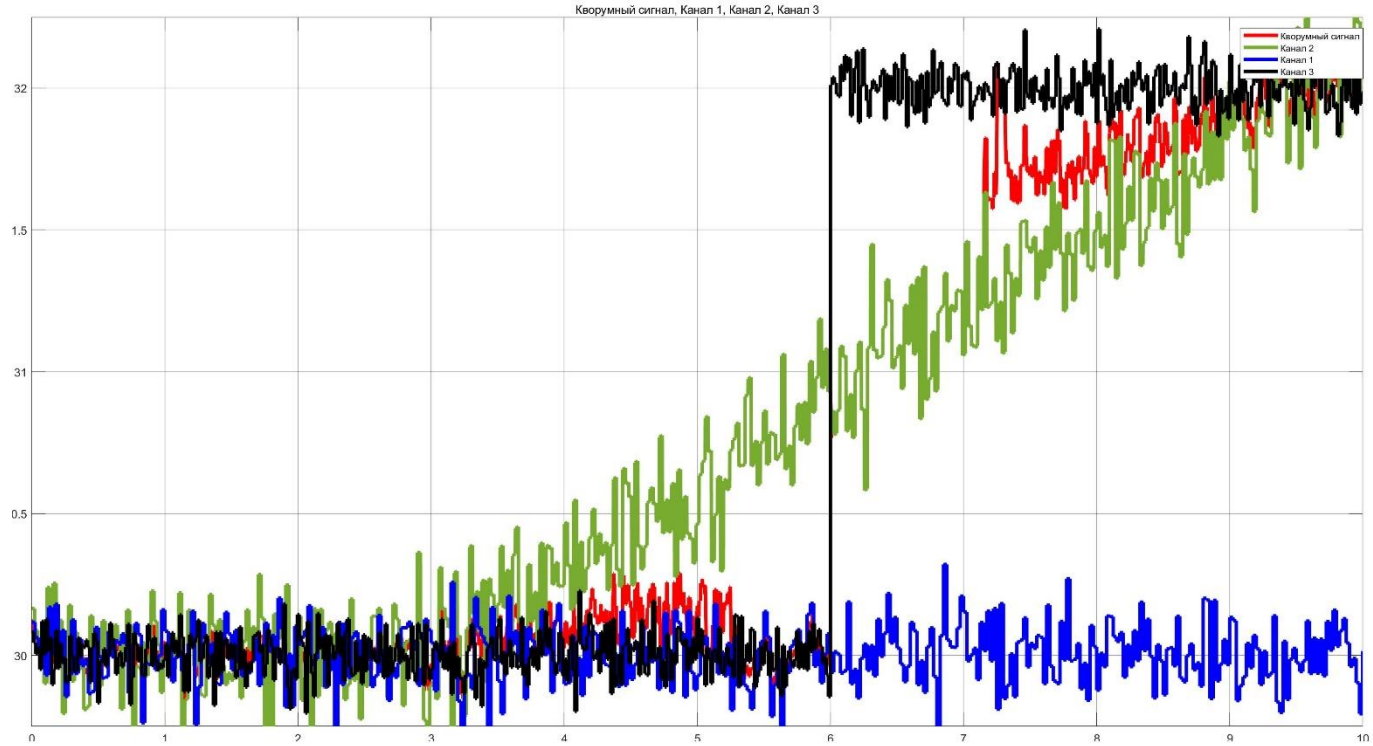

Рисунок 20. Результаты моделирования метода контроля по предыстории при постепенном отказе в одном канале и последующем мгновенном отказе в другом канале с учетом помех

Несмотря на хорошие показатели почти по всем результатам испытаний, постепенный отказ в одном канале с последующим мгновенным отказом в другом канале демонстрируют, что контроль по вычислению медианного значения также корректно функционирует до второго отказа, как и контроль медианного значения. Найдем вероятность перехода на резервный режим КСУ.

$$P_{\text{РР}}(t) = P_{\text{кпрр}}(t) + (P_{\text{БИНС1}}(t) * P_{\text{БИНС2}}(t) + P_{\text{БИНС1}}(t) * P_{\text{БИНС3}}(t) + P_{\text{БИНС2}}(t) * P_{\text{БИНС3}}(t)) + (P_{\text{СВС1}}(t) * P_{\text{СВС2}}(t) + P_{\text{СВС1}}(t) * P_{\text{СВС3}}(t) + P_{\text{СВС2}}(t) * P_{\text{СВС3}}(t)) + (P_{\text{КСУЛ1}}(t) * P_{\text{КСУЛ2}}(t) + P_{\text{КСУЛ1}}(t) * P_{\text{КСУЛ3}}(t) + P_{\text{КСУЛ2}}(t) * P_{\text{КСУЛ3}}(t)) * (P_{\text{КСУП1}}(t) * P_{\text{КСУП2}}(t) + P_{\text{КСУП1}}(t) * P_{\text{КСУП3}}(t) + P_{\text{КСУП2}}(t) * P_{\text{КСУП3}}(t))$$

Здесь $P_{PP}(t)$ – вероятность перехода на резервный режим КСУ, $P_{кпрр}(t)$ – вероятность отказа кнопки перехода на резервный режим, $P_{БИНСi}(t)$ – вероятность отказа i-го БИНС, $P_{СВСi}(t)$ – вероятность отказа i-го СВС, $P_{КСУЛi}(t)$ – вероятность отказа i-го левого вычислителя КСУ, $P_{КСУПi}(t)$ – вероятность отказа i-го правого вычислителя КСУ. Значением вероятности отказов КСУ можем пренебречь для простоты расчетов, т.к. параметр интенсивности отказов электронного оборудования КСУ, БИНС и СВС примерно равен. Требования АП-25 нормируют вероятность возникновения отказных состояний за 1 час полета. Тогда можем представить расчет вероятности в виде следующего выражения:

$$P_{\text{РР}}(t = 1\text{ч}) = \left(1 - e^{-\lambda_{\text{кпрр}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{БИНС1}}t}\right) * \left(1 - e^{-\lambda_{\text{БИНС2}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{БИНС1}}t}\right) * \left(1 - e^{-\lambda_{\text{БИНС3}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{БИНС2}}t}\right) * \left(1 - e^{-\lambda_{\text{БИНС3}}t}\right)\right) + \left(\left(1 - e^{-\lambda_{\text{СВС1}}t}\right) * \left(1 - e^{-\lambda_{\text{СВС2}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{СВС1}}t}\right) * \left(1 - e^{-\lambda_{\text{СВС3}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{СВС2}}t}\right) * \left(1 - e^{-\lambda_{\text{СВС3}}t}\right)\right)$$

Здесь параметр λ – интенсивность отказа соответствующих компонентов основного режима КСУ. Примем следующие значения: $\lambda_{\text{кпрр}} = 5{,}2 * 10^{-10}/\text{ч}$, $\lambda_{\text{БИНС1}} = \lambda_{\text{БИНС2}} = \lambda_{\text{БИНС3}} = 1{,}17 * 10^{-5}/\text{ч}$, $\lambda_{\text{СВС1}} = \lambda_{\text{СВС2}} = \lambda_{\text{СВС3}} = 6{,}72 * 10^{-5}/\text{ч}$. Тогда расчетное значение составит $P_{\text{РР}}(t = 1\text{ч}) = 1{,}49 * 10^{-8}$, что не является событием практически невероятным (то есть, имеющим вероятность менее 10-9 на один час).

Таким образом, контроль по предыстории сложнее является более сложным алгоритмически по сравнению с иными рассматриваемыми методами, но оставляет

проблему снижения вероятности перехода на резервный режим КСУ до практически невероятной нерешенной. Неисправный результирующий сигнал возникает при постепенном отказе в одном канале с последующим мгновенным отказом в другом канале.

Выводы по главе 1

1. На текущий момент известны «классические» методики контроля, являющиеся эвристическими, и предложены различные перспективные методики, включая использование элементов искусственного интеллекта. Тем не менее, наиболее распространенными являются методика вычисления среднего значения и методика вычисления медианного значения. Их достоинства заключается в простоте реализации на целевом вычислителе

2. Было проведено сравнение работы трех методик: методики вычисления среднего арифметического, методики вычисления медианного значения и методики вычисления сигнала по предыстории на основе формул Лорцзака.

3. Результаты анализа показали, что методика вычисления среднего арифметического дает худший результат, что вызвано влиянием отказа любого из каналов на результирующий сигнал. Вероятность перехода на резервный режим КСУ в таком случае составила 2,53e-4 за час полета.

4. Результаты анализа двух других методик показывают, что они имеют равную вероятность перехода на резервный режим КСУ, которая составляет 1,49e-8 за час полета. При этом методика выбора медианного значения работает неисправно при любом сочетании отказов в двух каналах, в то время как контроль по предыстории дает адекватный результат во всех случаях комбинаций отказов по двум каналам, за исключением последовательного возникновения сначала постепенного, а следом мгновенного отказа, но при отказе в одном канале лучший результат показывает методика вычисления медианного значения. Несмотря на то, что такое сочетание может быть достаточно редким явлением, нельзя утверждать, что данный метод решает поставленную задачу.

5. Исходя из указанных проблем, поставлена задача разработки такого метода, который будет обеспечивать адекватное результирующее значение при всех видах отказов, включая их комбинации в двух каналах. Конкретные требования и алгоритмическая реализация представлены в Главе 2.

ГЛАВА 2. МЕТОДИКА КВОРУМ-КОНТРОЛЯ БОРТОВОГО ОБОРУДОВАНИЯ

2.1 Требования к методике кворум-контроля бортового оборудования

Основываясь на результатах, полученных в Главе 1, можно сделать закономерный вывод, что, совместив два подхода, показывающих лучшие результаты в различных условиях, можно получить метод, дающий лучший результаты при всех исследуемых условиях. Однако, как показывают результаты Главы 1, полный набор событий не может быть обеспечен, если «переключать» два различных метода по какому-либо условию. Таким образом, требуется разработка новой методики, обеспечивающего следующие требования:

- Расчет результирующего значения должен осуществляться исправно при отсутствии отказов;
- Расчет результирующего значения должен осуществляться исправно при возникновении отказа в одном из каналов (при рассмотрении любого отдельного вида отказа);
- Расчет результирующего значения должен осуществляться исправно при возникновении отказов в двух каналах (при рассмотрении всех комбинаций возможных отказов и их последовательности).

2.2 Обоснование выбора математического аппарата

Известно, что измеряемые величины x_i подвержены нормально распределенным случайным ошибкам с нулевым математическим ожиданием и известной дисперсией (технические условия конкретного оборудования):

$$\begin{cases} x_1 = \hat{x} + \xi_1; \\ x_2 = \hat{x} + \xi_2; \\ x_3 = \hat{x} + \xi_3. \end{cases}$$

Здесь x_i – результаты измерений в соответствующем канале, $\hat{x}$ – истинное текущее значение измеряемого параметра, ξ_i – случайная ошибка измерения.

Распространенные эвристические методы подвержены воздействию этих ошибок. Так исправный сигнал может быть ложно определен как отказавший. После

первого отказа это может играть существенную роль в процессе определения истинного значения.

С учетом определенных проблем, данные требования могут быть воплощены при использовании различных методов обнаружения аномальных значений нестационарных случайных процессов. Можно выделить следующие критерии: критерий Томсона, критерий Шарлье, неравенство Чебышева, описанные ниже [77].

2.2.1 Критерий Томсона

Если рассматриваемый стационарный случайный процесс *Y(t) возможно* представить в виде некоторого вариационного ряда $Y_1, Y_2,\ldots,Y_n$, где Y_1 – минимальное значение; Y_n – максимальное значение; Y_k – распределенная случайная величина по закону Гаусса, с некоррелированными отсчетами, $Y_k \sim N(m_Y,\sigma_Y)$, $k = \overline{1,N}$, то гипотезу об аномальности крайних значений при известной величине дисперсии σ_Y^2 можно проверить с помощью U-статистик:

$$U = \frac{Y_k - \overline{m}_Y}{\sigma_Y}, \qquad \text{где } \overline{m}_Y = \frac{1}{\mathrm{N}}\sum_{k=1}^{\mathrm{N}} Y_k ,$$

представляющих собой случайные величины, распределенные по гауссовскому закону распределения плотности вероятности $U_k \sim N^*(0;1)$.

Таким образом, значение следует считать аномальным, если значение указанной статистики превышает квантиль гауссовского распределения при выбранном уровне значимости: $U_k > U_\beta$, где U_β – квантиль гауссовского распределения; $\alpha = 1 - \beta$ – уровень значимости. Если известны математическое ожидание m_Y и дисперсия σ_Y^2, то для проверки принадлежности аномальных значений к исходной выборке процесса применима статистика χ^2 и модифицированная статистика Фишера – Снедекора:

$\tilde{F} = \frac{(\sigma_Y^*)^2}{\sigma_Y^2}$, где $(\sigma_Y^*)^2$ – оценка дисперсии без учета аномального значения.

Априорная информация о параметрах математического ожидания и дисперсии часто недоступна на практике. Если известна только дисперсия, то вместо математического ожидания можно использовать его оценку $\overline{m_Y}$. Тогда аномальным значением можно считать крайний элемент выборки, если выполняется неравенство:

$$\frac{Y_i - \bar{m}_Y}{\sigma_Y} > U_\beta \sqrt{\frac{N-1}{N}}.$$

При отсутствии априорной информации о параметрах математического ожидания и дисперсии, одновременная замена этих параметров их оценками делает необходимым отказаться от использования квантилей гауссовского распределения. В этом случае в работе Томсона в качестве статистики для обнаружения аномальных значений в выборке стационарного случайного процесса, применяется стандартизованное экстремальное отклонение:

$\tau_k = \frac{Y_k - \bar{m}_Y}{\bar{\sigma}_Y}, k = \overline{1,N}$, где $\bar{\sigma}_Y = \sqrt{\frac{1}{N-1}\sum_{k=1}^{N}(Y_k - \bar{m}_Y)^2}$.

Величина τ_k отклонения выборочного значения Y_k от выборочного среднего значения, отнесенное к оценке среднеквадратичного отклонения $\bar{\sigma}_Y$, имеет особенное распределение, которое зависит только от объема выборки N:

$$f(\tau) = \frac{1}{\sqrt{(N-1)^\pi}} \frac{\Gamma\left(\frac{N-1}{2}\right)}{\Gamma\left(\frac{N-2}{2}\right)} \left(1 - \frac{\tau^2}{N-1}\right)^{\frac{N-4}{2}}$$

При N $\rightarrow\infty$ статистика стремится к *U* – статистики гауссовского распределения.

Использование критерия Томсона, эффективное при наличии более 40 измерений и когда известно о наличии только одного аномального значения. Данный метод не подходит к решаемой задаче, т.к. имеется всего три измерения, а аномальных значений может быть два.

2.2.2 Критерий Шарлье

Критерий Шарлье используется в тех случаях, когда объем выборки стационарного случайного процесса $N > 20$. Тогда в соответствии с теоремой Бернулле число значений, превышающих по абсолютной величине среднее арифметическое значение на величину $K_ш\bar{\sigma}_Y$, будет $N[1-\Phi(K_{Ш})]$, где $\Phi(K_{Ш})$ – значение нормированной функции Лапласа для $Y = K_{Ш}$. Если признаками аномальности в реализации процесса является одно значение, то $N[1-\Phi(K_{Ш})] = 1$. Используя критерий

Шарля, обнаруживается и исключается значение, для которого выполняется условие $|Y_k - \bar{m}_Y| > K_{Ш}\bar{\sigma}_Y$.

Если объем выборки стационарного случайного процесса $N > 20$, используется критерий Романовского. Для этого определяется критериальное значение $\left|\frac{Y-\bar{m}_Y}{\bar{\sigma}_Y}\right| = \beta$ и сравнивается с критерием β_T. Если $\beta \geq \beta_T$, то значение Y_i считается аномальным. Этот критерий применим только в случае наличия единственного аномального значения.

Общим недостатком методов, основанных на критериях Романовского-Шарля, является то, что оценка среднеквадратического отклонения процесса при задании порога принятия решения проводится без учета экстремальных значений (например, визуального контроля), и эти методы применимы для ограниченного объема выборки процесса.

2.2.3 Неравенство Чебышева

Рассмотренные статистики применимы для обнаружения аномальных значений в тех случаях, когда стационарный случайный процесс имеет гауссовский закон распределения плотности вероятности, а его выборочные значения являются статистически независимыми. Обнаружение аномальных значений для выборок произвольного закона распределения плотности вероятности также может быть выполнено с использованием неравенства Чебышева, в соответствии с которым любое выборочное значение Y_k отклоняется от математического ожидания m_Y не более, чем на величину $\frac{\sigma_Y^2}{\sqrt{1-\beta}}$, т.е.

$$\left|\frac{Y_k - m_Y}{\sigma_Y^2}\right| \leq \frac{1}{\sqrt{1-\beta}},$$

где m_Y, $\sigma_Y{}^2$ – известные значения математического ожидания и дисперсии процесса соответственно, β – доверительная вероятность.

2.3 Разработка алгоритмического обеспечения методики

Для достижения поставленных требований принято решение использовать в качестве «базовых» алгоритмов методы неравенства Чебышева и контроля по предыстории, как показывающие наилучшие результаты при различных отказах.

Разработанная методика может быть представлена в виде блок-схемы алгоритма, как показано на Рисунке 21.

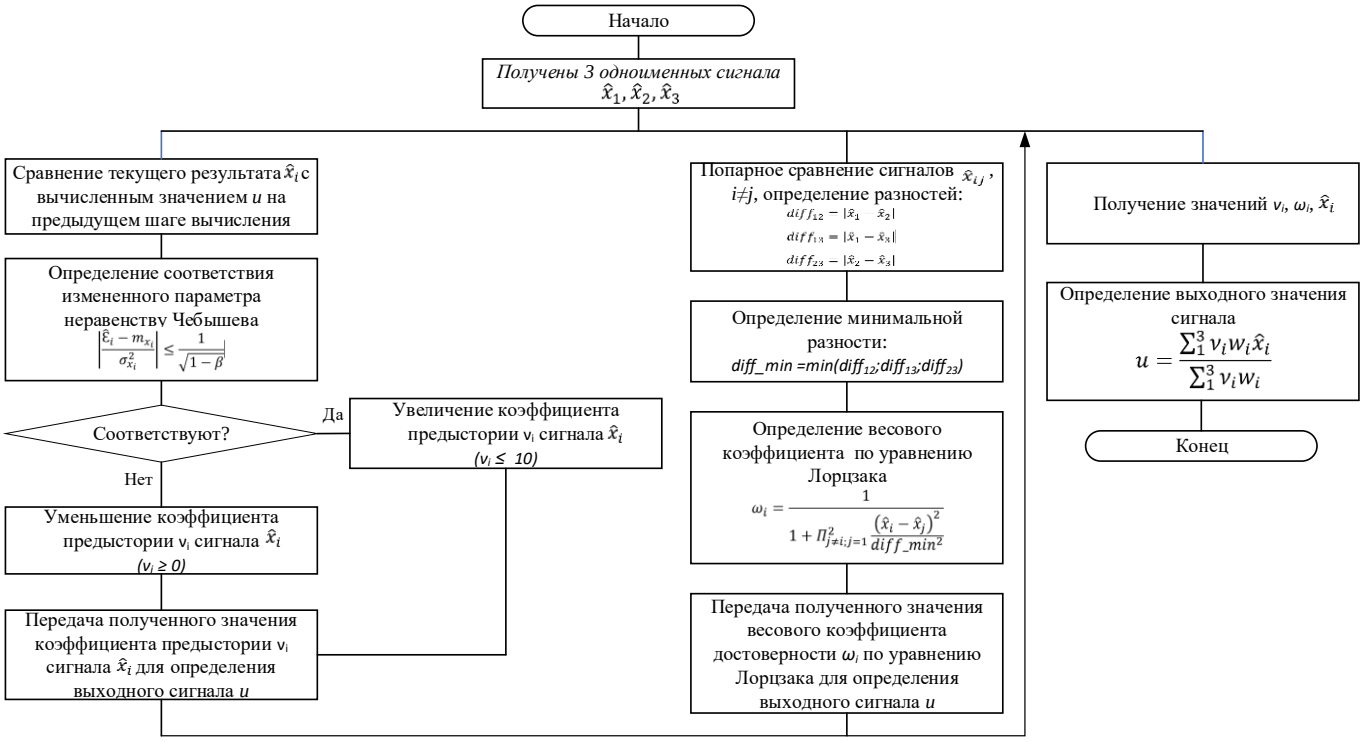

Рисунок 21. Блок-схема алгоритма адаптированной методики вычисления результирующего значения

2.4 Моделирование работы и сравнительный анализ

В данном разделе представлены результаты моделирования постепенных и внезапных отказов БИНС. Дополнительно учитывались погрешности измерений.

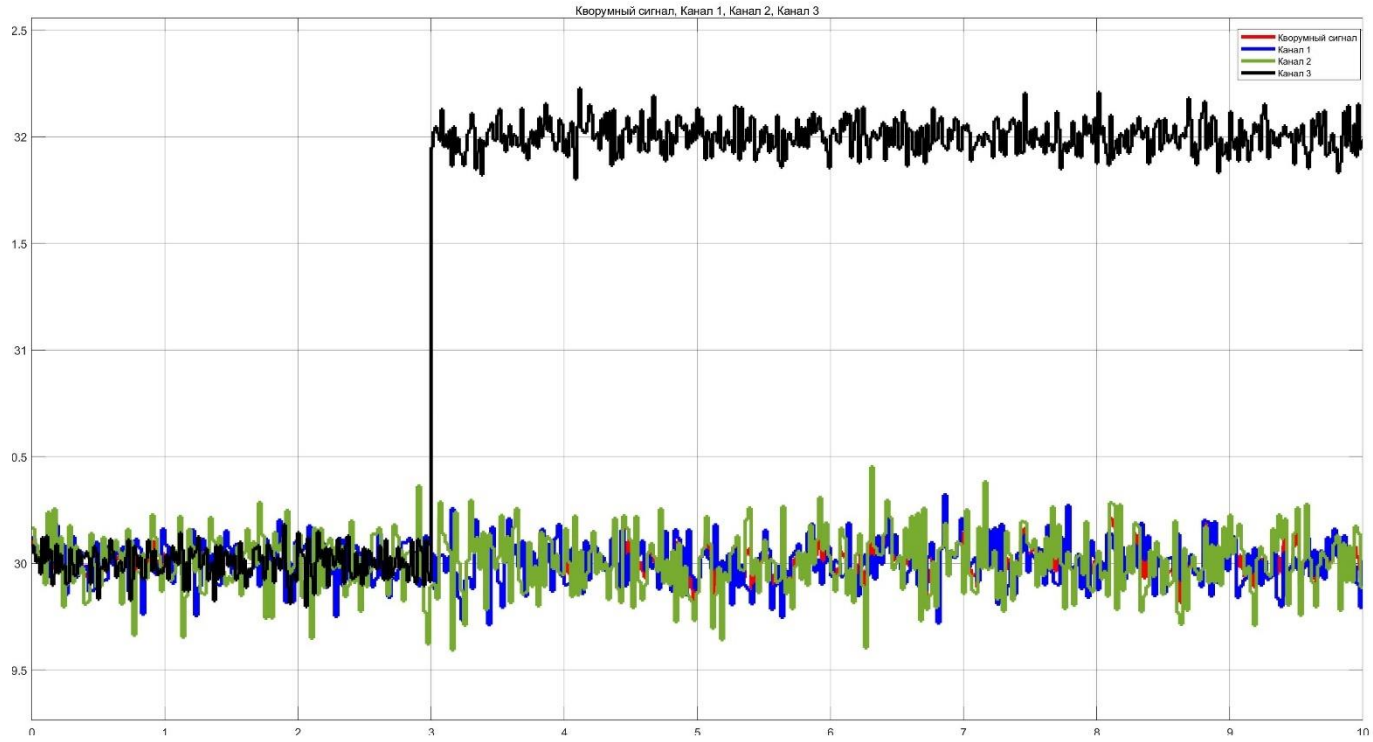

Рисунок 22. Результаты моделирования комбинированного метода при мгновенном отказе в одном канале с учетом помех

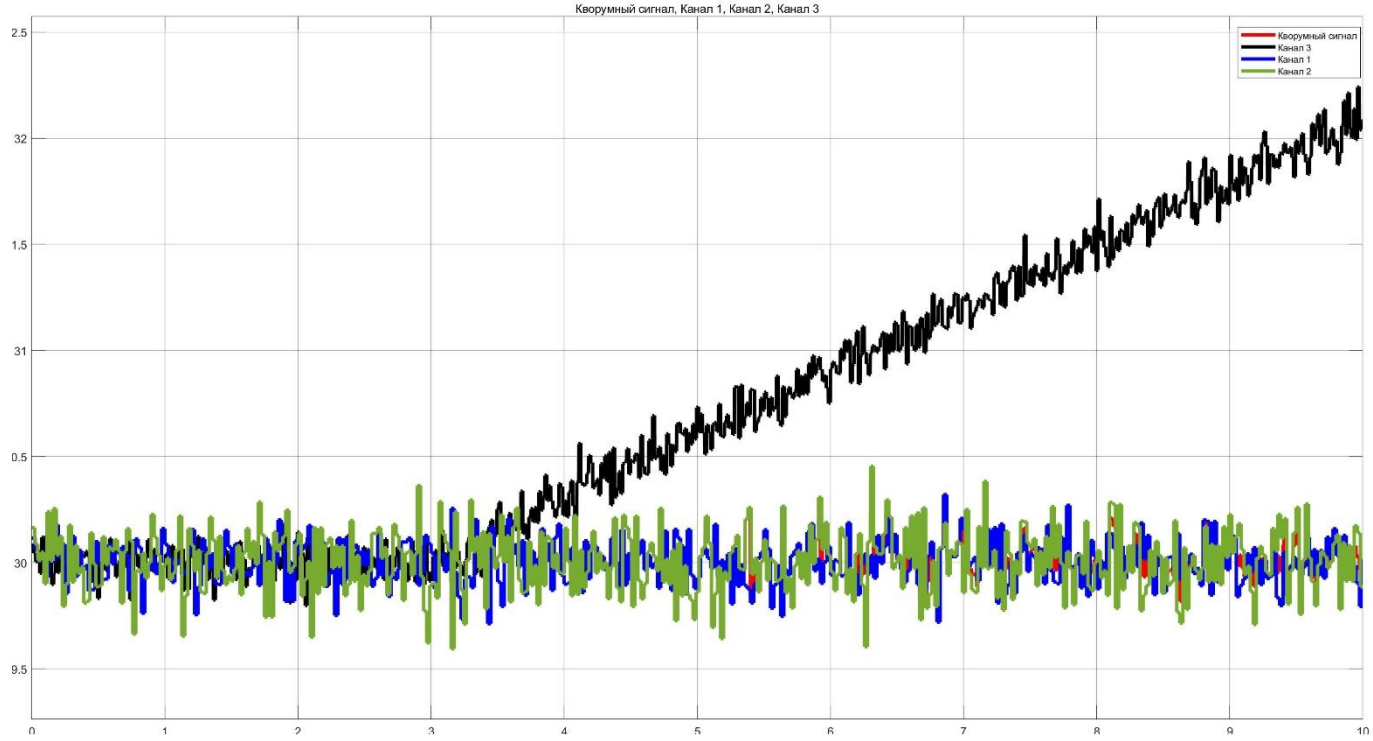

Рисунок 23. Результаты моделирования комбинированного метода при постепенном отказе в одном канале с учетом помех

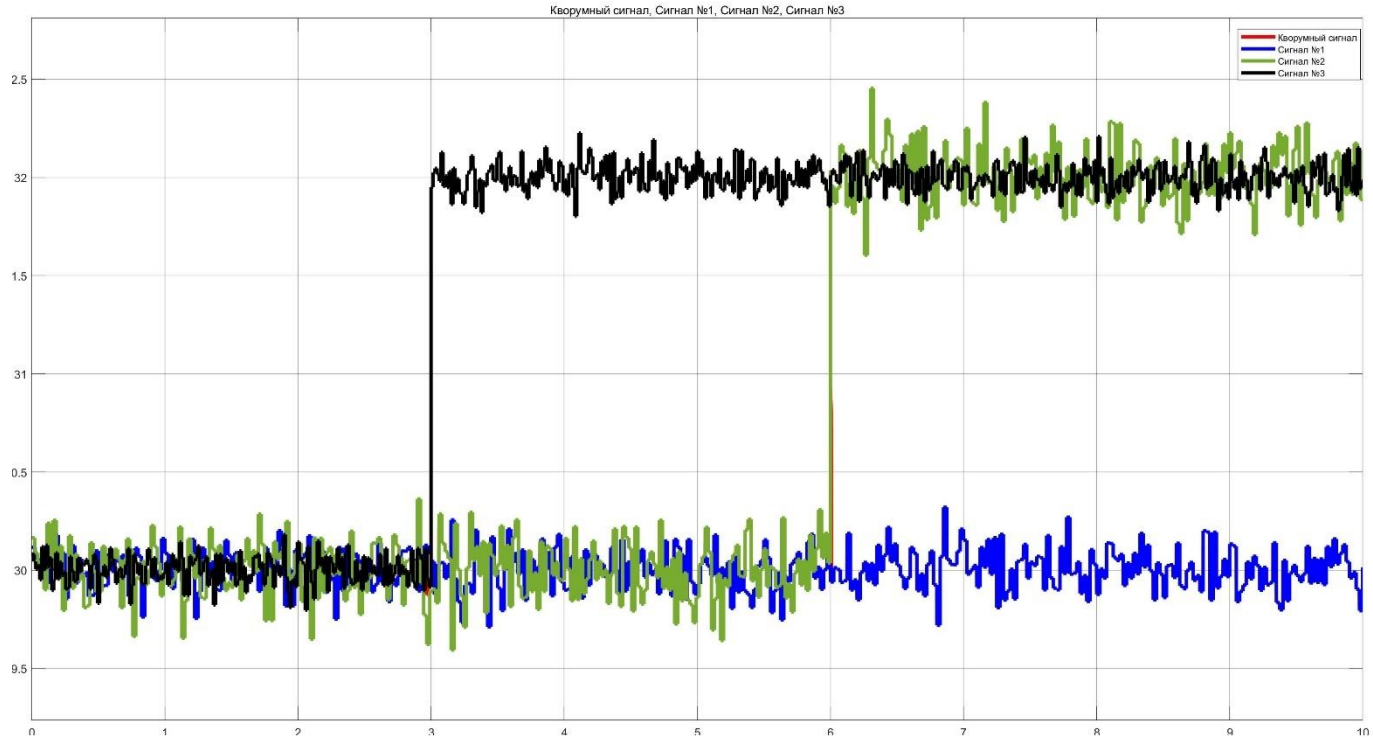

Рисунок 24. Результаты моделирования комбинированного метода при постепенном отказе в двух каналах с учетом помех

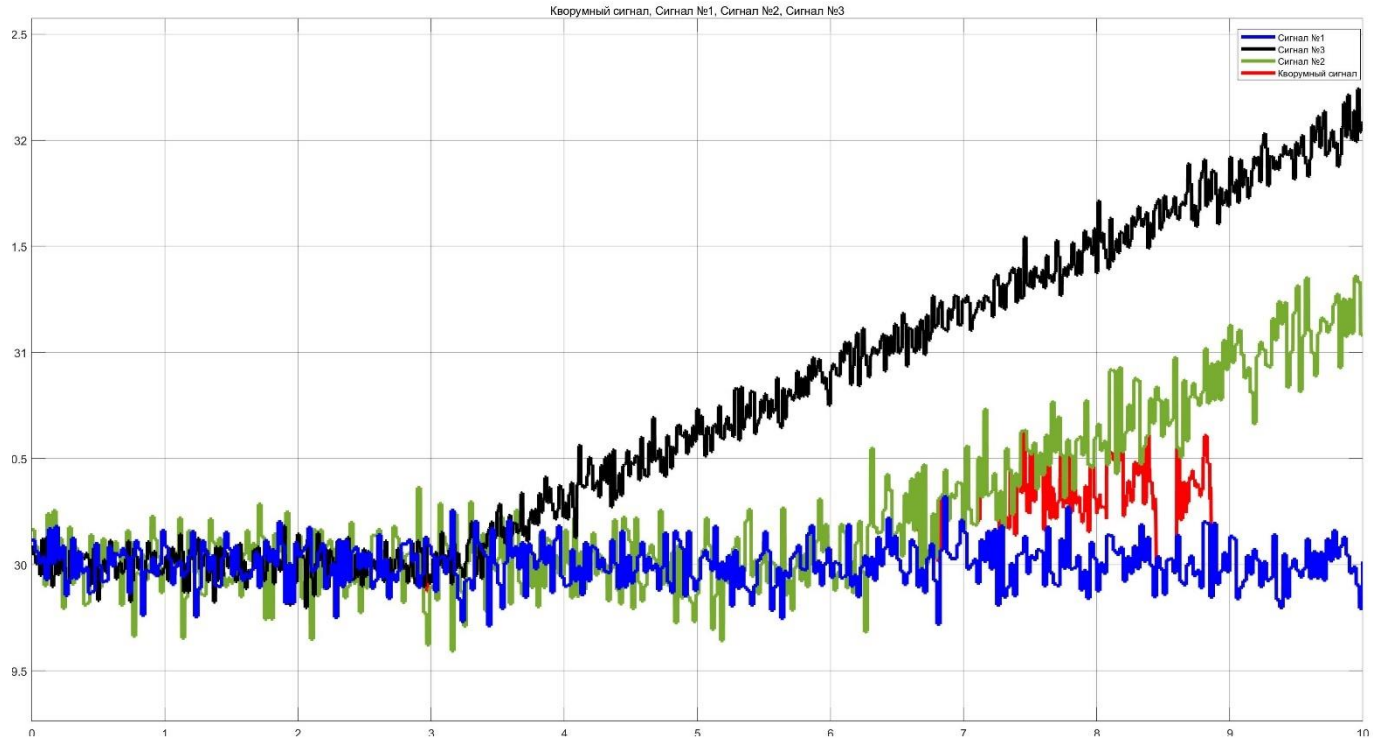

Рисунок 25. Результаты моделирования комбинированного метода при постепенном отказе в двух каналах с учетом помех

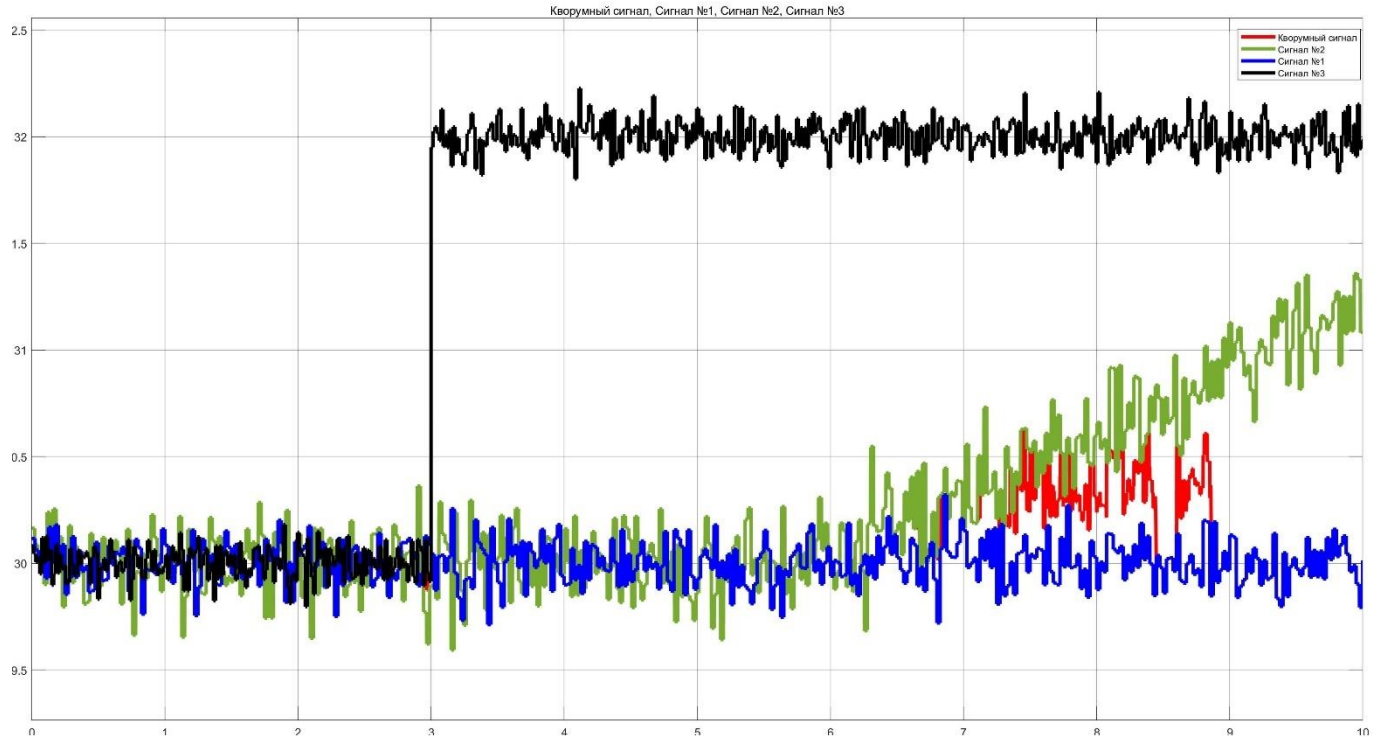

Рисунок 26. Результаты моделирования комбинированного метода при мгновенном отказе в одном канале и последующем постепенном отказе в другом канале с учетом помех

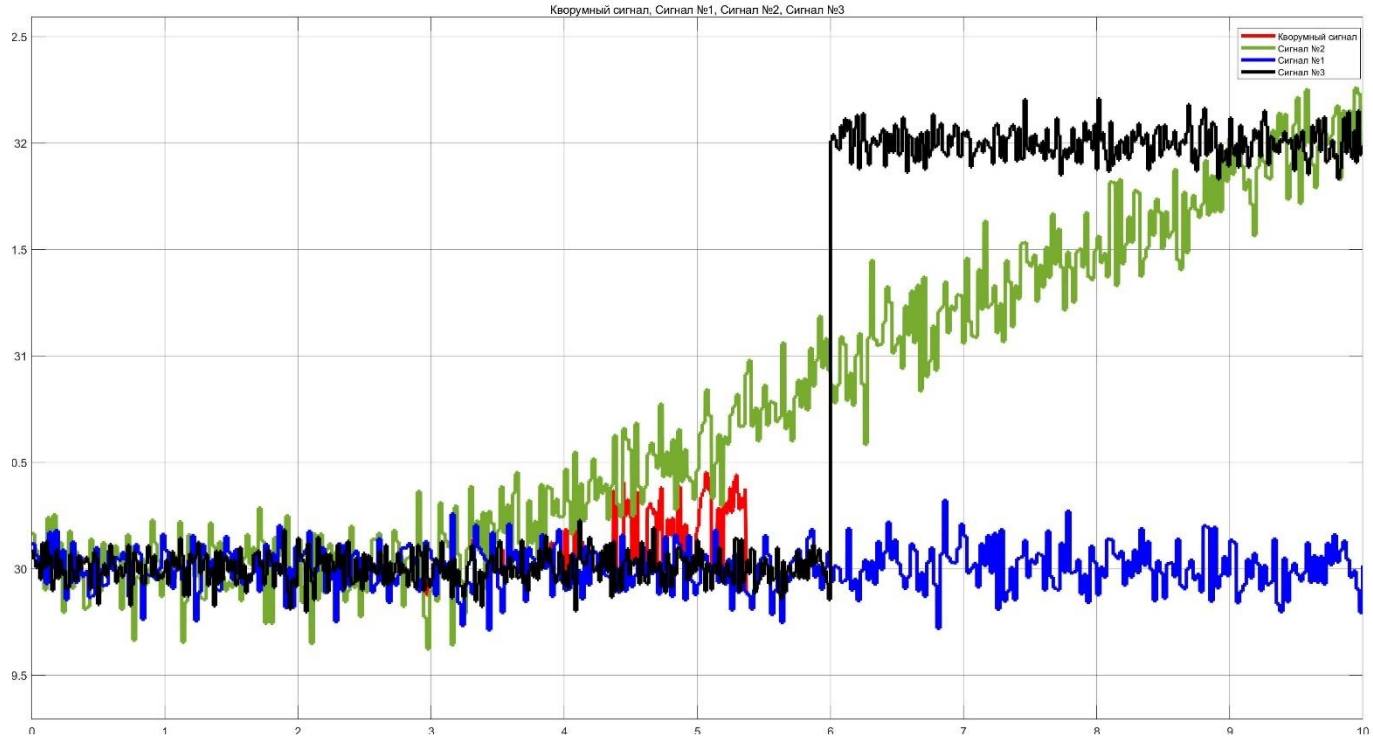

Рисунок 27. Результаты моделирования комбинированного метода при постепенном отказе в одном канале и последующем мгновенном отказе в другом канале с учетом помех

По результатам моделирования очевидно, что все заданные требования достигнуты при использовании данного метода. Найдем вероятность перехода на резервный режим КСУ.

$$P_{\text{РР}}(t) = P_{\text{кпрр}}(t) + (P_{\text{БИНС1}}(t) * P_{\text{БИНС2}}(t) * P_{\text{БИНС3}}(t)) + (P_{\text{СВС1}}(t) * P_{\text{СВС2}}(t) * P_{\text{СВС3}}(t)) + (P_{\text{КСУЛ1}}(t) * P_{\text{КСУЛ2}}(t) + P_{\text{КСУЛ1}}(t) * P_{\text{КСУЛ3}}(t) + P_{\text{КСУЛ2}}(t) * P_{\text{КСУЛ3}}(t)) * (P_{\text{КСУП1}}(t) * P_{\text{КСУП2}}(t) + P_{\text{КСУП1}}(t) * P_{\text{КСУП3}}(t) + P_{\text{КСУП2}}(t) * P_{\text{КСУП3}}(t))$$

Здесь $P_{PP}(t)$ – вероятность перехода на резервный режим КСУ, $P_{кпрр}(t)$ – вероятность отказа кнопки перехода на резервный режим, $P_{БИНСi}(t)$ – вероятность отказа i-го БИНС, $P_{СВСi}(t)$ – вероятность отказа i-го СВС, $P_{КСУЛi}(t)$ – вероятность отказа i-го левого вычислителя КСУ, $P_{КСУПi}(t)$ – вероятность отказа i-го правого вычислителя КСУ. Значением вероятности отказов КСУ можем пренебречь для простоты расчетов, т.к. параметр интенсивности отказов электронного оборудования КСУ, БИНС и СВС примерно равен. Требования АП-25 нормируют вероятность возникновения отказных состояний за 1 час полета. Тогда можем представить расчет вероятности в виде следующего выражения:

$$P_{\text{РР}}(t = 1\text{ч}) = \left(1 - e^{-\lambda_{\text{кпрр}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{БИНС1}}t}\right) * \left(1 - e^{-\lambda_{\text{БИНС2}}t}\right) * \left(1 - e^{-\lambda_{\text{БИНС3}}t}\right) + \left(\left(1 - e^{-\lambda_{\text{СВС1}}t}\right) * \left(1 - e^{-\lambda_{\text{СВС2}}t}\right) * \left(1 - e^{-\lambda_{\text{СВС3}}t}\right)\right)$$

Здесь параметр λ – интенсивность отказа соответствующих компонентов основного режима КСУ. Примем следующие значения: $\lambda_{\text{кпрр}} = 5{,}2 * 10^{-10}/\text{ч}$, $\lambda_{\text{БИНС1}} = \lambda_{\text{БИНС2}} = \lambda_{\text{БИНС3}} = 1{,}17 * 10^{-5}/\text{ч}$, $\lambda_{\text{СВС1}} = \lambda_{\text{СВС2}} = \lambda_{\text{СВС3}} = 6{,}72 * 10^{-5}/\text{ч}$. Тогда расчетное значение составит $P_{\text{РР}}(t = 1\text{ч}) = 5{,}21 * 10^{-10}$, что является событием практически невероятным (то есть, имеющим вероятность менее 10^{-9} на один час).

Таким образом, комбинированный контроль является достигает главной цели по снижению вероятности перехода на резервный режим КСУ до практически невероятной. Отмеченные в иных методах недостатки здесь отсутствуют.

2.5 Сравнение результатов работы трех алгоритмов

Дальнейшее сравнение будем вести исключительно по отклонению кворумного сигнала от реального для получения наиболее релевантных данных сравнения работ различных методик при различных видах отказов и их комбинаций без учета помех. Также не будем рассматривать метод вычисления среднего арифметического, т.к. ранее было показано, что он не обладает преимуществами по сравнению с иными методами.

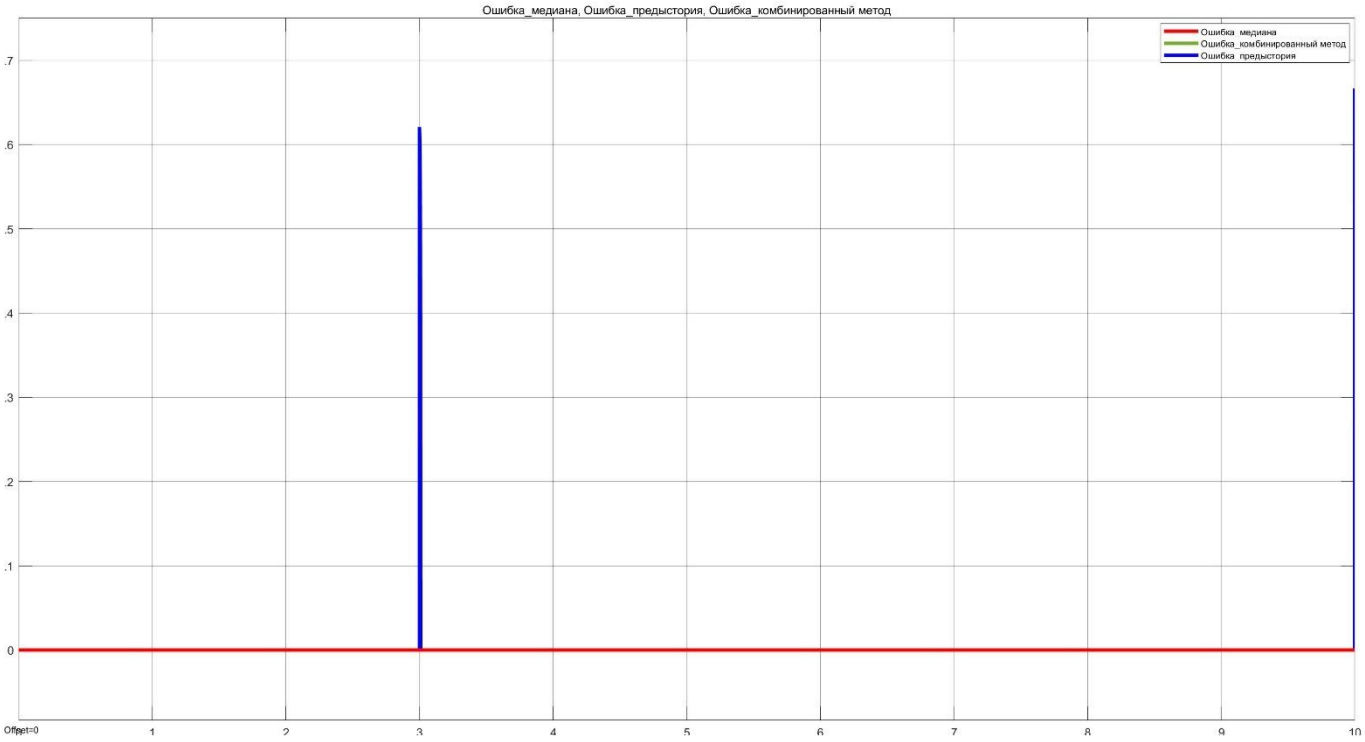

Рисунок 28. Сравнение погрешности работы трех методов кворум-контроля при мгновенном отказе в одном канале

Таблица 1. Сравнение погрешностей при мгновенном отказе в одном канале

Погрешность	**Медианное значение**	**Значение по предыстории**	**Комбинированный метод**
Абсолютная, ед	0	0,6	0
Относительная, %	0	2	0

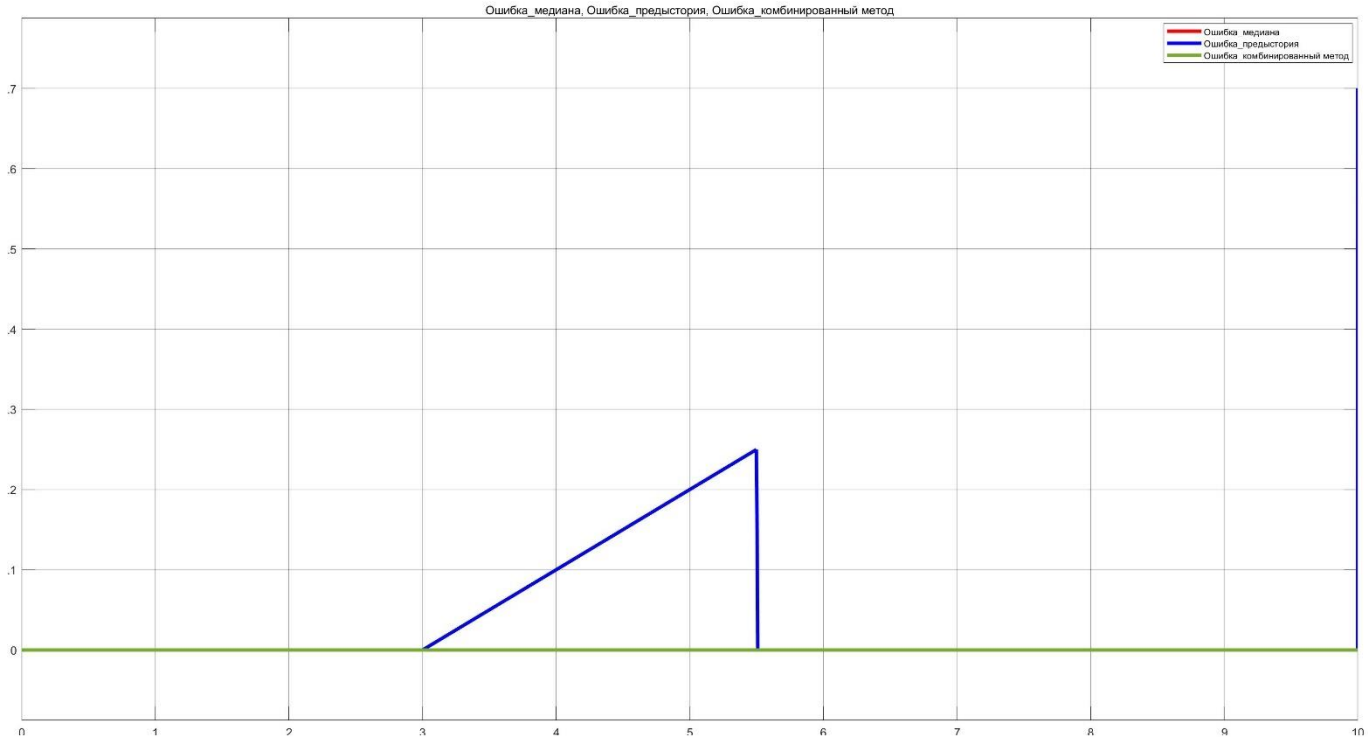

Рисунок 29. Сравнение погрешности работы трех методов кворум-контроля при постепенном отказе в одном канале

Таблица 2. Сравнение погрешностей при постепенном отказе в одном канале

Погрешность	**Медианное значение**	**Значение по предыстории**	**Комбинированный метод**
Абсолютная, ед	0	0,25	0
Относительная, %	0	0,83	0

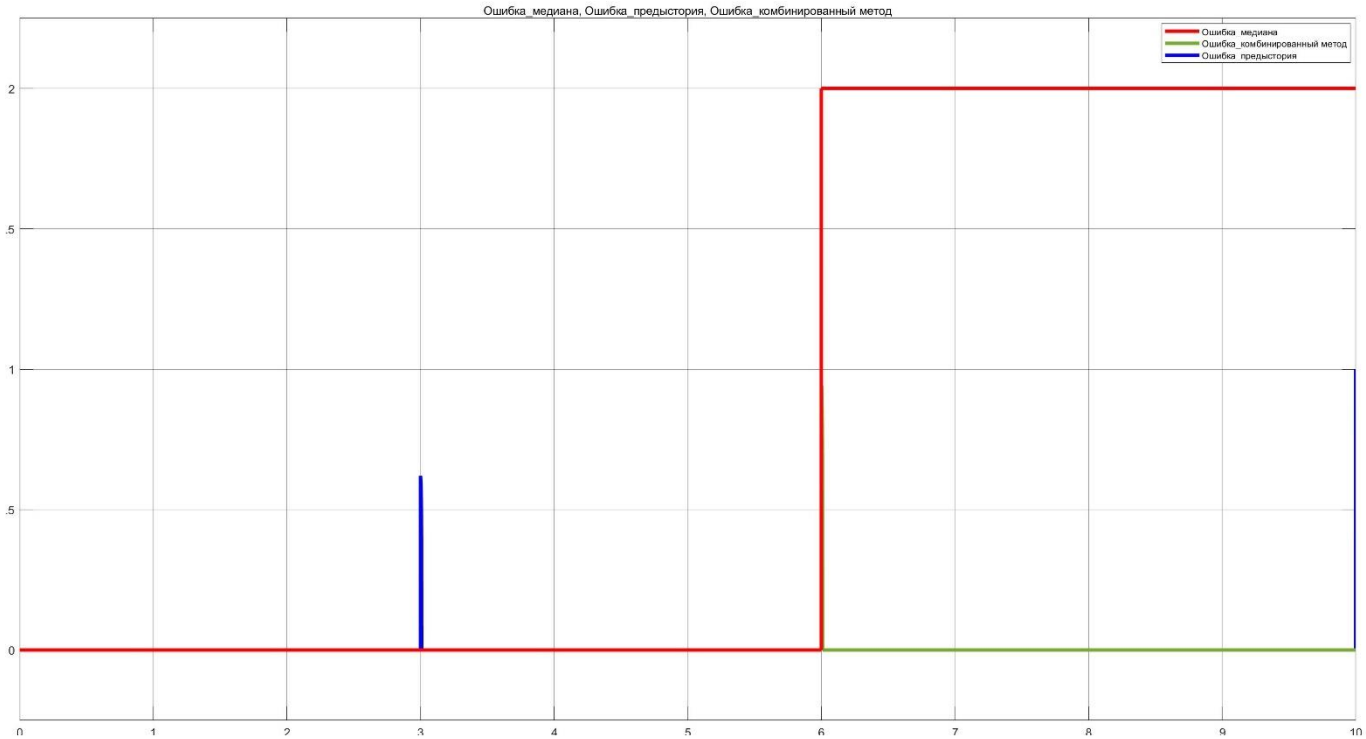

Рисунок 30. Сравнение погрешности работы трех методов кворум-контроля при мгновенном отказе в двух каналах

Таблица 3. Сравнение погрешностей при мгновенном отказе в двух каналах

Погрешность	**Медианное значение**	**Значение по предыстории**	**Комбинированный метод**
Абсолютная, ед	2	0,8	0,8
Относительная, %	6,67	2,67	2,67

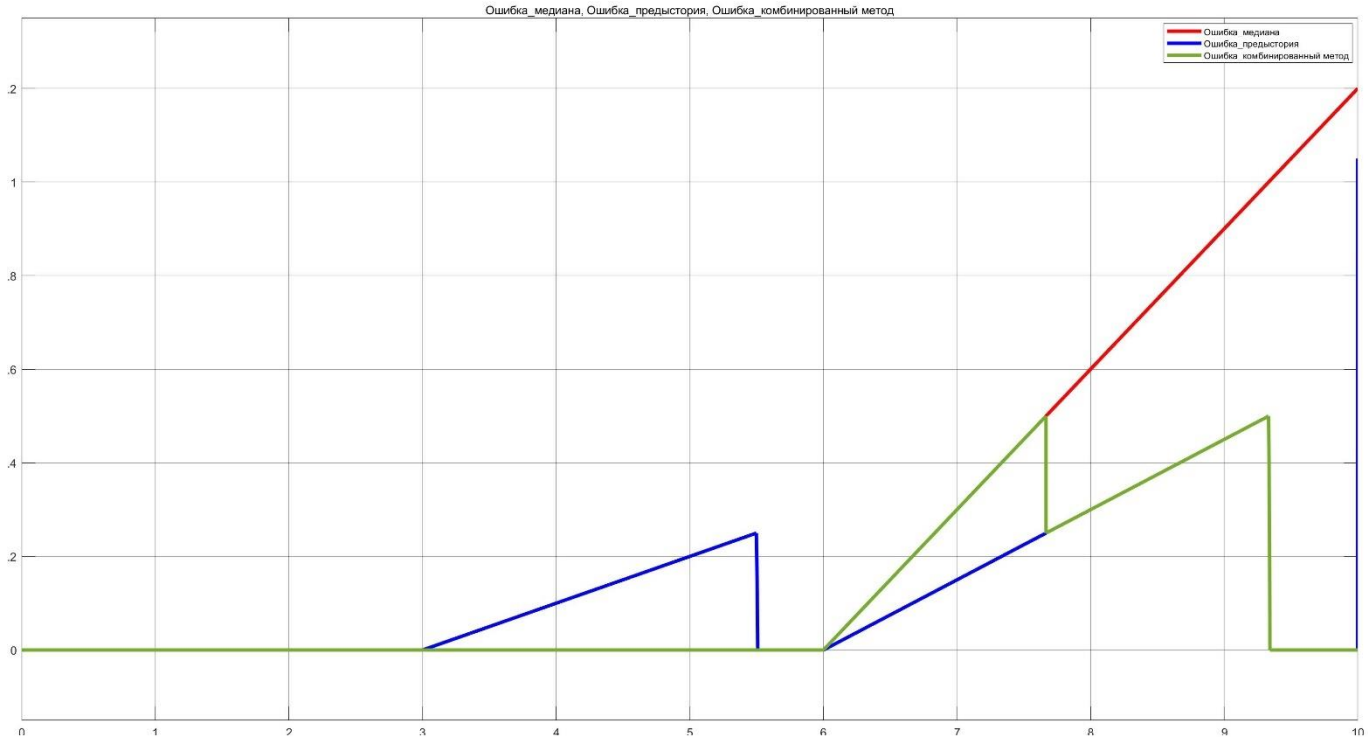

Рисунок 31. Сравнение погрешности работы трех методов кворум-контроля при постепенном отказе в двух каналах

Таблица 4. Сравнение погрешностей при постепенном отказе в двух каналах

Погрешность	**Медианное значение**	**Значение по предыстории**	**Комбинированный метод**
Абсолютная, ед	∞	0,5	0,5
Относительная, %	∞	1,68	1,68

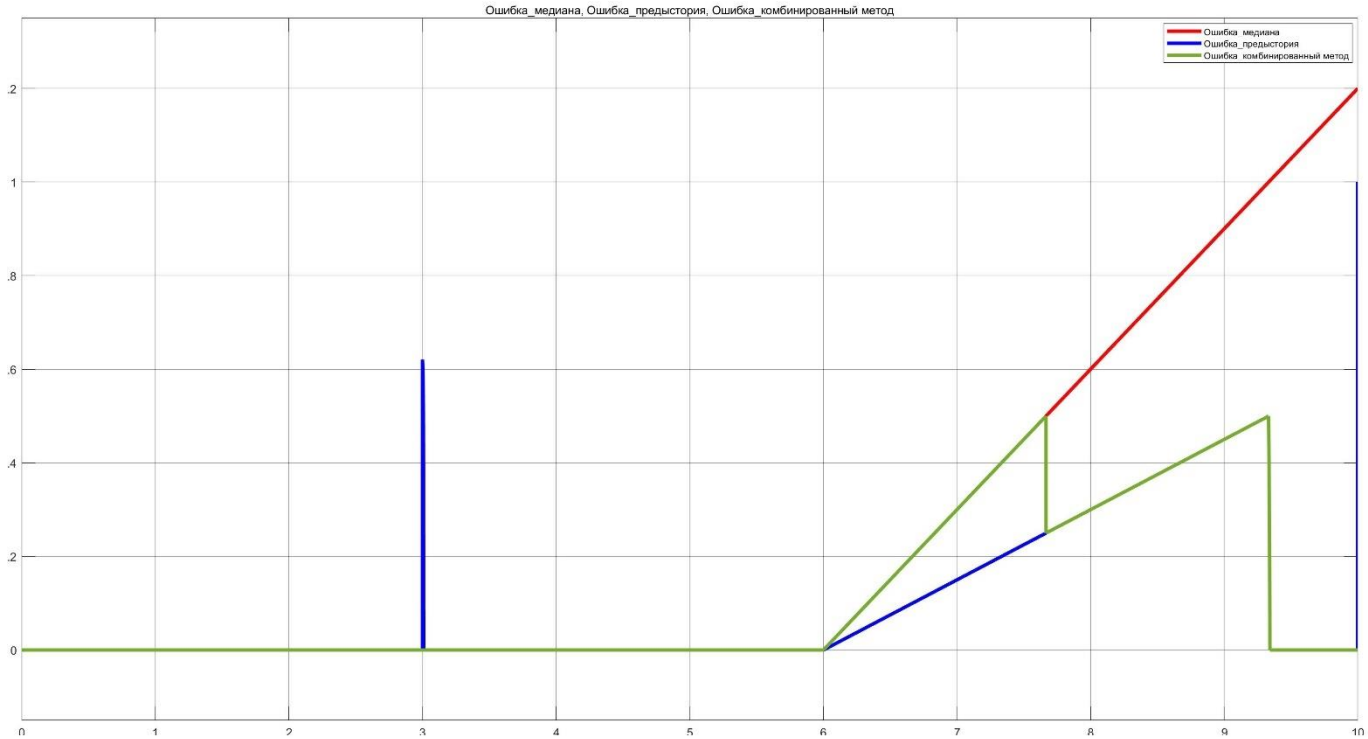

Рисунок 32. Сравнение погрешности работы трех методов кворум-контроля при мгновенном отказе в одном канале и последующем постепенном отказе в другом канале

Таблица 5. Сравнение погрешностей при мгновенном отказе в одном канале и последующем постепенном отказе в другом канале

Погрешность	**Медианное значение**	**Значение по предыстории**	**Комбинированный метод**
Абсолютная, ед	∞	0,5	0,5
Относительная, %	∞	1,68	1,68

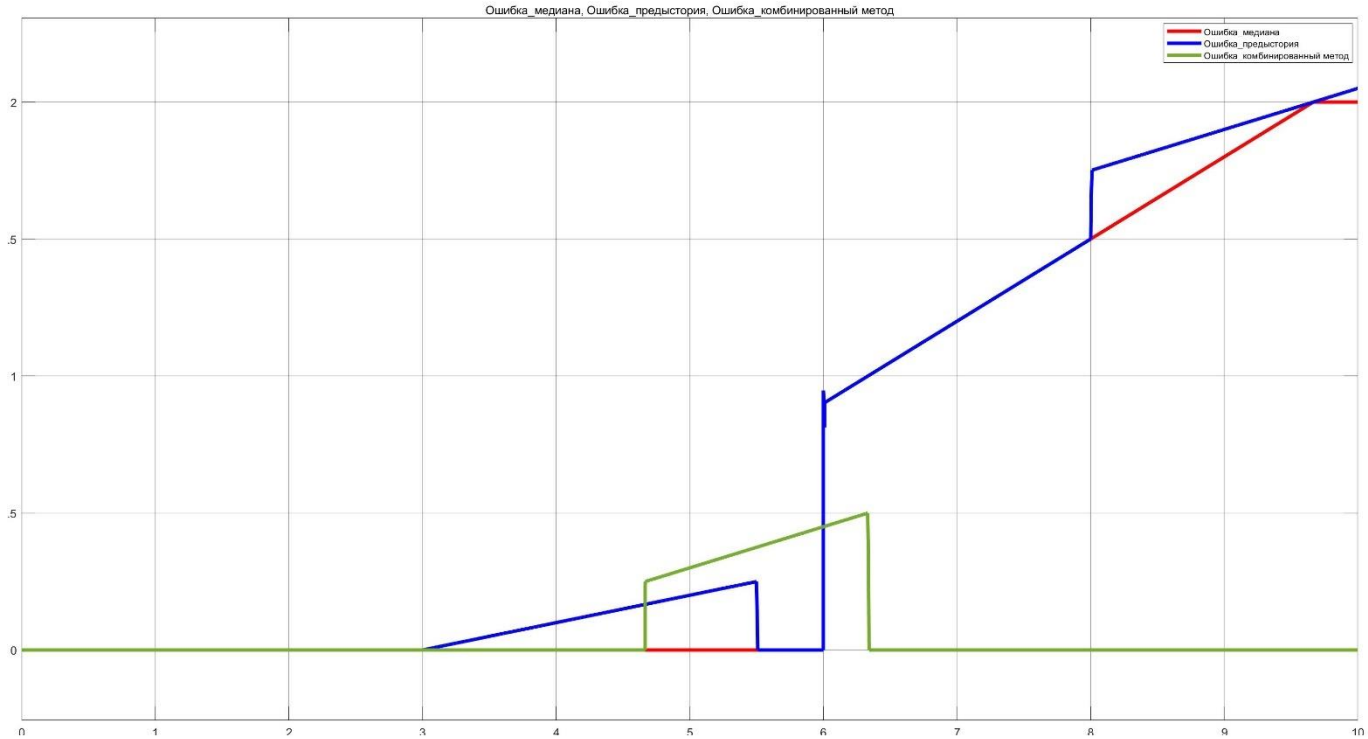

Рисунок 33. Сравнение погрешности работы трех методов кворум-контроля при постепенном отказе в одном канале и последующем мгновенном отказе в другом канале

Таблица 6. Сравнение погрешностей при постепенном отказе в одном канале и последующем мгновенном отказе в другом канале

Погрешность	**Медианное значение**	**Значение по предыстории**	**Комбинированный метод**
Абсолютная, ед	∞	∞	0,5
Относительная, %	∞	∞	1,68

По результатам сравнения результатов работы алгоритмов, можно сделать вывод о достигнутой цели в части вероятности перехода на резервный режим КСУ и количественных показателей погрешностей работы метод кворум-контроля.

Следующим шагом должна стать оценка управляемость воздушного судна при возникновении отказов с предложенным комбинированным методом контроля. Для этого должен быть реализован стенд полунатурного моделирования, как представлено в Главе 3.

Выводы по главе 2

1. Разработаны требования к комбинированному методу контроля.
2. Разработано алгоритмическое обеспечение для комбинированного методы контроля на основе свойств метода вычисления медианного значения и метода контроля по предыстории. Предусмотрены условия переключения для минимизации влияния паразитных сигналов на результирующий.
3. Проведено моделирование реализованного комбинированного метода контроля. По результатам обнаружено:
    a. Контроль обеспечивается вплоть до третьего отказа, что не было достигнуто ни одним из ранее анализированных методов;
    b. Вероятность перехода на резервный режим КСУ при использовании данного метода, становится практически невероятной, а именно 5,21e-10.
4. Следующим шагом должна стать оценка управляемости воздушного судна летным составом для определения приемлемости комбинированного метода в эксплуатации. С этой целью встает задача разработки программно-аппаратного комплекса, решение которой представлено в Главе 3.

ГЛАВА 3. РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО МОДЕЛИРОВАНИЯ ОТКАЗНЫХ СОСТОЯНИЙ

3.1 Функциональное описание испытательного стенда

С целью решения задачи оценки управляемость воздушного судна при возникновении отказов, контролируемых предложенным комбинированным методом, был разработан программно-аппаратный комплекс (стенд полунатурного моделирования), включающий в себя:

- Рабочее место оператора:
  - Рабочий компьютер (ПК или ноутбук);
  - Комплект физических имитаторов органов управления (БРУС, БРУД, педали);
- Математическая модель системы (на примере комплексной системы управления детально и упрощенно для взаимодействующих систем), имитирующая реальную динамику исполнительных механизмов (приводов) поверхностей, органов управления;
- Банк реальных аэродинамических характеристик самолета МС-21-300;
- Графические средства имитации пульта управления режимами системы автоматического управления (ПУ САУ);
- Графические средства индикации, визуализации закабинного пространства и введения отказов.

В качестве среды моделирования выбран MATLAB Simulink, как наиболее широко применяющийся на сегодняшний день комплекс ПО для решения задач математического моделирования. Математические модели комплексной системы управления, взаимодействующих систем и динамики полета самолета подготовлены с использованием встроенных в MATLAB Simulink средств стандартных библиотек.

Для выведения оператору автоматизированного рабочего места полетной информации предлагается использование различных средств визуализации закабинного пространства и предупреждающих средствах об отказах. Для этой задачи используются специализированные средства (Flight Ind, Flight Gear, Пульт ввода

отказов) с использованием протокола UDP (Universal Datagram Protocol), который не влияет на скорость моделирования, и, соответственно, оператор получают всю необходимую информацию, как ее бы получал пилот в ходе штатного полета.

ПУ САУ разработан с использованием межплатформенных программных библиотек Qt и таким же образом подключен к MATLAB Simulink с использованием UDP для повышения удобства пользователя и скорости обработки информации. Пульт ввода отказов комплексной системы управления (КСУ) представляет собой аналогично настроенный интерфейс, который включает в себя возможность отключения одного или нескольких исполнительных приводов на поверхности, отказов одной или нескольких гидравлических и электрических систем.

Для физической имитации оперативных органов управления в кабине экипажа используются коммерческие решения в области авиасимуляторов: сайдстик с программируемыми кнопками для управления по крену и тангажу, блок рычагов управления двигателями (совмещающий также функции управления механизацией крыла, тормозными щитками) и педальный пост управления для управления тормозами и рулем направления. Взаимодействие с моделью уравнений движения самолета и исполнительных устройств КСУ для замыкания системы «самолет-летчик» и динамикой самолета осуществляется с помощью драйверов и библиотеки FlightSim для MATLAB Simulink.

Реализованный стенд позволяет проводить моделирование в различных режимах для решения разных задач разных типов:

- в «нежестком» реальном времени,
- в режиме «ускоренного» времени.

Проведение моделирования в условиях «нежесткого» реального времени дает возможность оценить степень опасности имитируемых функциональных отказов за подготовленным рабочим местом оператора, в том числе, не привлекая профессиональных пилотов, т.к. использующиеся в стенде имитаторы оперативных органов управления экипажа, визуализация закабинного пространства и модель динамики самолета обеспечивают достоверное для данной задачи представление о влиянии отказов на систему и на безопасность продолжения полета. Использование

библиотек MATLAB Simulink позволяет изменять конфигурации системы и точки возникновения отказов. Благодаря данным решениям сокращаются сроки проведения имитационного моделирования по сравнению со стендовыми и летными испытаниями, требующими физической имитации отказов и «перепрошивки» ПО. Следует отметить, что данная реализация дополняет, а не заменяет стендовые и летные испытания, т.к. конечное подтверждение должно апробироваться в ходе реальных систем «самолет-летчик» для получения достоверных результатов, однако на ранних этапах разработки является полезным для сокращения ошибок при определении степени опасности функциональных отказов.

Проведение моделирования в режиме «ускоренного» времени дает возможность оценить последствия при большом количестве начальных условий введения отказа, когда не требуется оценивать вмешательство экипажа в действия самолета, либо их процедуры могут быть заданы в виде цифровой последовательности действий. Например, такое решение применимо при оценке последствий одного и того же функционального отказа на различных стадиях полета, при отличающихся метеоусловиях (сдвиги ветра, коэффициент скольжения по полосе и другие), аварийных конфигурациях, которые ухудшают последствий отказа (например, потеря работоспособности гидросистем, электросистем или критического двигателя). Используя данный способ моделирования, могут быть заданы матрицы начальных условий в цикле, при этом на операторе остается задача контроля хода моделирования. Результаты каждого отдельного моделирования анализируются на соответствие заранее сформированным критериям особых ситуаций (зависящим от углов, перегрузок, скоростей и т.д.), и на этом основании делается вывод о степени опасности каждого отказного состояния в различных условиях.

Функциональное взаимодействие компонентов аппаратного и программного обеспечения испытательного стенда представлено на рисунке 34 [10].

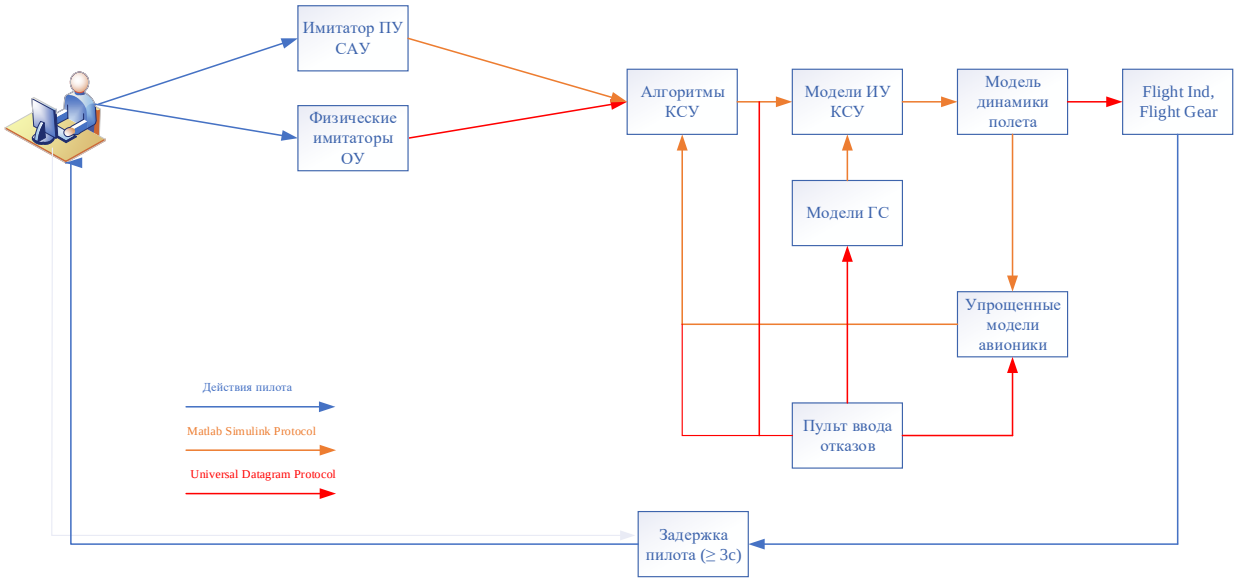

Рисунок 34. Функциональная схема разработанного стенда

3.2 Аппаратная реализация испытательного стенда

Для реализации указанного функционала были выбраны доступные в свободной продаже изделия. Следует иметь в виду, что для выбранного ноутбука могут использоваться аналогичные с соответствующими (или лучше) характеристиками. Оборудование было закуплено с использованием средств, полученных для реализации гранта РФФИ № 20-31-90028.

Для рабочего места оператора был выбран ноутбук Xiaomi Redmibook Pro со следующими основными характеристиками:

- Процессор Intel Core i7 11-ого поколения с тактовой частотой 3200 МГц;
- Оперативная память – 16 Гб;
- Видеокарта – NVIDIA GeForce MX450, 2Гб;
- Операционная система – Windows 10 Home.

В качестве физических имитаторов органов управления были выбраны:

- Для БРУС: джойстик Thrustmaster Hotas Warthog Flight Stick (см. Рисунок 35);
- Для БРУД, РУМК, РУВТ: Thrustmaster Hotas Warthog Dual Throttle (см. Рисунок 36);
- Для педалей: Logitech G Saitek Pro Flight Rudder Pedals (см. Рисунок 37).

Рисунок 35. Thrustmaster Hotas Warthog Flight Stick

Рисунок 36. Thrustmaster Hotas Warthog Dual Throttle

Рисунок 37. Logitech G Saitek Pro Flight Rudder Pedals

Банк аэродинамических характеристик задается в виде табличной функции на основе результатов исследования аэродинамических свойств воздушного судна. Значения аэродинамических коэффициентов зависят от варьируемых параметров массы, центровки, положения закрылков и предкрылков, этапов полета и иных параметров.

Каждый вид отказа моделируется исходя из консервативных предположений, что отказ случится наихудшим образом (например, скорость самопроизвольного перемещения привода будет такова, что контроль по скорости или положению не сможет его определить). Алгоритмическая реализация каждого вида отказа

индивидуальна и выполняется также с использованием стандартных функций MATLAB Simulink.

3.3 Результаты испытаний

Было проведено по 48 испытаний на наиболее критичных этапах полета – взлете и посадке при различных конфигурациях механизации крыла, массы и центровки для каждого из методов контроля. Отказы имитировались в канале угла крена КСУ для ручного режима управления системой электродистанционного управления (СДУ) и автоматического режима управления системой автоматического управления (САУ). Оценка проводилась по качественным ощущениям оператора стенда полунатурного моделирования.

№	Режим	RUM	H, м	VCAS, км/ч	G, кг	Xт, доли ba	Yт, м	Zт, м	Ix, кгмс2	Iy, кгмс2	Iz, кгмс2	Ixy, кгмс2	ϕ0, град	Вид отказа	Оценка (медиана)	Оценка (предыстория)	Оценка (комбинированный метод)
1.	КСУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
2.	КСУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
3.	КСУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС/УУП	БС/УУП
4.	КСУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
5.	КСУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
6.	КСУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
7.	КСУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
8.	КСУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
9.	КСУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС/УУП	БС/УУП
10.	КСУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
11.	КСУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС

№	Режим	RUM	H, м	VCAS, км/ч	G, кг	Xт, доли ba	Yт, м	Zт, м	Ix, кгмс2	Iy, кгмс2	Iz, кгмс2	Ixy, кгмс2	ϕ0, град	Вид отказа	Оценка (медиана)	Оценка (предыстория)	Оценка (комбинированный метод)
12.	КСУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
13.	КСУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
14.	КСУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
15.	КСУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС/УУП	БС/УУП
16.	КСУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
17.	КСУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
18.	КСУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
19.	КСУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
20.	КСУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
21.	КСУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС/УУП	БС/УУП
22.	КСУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
23.	КСУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
24.	КСУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
25.	КСУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
26.	КСУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
27.	КСУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС/УУП	БС/УУП
28.	КСУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС

№	Режим	RUM	H, м	VCAS, км/ч	G, кг	Xт, доли ba	Yт, м	Zт, м	Ix, кгмс2	Iy, кгмс2	Iz, кгмс2	Ixy, кгмс2	ϕ0, град	Вид отказа	Оценка (медиана)	Оценка (предыстория)	Оценка (комбинированный метод)
29.	КСУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
30.	КСУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
31.	КСУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
32.	КСУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
33.	КСУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС/УУП	БС/УУП
34.	КСУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
35.	КСУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
36.	КСУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
37.	КСУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
38.	КСУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
39.	КСУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС/УУП	БС/УУП
40.	КСУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
41.	КСУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
42.	КСУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
43.	КСУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
44.	КСУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
45.	КСУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС/УУП	БС/УУП

№	Режим	RUM	H, м	VCAS, км/ч	G, кг	Xт, доли ba	Yт, м	Zт, м	Ix, кгмс2	Iy, кгмс2	Iz, кгмс2	Ixy, кгмс2	ϕ0, град	Вид отказа	Оценка (медиана)	Оценка (предыстория)	Оценка (комбинированный метод)
46.	КСУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
47.	КСУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
48.	КСУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
49.	САУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
50.	САУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
51.	САУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС	БС
52.	САУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
53.	САУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
54.	САУ	0	500	570	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
55.	САУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
56.	САУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
57.	САУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС	БС
58.	САУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
59.	САУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
60.	САУ	0	500	400	60000	0,25	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
61.	САУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
62.	САУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС

№	Режим	RUM	H, м	VCAS, км/ч	G, кг	Xт, доли ba	Yт, м	Zт, м	Ix, кгмс2	Iy, кгмс2	Iz, кгмс2	Ixy, кгмс2	ϕ0, град	Вид отказа	Оценка (медиана)	Оценка (предыстория)	Оценка (комбинированный метод)
63.	САУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС	БС
64.	САУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
65.	САУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
66.	САУ	0	1000	450	60000	0,30	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
67.	САУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
68.	САУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
69.	САУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС	БС
70.	САУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
71.	САУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
72.	САУ	0	1000	400	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
73.	САУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
74.	САУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
75.	САУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС	БС
76.	САУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
77.	САУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
78.	САУ	0	4000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
79.	САУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС

№	Режим	RUM	H, м	VCAS, км/ч	G, кг	Xт, доли ba	Yт, м	Zт, м	Ix, кгмс2	Iy, кгмс2	Iz, кгмс2	Ixy, кгмс2	ϕ0, град	Вид отказа	Оценка (медиана)	Оценка (предыстория)	Оценка (комбинированный метод)
80.	САУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
81.	САУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС	БС
82.	САУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
83.	САУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
84.	САУ	0	5000	420	70000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
85.	САУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
86.	САУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
87.	САУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС	БС
88.	САУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
89.	САУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
90.	САУ	3	400	335	75000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС
91.	САУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в одном канале БИНС	БС	БС	БС
92.	САУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в одном канале	БС	БС	БС
93.	САУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный в двух каналах	КС	БС	БС
94.	САУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный в двух каналах	КС	БС	БС
95.	САУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Мгновенный + постепенный	КС	БС	БС
96.	САУ	3	400	300	50000	0,17	-0,661	0	0	0	362769	-15535	-1	Постепенный + мгновенный	КС	КС	БС

По результатам проведенных 288 испытаний были подтверждены выводы, полученные в ходе второй главы, о наибольшей приемлемости предложенного комбинированного метода кворум-контроля как для ручного режима управления, так и при управлении под автопилотом.

Дальнейшие результаты должны найти отражение в виде расчета вероятностей с помощью анализа дерева отказов. Концепция модельно-ориентированного подхода к оценке безопасности предполагает возможность использования диаграмм состояния.

3.4 Алгоритмическое обеспечение выполнение анализа дерева отказов

3.4.1 Алгоритмическое обеспечение разработки диаграмм состояния

Моделирование состояний системы и переходов между ними в научных работах подразделяются на использование концепций диаграмм состояния, использующих в своей концепции метод детерминированных конечных автоматов [11 – 18], и сетей Петри [19 – 31]. В ходе настоящей работы будет использоваться подход диаграмм состояний как более современный, удобный для практического применения и имеющий непосредственную реализацию в инструменте MATLAB Simulink с интеграцией в инструмент по расчету надежности и оценке безопасности ANSYS medini analyze.

Для описания концепции учитываются термины:

Детерминированные конечные автоматы (далее – автомат) включают набор состояний и переходов между ними, зависящих от входных данных. При этом, такие автоматы характеризируются тем, что следующее состояние однозначно определяется текущим состоянием и выход зависит только от текущего состояния и текущего входа.

Детерминированный конечный автомат состоит из следующих компонентов:

- конечное множество *состояний,* обозначаемых *Q;*
- Конечное множество *входных символов*, обозначаемых обычно как Σ.
- *Функция переходов,* аргументами которой являются текущее состояние и входной символ, а значением – новое состояние. Функция переходов

обычно обозначается как δ. Далее представляя автомат в виде графа, δ будет изображаться отмеченными дугами, соединяющими состояния. Если q – состояние и a – входной символ, то $\delta(q, a)$ – это состояние p, для которого существует дуга, отмеченная символом a и ведущая из q в p.

- *Начальное состояние* – одно из состояний в Q;
- Множество *заключительных* состояний F, являющегося подмножеством Q.

Таким образом, автомат может быть представлен в виде $A = (Q, \Sigma, \delta, q_0, F)$, где A – имя автомата, Q – множество состояний, Σ – множество входных символов, δ – функция переходов, q_0 – начальное состояние и F – множество заключительных состояний.

Определение ДКА как набор пяти объектов с подробным описанием функции переходов достаточно трудно для восприятия. Существует два более удобных способа описания автоматов:

1. *Диаграмма переходов*, которая представляет собой граф;
2. *Таблица переходов*, дающая табличное представление функции δ. Из нее очевидны состояния и входной алфавит.

Диаграмма переходов для автомата вида $A = (Q, \Sigma, \delta, q_0, F)$ есть граф, определяемый следующим образом:

- Всякому состоянию из Q соответствует некоторая вершина;
- Пусть $\delta(q,a)=p$ для некоторого состояния $q \in Q$ и входного символа $a \in \Sigma$. Тогда диаграмма переходов должна содержать дугу из вершины q в вершину p, отмеченную a. Когда присутствуют более одного входных символов, переводящих автомат из состояния q в состояние p, то диаграмма переходов может содержать одну дугу, отмеченную списком этих символов;
- диаграмма содержит стрелку в начальное состояние, отмеченную как *Начало*. Эта стрелка не выходит ни из какого состояния;

- вершины, соответствующие заключительным состояниям (состояниям из *F*), отмечаются двойным кружком. Состояния, не принадлежащие *F*, изображаются простым (одинарным) кружком [32].

В поддержку выполнения АДО, должен быть разработан автомат, где начальным состоянием является полностью исправное состояние части системы, а заключительным состоянием является непосредственно отказное состояние, определенное в ОФО.

3.4.2 Алгоритмическое обеспечение генерации дерева

Генерация дерева отказов из модели MATLAB Simulink происходит встроенными средствами инструмента Ansys medini analyze, который широко применим в авиационной промышленности.

Для выбранного порта вывода в АДО создается узел как сценарий события верхнего уровня. Этот сценарий возникает либо в случае, если выходной порт предоставляет неправильный результат, вызванный неправильным расчетом или неправильными входными сигналами, либо в случае, если контейнер этого выходного порта вообще выходит из строя, например, из-за аппаратного сбоя. В обоих случаях генерируются события, которые связаны с событием верхнего уровня (сценарием) логическим элементом ИЛИ.

Если выходной порт соединен с выходным портом изолированного блока или подсистемы, то этот порт вывода выйдет из строя в случае, если содержащийся блок (или подсистема) выйдет из строя или выходной порт содержащегося блока предоставит неверный сигнал.

Если содержащийся блок или подсистема не содержит каких-либо дополнительных блоков или подсистем, тогда выходной порт, подключенный к этому содержащемуся блоку (или подсистеме), выйдет из строя либо при сбое контейнера, либо в случае, если его входы предоставляют неправильные сигналы.

Набор конечных событий в АДО включает все входы на том же уровне иерархии выбранного выходного порта, которые вносят вклад в этот выходной порт.

Если событие происходит более одного раза в сгенерированном АДО, то оно создается только один раз, а для всех остальных событий создаются соответствующие символы перехода.

В случае, если базовая модель Simulink вызовет цикл в дереве отказов, этот цикл предотвращается путем создания копии события для уже посещенного выходного порта, который получает постфикс имени «+ T», который означает, что это же событие происходит на шаг позже. После этого навигация по этому пути модели Simulink отменяется. На этот механизм предотвращения зацикливания может влиять параметр, который позволяет выполнять цикл более одного раза.

3.4.3 Алгоритмическое обеспечение бюджетирования вероятности

На этапе предварительной оценки безопасности в ходе выполнения АДО стоит задача бюджетирования заданных показателей надежности (в виде максимально допустимой вероятности) на компоненты системы. Алгоритм такого бюджетирования представлен на рисунке 38.

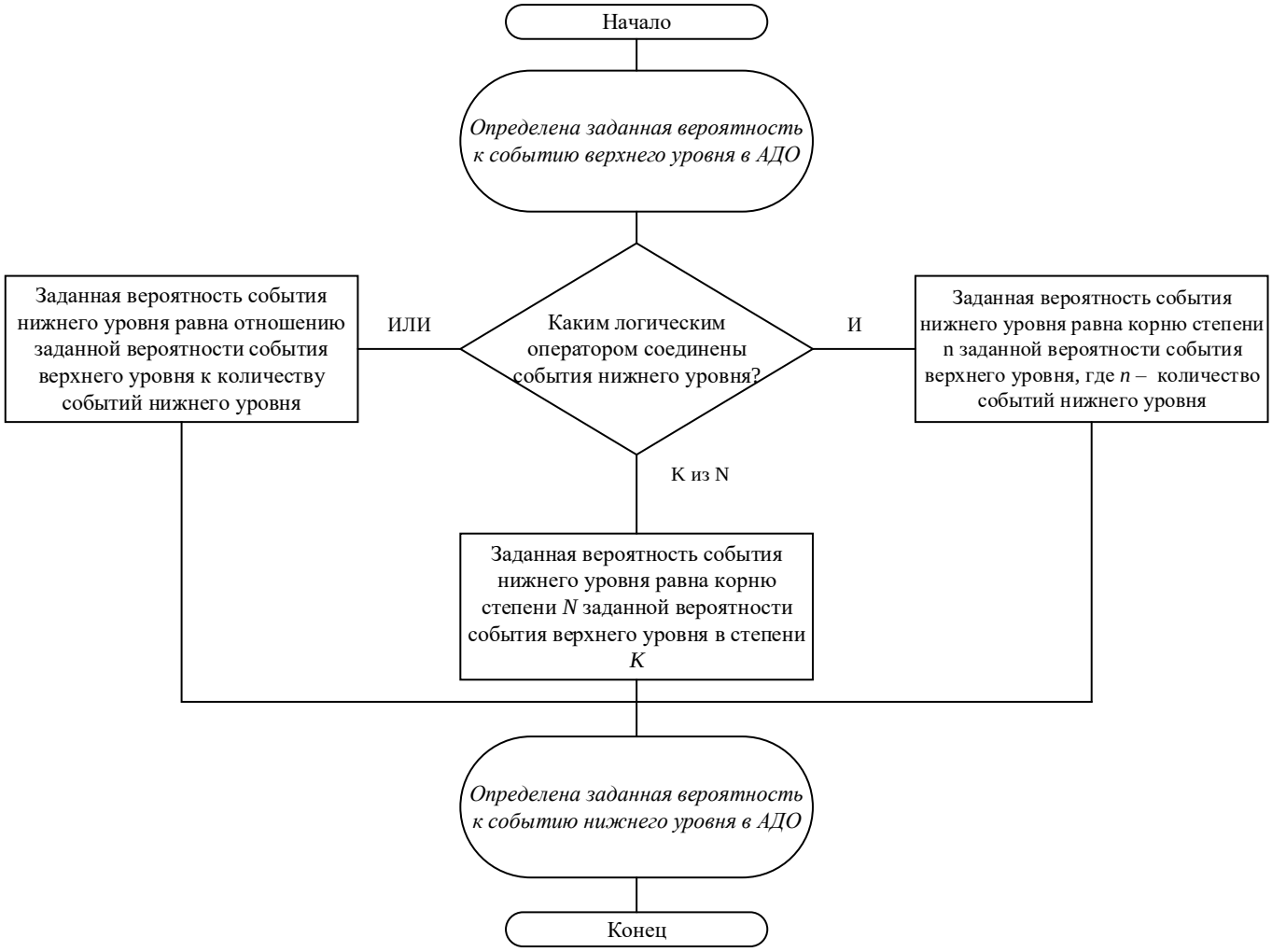

Рисунок 38. Алгоритм бюджетирования заданных показателей вероятности

3.4.4 Алгоритмическое обеспечение расчета вероятности отказного состояния

В ходе выполнения количественного АДО требуется расчет итоговой вероятности отказного состояния. Выделяют различные количественные характеристики:

1. Недоступность *Q(t)*, рассчитывающаяся по формуле Шеннона [33]:

$$Q(t) = P(E_i)P(TLE \mid E_i) + P\left(\overline{E_i}\right)P(TLE \mid \overline{E_i}) \qquad (1),$$

Где E_i – каждое базовое событие в АДО, а TLE – Top Level Effect – событие верхнего уровня.

2. Средняя вероятность отказа в произвольный момент времени в соответствии с IEC 61508 [34]:

$$Q_{cp}(T) = \frac{\int_{o}^{T} Q(t)dt}{T} \qquad (2)$$

3. Ненадежность (по Везели) – вероятность возникновения верхнего события в интервале [0..T]. Ненадежность вычисляется на основе формулы аппроксимации Везели, то есть через условную интенсивность отказов, которая, в свою очередь, выводится из частоты отказов *w(t)*: [35]:

$$F(T) = 1 - e^{-\int_{0}^{T} \lambda(t)dt} \qquad (3), \text{ где}$$

$$\lambda(t) = \frac{w(t)}{1 - Q(t)} \qquad (4).$$

Существуют и другие способы расчета надежности, но данные три являются основными в авиационной сфере. В работе использовался метод Шеннона, использующий в своей основе расчет величины недоступности *Q(t).* Следует отметить, что вероятности базовых отказов зависят от параметра интенсивности отказа, ремонтопригодности и обследуемости, т.е. должны учитывать период проявления (скрытого состояния) отказа. В таком случае, вероятность каждого базового события принимает вид, как представлено на формулах (5) для обследуемых и (6) для ремонтопригодных изделий.

$$P(E_i) = 1 - e^{-\lambda(t \bmod \tau)} \qquad (5)$$

$$P(E_i) = \left(\frac{\lambda}{\lambda + \mu}\right)\left(1 - e^{-(\lambda+\mu)t}\right) \qquad (6)$$

Здесь τ – параметр обследуемости (в часах) и μ - показатель ремонтопригодности (в 1/ч).

3.4.5 Алгоритмическое обеспечение анализа надежности

Ключевым подготовительным этапом выполнения АВПО является расчет надежности компонентов системы. Лучшим способом является изучение опыта эксплуатации аналогичных изделий в аналогичных условиях эксплуатации. Чаще

всего эта информация недоступна, т.к. является коммерческой тайной, либо наработка достаточно мала и любой отказ сильно влияет на имеющуюся выборку. В таких случаях прибегают к методам прогнозирования надежности. Методики прогнозирования надежности оборудования различаются для электронных и механических компонентов.

Надежность электронных компонентов можно прогнозировать в соответствии со справочниками. Отечественный справочник ЭРИ-2006 дает достаточное количество информации о стандартных радиоэлектронных изделиях и конкретных типономиналах в различных ожидаемых условиях эксплуатации. Согласно данному справочнику, эксплуатационная интенсивность отказов $\lambda_э$ любой группы ЭРИ может быть представлена в соответствии со следующей математической моделью:

$$\lambda_э = \lambda_б \prod_{i=1}^{n} K_i \qquad (7),$$

где $\lambda_б$ – базовая интенсивность отказов типа ЭРИ, рассчитанная по результатам испытаний ЭРИ на безотказность, долговечность и ресурс;

K_i – коэффициенты, учитывающие изменения эксплуатационной интенсивности в зависимости от различных факторов;

n – число учитываемых факторов.

Таблица 7 содержит основные коэффициенты, относящиеся к различным типам ЭРИ.

Таблица 7. Основные коэффициенты, использующиеся при прогностическом расчете надежности некоторых типов ЭРИ

Условное обозначение коэффициента	Физический смысл коэффициента
Общие коэффициенты моделей	
Кр	коэффициент режима (воспринимаемая электрическая нагрузка, температура окружающей среды)
Кпр	коэффициент приемки
Кэ	коэффициент условий эксплуатации
Коэффициенты для интегральных микросхем	
Кс.т	коэффициент условий эксплуатации

Условное обозначение коэффициента	Физический смысл коэффициента
Kv	коэффициент величины напряжения питания
Ккорп	коэффициент типа корпуса ИС
Коэффициенты для полупроводниковых приборов	
Кф	коэффициент функционального назначения
Кд.н	коэффициент допустимый нагрузки рассеивающей мощности
Ks	коэффициент отношения номинального напряжения в цепи к допустимому
K_F	коэффициент частоты
Кк	коэффициент качества
Коэффициенты для конденсаторов	
K_C	коэффициент емкостного номинала
Кп.с	коэффициент сопротивления соединенного последовательного резистора
Коэффициенты для резисторов	
K_R	коэффициент номинала сопротивления
Км	коэффициент номинальной мощности резистора
Ks	коэффициент отношения номинального напряжения в цепи к допустимому
Ксл	коэффициент комплексности сборки, зависящий от количества элементов в сборке
Кстаб	коэффициент допуска резистор
Ккорп	коэффициент материала корпуса
Коэффициенты для коммутационных изделий	
Кк.к	коэффициент коммутируемых контактов
Kf	коэффициент частоты коммутаций
Коэффициенты для соединителей	
Кк.к	коэффициент использующихся контактов
Кк.с	коэффициент частоты подключений и отключений в ходе эксплуатации
Коэффициенты для электрических кабелей и проводов	
Kt	коэффициент окружающей среды
L	коэффициент длины провода

Значения базовой интенсивности отказов рассчитываются с учетом всех видов отказов; в разделах справочника приведено их суммарное количество для групп (подгрупп, типов) ЭРИ. Для расчета значений $\lambda_э$ следует учитывать отдельные виды отказов. Распределение представлено в том же справочнике в виде процентного соотношения от общего параметра интенсивности отказа. Типовыми видами отказа для ЭРИ являются обрыв, пробой и короткое замыкание. Для сложных ЭРИ виды отказов определяются исходя из функционала.

Надежность механических компонентов в отечественной литературе освещена достаточно слабо. Бытует мнение, что надежность механических компонентов вообще можно не учитывать при расчете надежности систем. Однако, показано, что ненадежность механических компонентов вносит до 20% отказов [36]. Особенно это касается сложных современных систем управления, где большую долю составляют электромеханических и гидравлических исполнительных устройств. Универсальных методик, как в случае с ЭРИ, для прогнозирования надежности не существует. Известен и широко применим справочник NPRD-2016 [37], однако он не содержит чертежей или иных способов идентифицировать принадлежность конкретного типономинала тому или иному компоненту из справочника. Взаимен него может использоваться (но на практике редко встречается) справочник NSWC-11 [38], который позволяет рассчитывать интенсивности отказов таких механических компонентов, как уплотнения и прокладки, пружины, соленоиды, клапаны, подшипники, шестерни, насосы, втулки, валы.

Выводы по главе 3

1. Разработан стенд имитационного моделирования для оценки последствий возникновения видов отказов при различных методах кворум-контроля. Стенд включает в себя как физические имитаторы органов управления (БРУС, ППУ, БРУД, который включает в себя также элементы управления воздушными тормозами и механизацией крыла).

2. Проведено 288 испытаний в различных конфигурациях самолета (положение механизации крыла, масса, скорость, центровка) в автоматическом и ручном режиме управления. Результаты испытаний по качественной оценке подтверждают, что комбинированный метод показывает лучшие результаты, степень опасности возникающих ситуаций не превышает «УУП», в то время как методы выбора медианного значения и метод контроля по предыстории приводят к ситуациям «КС».

3. Определено алгоритмическое обеспечения выполнения анализа дерева отказов: разработка детерминированного конечного автомата в виде диаграмм состояний для реализации логики деградации системы; определен подход к миграции данной модели в инструмент по расчету показателей надежности; определена потребная количественная характеристика, которая будет рассчитываться в ходе количественного анализа дерева отказов.

4. Определены математические модели и источники данных для расчета надежности электронных и механических компонентов в интересах анализа видов и последствий отказов.

ГЛАВА 4. МОДЕЛЬНО-ОРИЕНТИВАРОННАЯ ОЦЕНКА БЕЗОПАСНОСТИ КОМБИНИРОВАННОГО МЕТОДА КВОРУМ-КОНТРОЛЯ

4.1 Роль безопасности в процессе разработки систем воздушного судна

Сертификации воздушных судов – формализованный процесс демонстрации соответствия разрабатываемого изделия заданным требованиям, обеспечивающим безопасность и корректное функционирование в ожидаемых условиях эксплуатации. Ключевым источником требований являются Авиационные правила, часть 25 (АП-25).

АП-25 состоит из следующих разделов:

- Раздел A посвящен различным характеристикам самолета;
- Раздел B включает в себя требования, характеризующие способность воздушного судна выполнять полет;
- Раздел C включает в себя общие требования к прочности конструктивных единиц;
- Раздел D включает в себя требования к ключевым функциональным системам воздушного судна;
- Раздел E включает в себя требования к силовой установке;
- Раздел F включает в себя требования к авиационному оборудованию;
- Раздел G включает в себя требования, которые должны быть учтены при разработке эксплуатационной документации.

Основные требования по безопасности, относящиеся к системам воздушных судов, представлены в разделе A-0 и пункте 25.1309 раздела F АП-25. При этом раздел A-0 не представлен в требованиях зарубежных Авиационных правил (FAR-25 и CS-25). Данный раздел повторяет редакцию главы 2 НЛГС-3 (разработанных в 1977-1980 гг. в СССР), для которого группой авторов под руководством начальника сектора лаборатории 28 Летно-исследовательского института им. М. М. Громова Министерства авиационной промышленности Чуркина С. Н. (Великанов С. П., Павлов М. М., Бычкова Н. А. Винник А. М. и др.) при активном участии Круглова А.

Г. (Госавиарегистр СССР) и Михеева А. А. (ГосНИИ ГА) были разработаны Методы определения соответствия к Главе 2 указанных Норм (МОС2).

Раздел А-0 АП-25 позволяет однозначно идентифицировать требования, обеспечивающие указание в эксплуатационной документации рекомендаций экипажу, позволяющих безопасно продолжить и завершить полет в случае возникновения отказных состояний, не отнесенных к категории практически невероятных, а также включить требования по методам верификации (летные, наземные, стендовые испытания, моделирование, расчеты и т.д.) в различных ожидаемых условиях эксплуатации.

Основные требования по отказобезопасности содержатся в Разделе А-0 и в пункте 25.1309 Раздела F АП-25. Требования во многом идентичны и дополняют друг друга [39]. При этом отдельные требования АП-25 также имеют большое значение для используемых методов оценки и анализа отказобезопасности. К таким пунктам, например, можно отнести специализированный пункт АП-25.671, относящийся к отказам непосредственно систем управления ВС.

Опыт разработки современных отечественных гражданских воздушных судов предусматривает выполнение мероприятий как по МОС-2 в обеспечение пунктов А-0, так и по Р-4761 в обеспечение пункта 25.1309. Подходы к демонстрации соответствию требования безопасности в данных стандартах дополняют друг друга, т.к. сосредотачиваются на различных аспектах. Следуя руководству Р-4761, возможно корректно сформулировать требования безопасности, а выполняя мероприятия по МОС-2 – корректно продемонстрировать соответствие этим требованиям.

АП-25 основаны на принципах обеспечения отказобезопасной конструкции, которые учитывают вероятности и последствия отказов и их комбинаций. В отношении отказов установлены следующие основные цели:

- Допускается наличие любого единичного отказа в ходе любого полета, если отказ не приводит к катастрофическим последствиям;

- Допускается возникновение следующих за первым отказов (как скрытых, так и явных) в том же полете при условии, что такая комбинация отказов является практически невероятной.

Эти цели в требованиях АП-25 превращаются в требования к вероятности возникновения отказных состояний разного уровня тяжести последствий:

- *Без влияния на безопасность.* Такие отказы не ведут к неблагоприятным последствиям на функциональные возможности самолета, не влияют на загруженность экипажа и не ощущаются пассажирами воздушного судна;
- *Усложнение условий полета.* Такие отказы без приложения особых усилий парируются экипажем, не оказывают существенного влияния на статические и динамические характеристики самолета, не приводят к существенному дискомфорту пассажиров. В эту же категорию могут быть отнесены отказы, приводящие к необходимости внесения корректировок в запланированный маршрут полета, снижающие запасы безопасности, прочности или надежности оборудования;
- *Сложные ситуации*. Такие отказы могут быть парированы экипажем, однако требуют повышенного внимания, концентрации и демонстрации повышенных навыков пилотирования. Получение пассажирами незначительных травм также относится к данной категории. Запасы безопасности, прочности и надежности оборудования значительно снижаются;
- *Аварийные ситуации.* Такие отказы требуют от летного состава демонстрации исключительных навыков пилотирования. Ожидается, что основные задачи управления полетом не смогут быть решены полно и точно. Конструкция самолета теряет запасы безопасности, прочности и надежности. Предполагается, что возможны серьезные травмы пассажиров.
- *Катастрофические ситуации.* Наиболее серьезные последствия отказов, характеризующиеся невозможность экипажем предотвратить гибель

людей. Чаще всего связано с разрушением конструкции самолета и многочисленными жертвами.

В зависимости от классификации по степени опасности, определяются следующие вероятностные термины:

- Вероятные отказы – отказные состояния, которые могут возникнуть в процессе эксплуатации самолета более одного раза.
- Маловероятные отказы – отказные состояния, которые на отдельно взятом самолете во время эксплуатации могут не проявиться, но при анализе данных эксплуатируемого парка воздушных судов данного типа могут встречаться.
- Крайне маловероятные отказы – отказные состояния, которые на отдельно взятом самолете во время эксплуатации могут не проявиться, но при анализе данных эксплуатируемого парка воздушных судов данного типа могут встречаться несколько раз.
- Практически невероятные отказы – отказные состояния, которые не ожидаются в ходе эксплуатации всех самолетов данного типа в ходе всего жизненного цикла эксплуатации.

Вероятностным характеристикам, используемым в требованиях АП-25, установлены конкретные допустимые диапазоны количественных значений, которые учитываются в ходе проектирования:

- Вероятные отказные состояния – отказные состояния, средняя вероятность возникновения которых превышает величину 10^{-5} на час полета: $P_{ср}(t=1ч) \geq 10^{-5}$;
- Маловероятные отказные состояния – отказные состояния, средняя вероятность возникновения которых превышает величину порядка 1 х 10^{-5} или менее, однако превышает величину порядка 1 х 10^{-7} на час полета.: $10^{-7} \leq P_{ср}(t=1ч) < 10^{-5}$;
- Крайне маловероятные отказные состояния – отказные состояния, средняя вероятность возникновения которых порядка 1 х 10^{-7} или менее,

однако превышает величину порядка 1 х 10^{-9} на час полета: $10^{-7} \le P_{ср}(t = 1ч) < 10^{-9}$.

- Крайне (практически) невероятные отказные состояния – отказные состояния, средняя вероятность возникновения которых составляет величину порядка 1х 10^{-9} или менее на час полета: $P_{ср}(t = 1ч) < 10^{-9}$.

Таким образом обеспечивается взаимосвязь между степенью опасности и соответствующим количественным требованием вероятности отказного состояния. Эта информация указана в таблице 8.

Таблица 8. Требование к минимально допустимой вероятности возникновения отказных состояний различной классификации по степени опасности

Степень опасности отказного состояния	**Соответствующее требование вероятности, на 1 час полета**
Нет влияния на безопасность (БС)	Требования по безопасности не предъявляются
Усложнение условий полета (УУП)	$P_{ср}(t = 1ч) < 10^{-3}$
Сложная ситуация (СС)	$P_{ср}(t = 1ч) < 10^{-5}$
Аварийная ситуация (АС)	$P_{ср}(t = 1ч) < 10^{-7}$
Катастрофическая ситуация (КС)	$P_{ср}(t = 1ч) < 10^{-9}$

Для достижения указанных целей и требований безопасности обычно применяют комбинации нескольких методов проектирования отказобезопасной конструкции. К таким методам можно отнести резервирование, сигнализацию и индикацию, рекомендации экипажу по парированию, запасы безопасности в прочности узлов и др.

При этом для современных сложных систем исключительно методы отказобезопасной конструкции не применимы, в том числе в связи со сложностью анализа и доказательства причин и последствий отказов. Для таких сложных систем дополнительно применяются методы гарантии разработки, в которых используется сочетание критериев обеспечения гарантии процесса разработки и критериев полноты верификации, а также специализированные методы анализа безопасности. Полнота методов, использование которых принимаются авиационными властями в

качестве демонстрации соответствия требованиям пункта АП-25.1309 представлены в стандартах Р-4754А и Р-4761, описывающих процессы разработки и оценки безопасности воздушных судов. Системное следование нормам указанных стандартов и выполнению мероприятий процесса оценки безопасности является необходимым условием для удовлетворения требованиям АП-25.

Процесс оценки безопасности включает в себя формирование, валидацию и верификацию требований по безопасности. Процесс оценки безопасности проходит на протяжении всего жизненного цикла разработки нового типа ВС и включает в себя качественные и количественные методы оценки функций самолета и выполняющих их систем для определения того, что соответствующие опасности точно установлены и выполнены мероприятия, минимизирующие риски.

Процесс проектирования является итеративным. Соответственно, процесс оценки безопасности также является итеративным, т.к. должен отслеживать любые изменения в концепции и реализации проекта. Старт процесса оценки безопасности осуществляется на этапе эскизного проекта (планируются работы определенным в стандарте Р-4754А формальным образом) и формируются требования по безопасности). В ходе более детальной проработки требования безопасности также должны быть уточнены. Обновленные требования безопасности при этом также могут влиять на архитектуру разрабатываемой системы (количество резервируемого оборудования, разнородность и т.д.). Процесс оценки безопасности завершается при подтверждении в ходе верификации, что воздушное судно (или сертифицируемая система) соответствует требованиям по безопасности, определённым на старте проекта и в АП-25.

Ключевыми этапами процесса оценки безопасности являются:

- Оценка функциональных опасностей ВС / системы (этап идентификации требований к ВС / системе);
- Предварительная оценка безопасности ВС / системы (этап идентификации требований к ВС / системе);
- Оценка безопасности системы / ВС (этап верификации системы / ВС).

Каждый последующий уровень детализации процесса оценки безопасности при этом валидирует или верифицирует (в зависимости от этапа разработки) требования по безопасности на верхнем уровне за счет демонстрации возможности выполнения заданных требований или действительного выполнения данных требований.

Независимо от этапа процесса оценки безопасности (т.к. он является итеративным) выделяются следующие методы:

- Оценка функциональных опасностей;
- Анализ видов и последствий отказов;
- Анализ дерева отказов.

Подробное описание данных методов с существующими проблемами представлено в подразделах настоящей Главы.

4.2 Постановка задачи разработки методики модельно-ориентированного подхода к оценке безопасности и анализу надежности

Современные подходы к выполнению различных анализов безопасности (оценка функциональных опасностей, анализ дерева отказов, анализ видов и последствий отказов) известны в инженерной практике и описаны как в нормативной документации (ARP/P-4761), так и во множестве научных трудов (например, в работах отечественных авторов [40 – 45] и зарубежных авторов [46 – 52]).

По результатам анализа выполняемых мероприятий в ходе процесса оценки безопасности, ключевыми проблемами является человеческий фактор, приводящий к финансовым задержкам и срыву сроков работ, а в худшем случае – непосредственном негативном влиянии на безопасность воздушного транспорта.

В настоящий момент широко развиты принципы модельно-ориентированного проектирования (МОП) [53 – 58]. Основная часть работ при проектировании систем с использование МОП заключается в моделировании различных физико-математических свойств системы. На сегодняшний день существует ряд языков, позволяющих осуществлять архитектурное моделирование систем, такие как UML, SysML, AADL и другие. UML предназначен для моделирования программных систем, SysML, основанный на UML, предназначен для моделирования любых систем и AADL – для моделирования технических систем [59].

Принципы МОП могут быть применены и к процессам оценки безопасности, что позволяет заранее формализовать причинно-следственные связи отказов и валидировать совместно с разработчиками системы. Сейчас научное сообщество решает частично задачи, относящиеся к модельно-ориентированному подходу к оценке безопасности (МОПОБ). Решаемые задачи можно подразделить на следующие категории:

- Расширение языка разработки и анализа архитектур AADL с помощью модели погрешностей [60];
- Внедрение данных по надежности в модели MATLAB с последующей генерацией деревьев [61];
- Использование моделей SysML при создании анализа дерева отказов [62];
- Разработка новых языков моделирования характеристик безопасности, так или иначе основанных на имеющихся языках моделирования систем SysML и AADL [63 – 64].

Нотация SysML широко применяется для высокоуровневого моделирования систем и поддерживает различные виды представления поведения систем, такие как: диаграммы состояний, последовательностей, требований и параметрические. С помощью него можно смоделировать такие параметры, как «функция», «интерфейс» и другие, характеризующие систему. Также его использование позволяет моделировать характеристики безопасности, например «DAL».

Несмотря на наличие проработки части вопросов, связанных с МОПОБ, существует ряд нерешенных проблем:

1. Текущие стандарты, требующие выполнение мероприятий процесса оценки безопасности, не требуют использования МОПОБ;
2. Отдельно взятые работы решают отдельные частные задачи и не связаны между собой методологически, что ведет к усложнению и нагромождению различных частных решений, не всегда отвечающих производственным задачам.
3. Отдельно взятые работы решают частные задачи и не связаны с собой инструментально, что ведет к усложнению освоения конечными

пользователями разработанных методов, а также росту количества инструментов, которые должны быть закуплены и квалифицированы разработчиком систем.

Указанные проблемы могут препятствовать процессу внедрения МОПОБ на большинстве отечественных предприятий, связанных с разработкой авиационной техники. Решение этих проблем должно быть представлено в виде разработки единой методологической и инструментальной системной методики выполнения мероприятий процесса оценки безопасности.

В настоящей Главе рассматриваются ключевые проблемы отдельно взятых мероприятий в классическом походе к процессу оценки безопасности, предлагаются частные (детализированные) методики выполнения такие, что могут быть интегрированы в общую идеологически и инструментально системную методику процесса оценки безопасности. Системная методика процесса оценки безопасности является ключевой и завершающей частью настоящей Главы.

4.3 Современный подход к выполнению оценки функциональных опасностей

Целью Оценки функциональных опасностей (ОФО/FHA) является анализ каждой функции на рассматриваемом уровне, в ходе которого должны быть выявлены и классифицированы отказные состояния вследствие как потери, так и неправильного выполнения этих функций. ОФО анализирует отказные состояния для каждого этапа полета, т.к. проявление одного и того же отказа может иметь различную классификацию в зависимости от этапа полета, на котором данный отказ произойдет. В результате ОФО идентифицируются требования безопасности. Эти требования могут выражаться в виде ограничений на проектирование, необходимости сигнализации об отказных состояниях, рекомендуемых действий летному экипажу или техническому персоналу и т.д.

ОФО является первым шагом процесса оценки безопасности, который выполняется при создании новых самолетов.

Процесс ОФО выполняется для определения отказных состояний и оценки их последствий, при этом не учитываются технические реализации.

Оценка выполняется в следующем порядке:

a. определяются все функции, относящиеся к рассматриваемому объекту (собственные и интерфейсные функции ВС или рассматриваемой системы);
b. определяются отказные состояния данных функций с учетом различных внешних условий (конфигураций самолета и ожидаемых условий эксплуатации); примерами таких внешних условий могут служить вынужденная посадка, отказ двигателя, потеря связи, разгерметизация, потеря гидросистемы и т.д.
c. определяются последствия данных отказных состояний;
d. классифицируются по степени опасности отказные состояния в соответствии с последствиями для самолета, экипажа и пассажиров;
e. назначаются требования к отказным состояниям;
f. определяются методы валидации классификации по степени опасности отказных состояний;
g. определяются методы верификации соответствия требованиям к отказным состояниям.

Одним из основных результатов выполнения ОФО является определения Уровня гарантии разработки функции (FDAL), который напрямую зависит от наихудшей степени опасности функции, как представлено в таблице 9.

Таблица 9. Требование к уровням гарантии разработки функций различной классификации по степени опасности

Наихудшая степень опасности функции	**Соответствующий уровень FDAL**
БС	E
УУП	D
СС	C
АС	B
КС	A

Уровень гарантии разработки функций ВС/системы напрямую влияет на множество характеристик, включая сроки и итоговую стоимость разработки, т.к.

определяет требования к независимости, разнородности и в целом «строгости» разработки данной функции.

Соответственно, некорректное определение степени опасности может повлечь за собой две ситуации:

- система удовлетворяет требованиям безопасности, но необоснованно дорого в разработке;
- система не удовлетворяет требованиям безопасности (что влечет за собой необходимость изменений в конструкции, возможно, на поздних этапах работки).

Валидация степени опасности ОФО предназначена для избегания указанных проблем на поздних этапах. Однако, часто мероприятия валидации представляют собой стендовые испытания на стендах типа «железная птица» или «электронная птица», что заставляет ожидать реализации комплекса бортового оборудования.

Таким образом, одной из основных проблем выполнения ОФО на текущий момент является срок выполнения валидации степени опасности [65].

4.4 Разработка методики модельно-ориентированного подхода к выполнению оценки функциональных опасностей

4.4.1 Цели и проблематика выполнения Оценки функциональных опасностей

Ранее было определено, что ОФО является первым шагом в работах по оценке безопасности систем и напрямую влияет на проектирование, безопасность и конечную стоимость проекта. Применение методов модельно-ориентированного проектирования позволяет сократить время на обнаружение и устранение погрешностей в алгоритмах и программном обеспечении. Достаточный уровень детализации моделей позволяет адекватно оценить влияние последствий функциональных отказов на динамику самолета с пилотом в контуре.

Целью проведения ОФО является четкое определение каждого отказного состояния наряду с обоснованием их классификации по степени тяжести. Основной проблемой обеспечения цели ОФО является отсутствие регламентированных нормативной документацией методик и принятых процессов валидации классификации по степени тяжести каждого отказного состояния. Актуальность

данной проблемы заключается в том, что материалы валидации должны быть подготовлены по требованию сертифицирующего органа при сертификации.

В ходе ОФО определяются требования к системам. Эти требования заключаются, как правило, в уровне гарантии разработки (УГР/DAL) для функций (FDAL), которые затем с использованием анализа дерева отказов (АДО/FTA) уточняются для компонентов система (IDAL), а также допустимой вероятности возникновения данных отказных состояний. Для критических уровней DAL (A и B) исходят требования по обязательной независимости проектирования, валидации, верификации и технических решений, не предполагающих возможность отказов по единой причине. Исходя из этого следует, что неверно заданный уровень степени опасности в ходе ОФО может повлечь за собой неверные решения относительно всего процесса разработки

- система будет удовлетворять требуемому уровню безопасности, но исчерпывающе, что приведет к удорожанию проекта и увеличению сроков выполнения;
- система не будет удовлетворять требованиям по безопасности. В случае выявления, потребуется переработка на более поздних стадиях работы. В случае не выявления – возможны критические последствия, вплоть до авиационных происшествий с человеческими жертвами.

Зачастую суждение о последствиях степени опасности выполняется путем экспертной оценки, что может привести к неверному определению степени опасности отказа. В рамках данной задачи предлагается использование МОПОБ для целей валидации критичности последствий, определенных в ОФО. Предполагается, что специалист, выполняющий оценку, сможет провести упрощенное имитационное моделирование на реальных моделях с имитаторами органов управления в кабине экипажа. При этом преследуется задача возможности специалистом самостоятельно примерить на себя роль «пилота» при моделировании в режиме реального времени для определения устойчивости и управляемости самолета в случае возникновения отказного состояния. Применение такого подхода позволит использовать даже не высококвалифицированных специалистов, которые обладают навыками

моделирования и имеют представление о динамике полета, принципах и алгоритмах работы разрабатываемой системы.

4.4.2 Методика модельно-ориентированного подхода к Оценке функциональных опасностей

Разработанная методика выполнения ОФО представлена в виде алгоритма на рисунке 39.

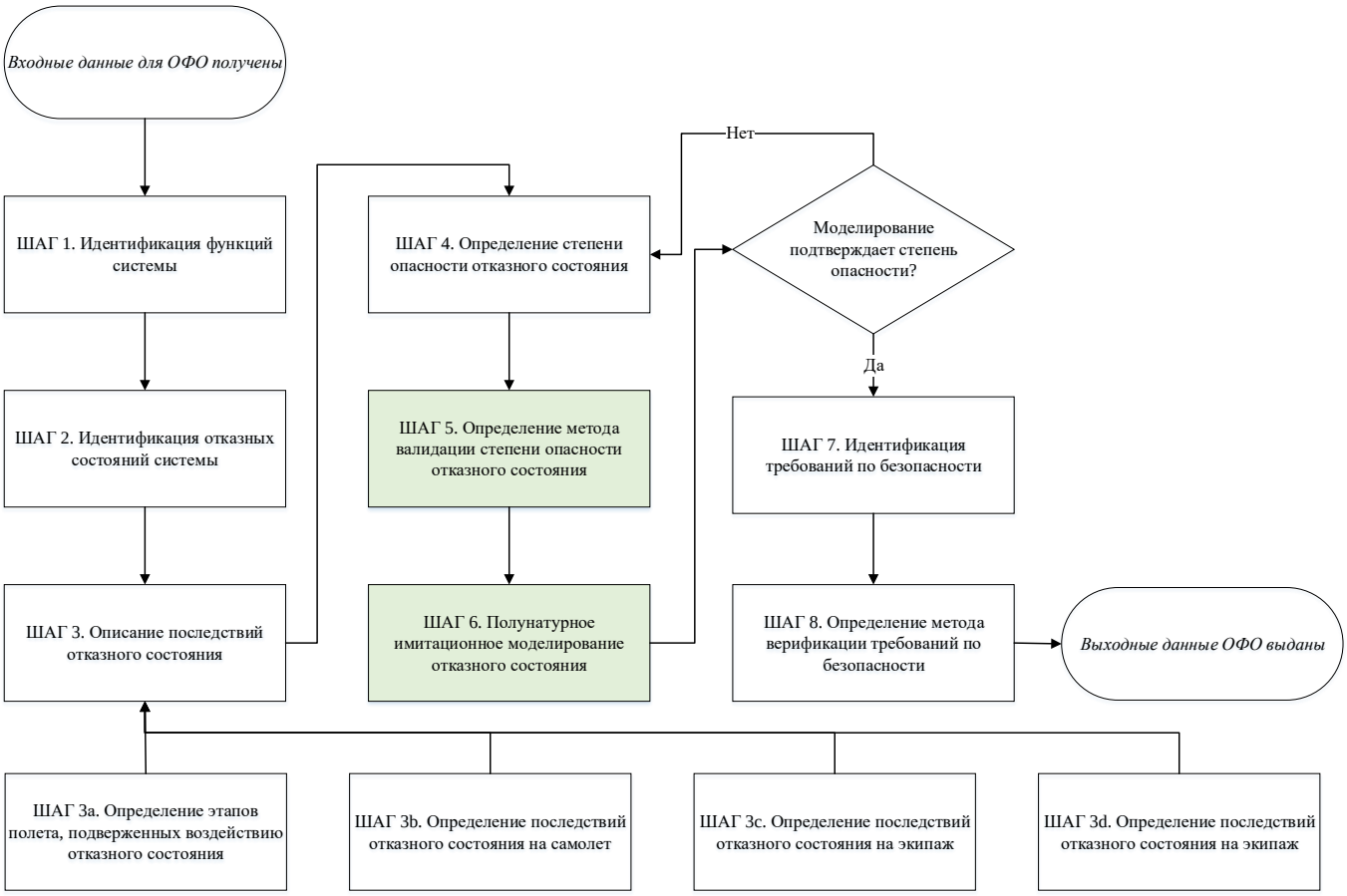

Рисунок 39. Алгоритм модельно-ориентированного подхода к ОФО

Входными данными для выполнения ОФО являются:

- Функции разрабатываемой системы;
- Результаты ОФО/ПОБ на вышестоящем уровне иерархии;

ШАГ 1. Идентификация функций

В ходе выполнения данного шага должны быть выбраны все функции, относящиеся к рассматриваемой системе, как внутренние, так и функции интерфейсов с внешним сопрягаемым оборудованием.

ШАГ 2. Идентификация отказных состояний системы

Все возможные отказные состояния функции системы определяются в соответствии с алгоритмом, представленном на Рисунке 40.

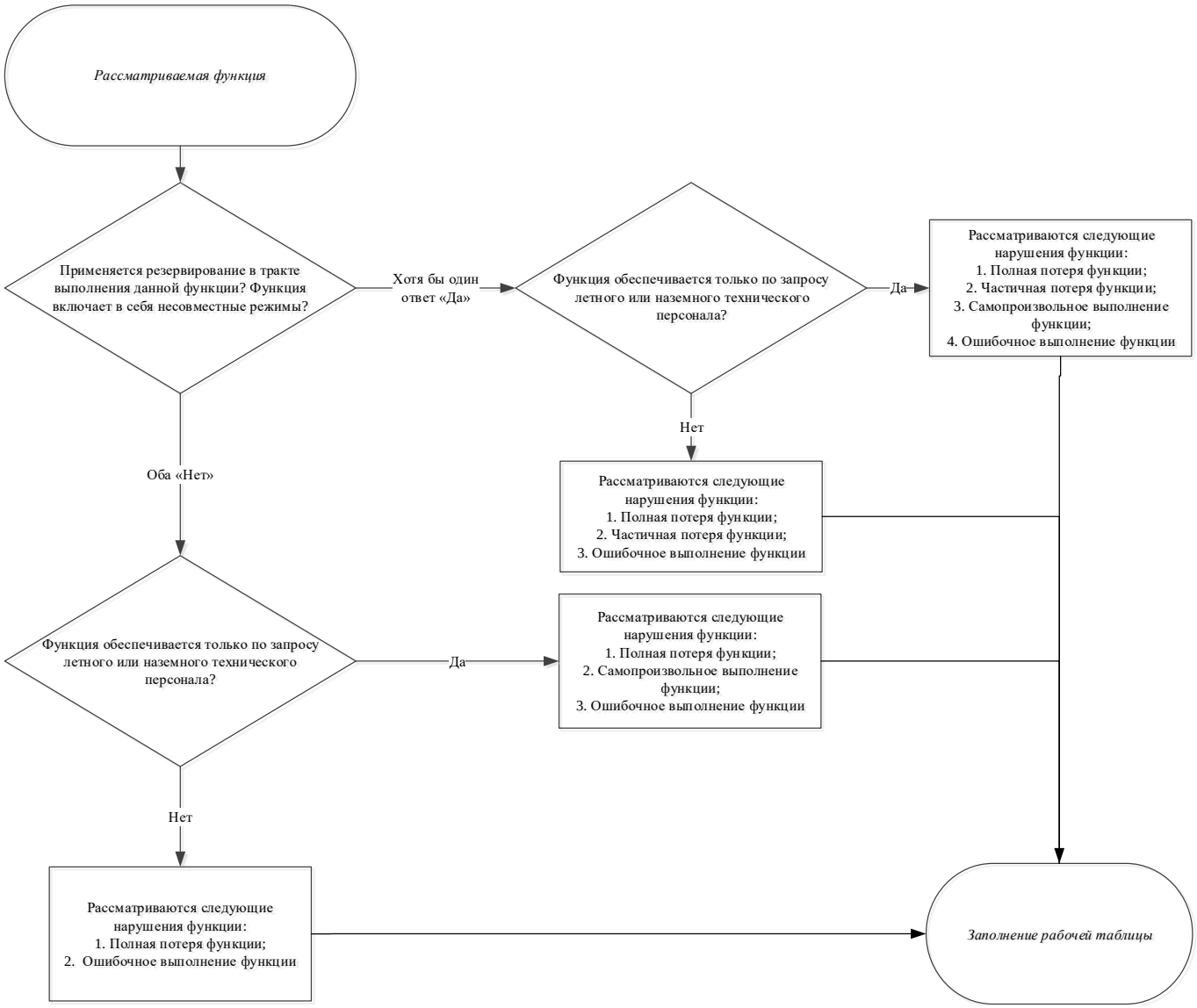

Рисунок 40. Алгоритм определения отказных состояний

ШАГ 3. Описание последствий отказного состояния

Шаг 3а. Определение этапов полета, подверженных воздействию отказного состояния

Отказные состояния, идентифицированные на предыдущем шаге, могут по-разному проявляться на различных этапах полета. Для каждого отказного состояния требуется определить для каждого из типовых этапов полета: взлет, набор высоты, крейсерский полет, снижение, заход на посадку, посадка, уход на второй круг, выруливание, заруливание.

Шаг 3b. Определение последствий отказного состояния на самолет

Последствия отказного состояния на самолет определяются исходя из влияния на характеристики устойчивости, управляемости и прочности. В соответствии с РЦ-АП-25.1309 требуется указать следующее:

- Управляемость самолета: сохраняется или ухудшается *(до какой степени?);*
- Устойчивость самолета: сохраняется или ухудшается *(до какой степени?);*
- Герметичность самолета: сохраняется или ухудшается *(до какой степени?);*
- Прочность конструкции самолета: сохраняется или ухудшается *(до какой степени?).*

Шаг 3c. Определение последствий отказного состояния на летный экипаж

Последствия отказного состояния на экипаж определяются исходя из влияния на работоспособность экипажа. В соответствии с РЦ-АП-25.1309 требуется указать следующее:

- Способ обнаружения отказного состояния экипажем;
- Предпринимаемые действия по парированию отказного состояния;
- Изменение рабочей нагрузки на экипаж: отсутствует, незначительно увеличивается, значительно увеличивается, возрастает до такой степени, что нельзя ожидать полное и корректное выполнение требуемых процедур.

Шаг 3d. Определение последствий отказного состояния на пассажиров

Последствия отказного состояния на пассажиров определяются исходя из влияния на комфорт и самочувствие пассажиров. В соответствии с РЦ-АП-25.1309 требуется указать изменение самочувствия пассажиров: неудобство, физический дискомфорт, травмы, серьезные травмы, многочисленные жертвы.

ШАГ 4. Определение степени опасности отказного состояния

На каждом этапе полета определяется степень опасности отказного состояния исходя из условий, определенных в РЦ-АП-25.1309 и представленной в таблице 10.

Таблица 10. Условия выбора степени опасности

Условие	**Степень опасности**
Фатальные последствия для конструкции, экипажа или пассажиров предотвратить практически невозможно	КС
Выход на предельные характеристики конструкции самолета или невозможность летного экипажа выполнить задачи полно и точно	АС
Выход за эксплуатационные (но не предельные) ограничения отдельных характеристик самолета или снижение эффективности действий экипажа	СС
Пилотирование в незначительно ухудшающихся условиях с небольшим увеличением рабочей нагрузки на экипаж по сравнению со штатным полетом	УУП
Полет осуществляется в штатном режиме	БС

ШАГ 5. Определение метода валидации степени опасности отказного состояния

Предполагается, что валидация степени опасности требуется для отказных состояний, которые не классифицированы как КС. Для всех остальных отказных состояний должен применяться метод имитационного полунатурного математического моделирования.

ШАГ 6. Полунатурное имитационное моделирование отказного состояния

Выполнение полунатурного имитационного моделирования может заключаться в неформальном (для первичной оценки) и формальной проведении

испытаний с целью подтверждения описанных в ОФО последствий. Каждый отказ, не отнесенный к категории КС, должен быть промоделирован. Для некоторых типов отказов могут быть предусмотрены различные способы его проявления. В таком случае выбираются наихудшие условия.

Моделирование включает в себя разработку модели отказа в среде MATLAB Simulink (на базе уже имеющейся системной модели), непосредственное моделирование в режиме реального времени и анализ результатов по соответствию критериям отказных ситуаций, определенных в МОС-2. Основные положения, необходимые для методических указаний представлены ниже.

В методике используются стандартные обозначения:

kt – knot (узел).

ft – foot (фут).

$A_{т\ пред}$ – предельная энергонагруженность тормозов колес шасси.

$A_{т\ эксп}$ –максимальная эксплуатационная энергонагруженность тормозов колес шасси.

V_1– минимальная скорость при взлете, на которой пилот должен принять первое действие (применить тормоза, уменьшить тягу, отклонить тормозные щитки) для остановки самолета в пределах дистанции прерванного взлета. Это также минимальная скорость на взлете, на которой пилот может продолжить взлет после отказа критического двигателя и достичь требуемой высоты над поверхностью взлета в пределах потребной дистанции взлета.

V_{LOF} ($V_{отр}$) – скорость отрыва на взлете.

V_{MU} ($V_{min\ отр}$) – минимальная скорость отрыва на взлете.

V_{LS}–минимальная выбираемая эксплуатационная скорость при фактической конфигурации.

$V_{ВПП\ пред}$–предельная скорость движения по ВПП при взлете и посадке.

V_{SW}– скорость, на которой срабатывает сигнализация о приближении сваливания.

V_R–скорость в момент подъема носовой опоры шасси.

V_2 – безопасная скорость взлета.

V_{2MIN}–минимальная безопасная скорость взлета.

V_{FTO}–конечная скорость взлета или скорость самолета в конце траектории взлета при крейсерской конфигурации с одним неработающем двигателем.

V_{FE}– максимально допустимая скорость в полете при выпущенной механизации.

V_F – расчетная скорость при выпущенной механизации.

V_{SR}– нормируемая скорость сваливания.

V_{SR0} – нормируемая скорость сваливания в посадочной конфигурации.

V_{SR1} – нормируемая скорость сваливания в рассматриваемой конфигурации.

V_{MO} ($V_{max\ э}$) – максимальная скорость при эксплуатации самолета.

V_{FC} – максимальная скорость для характеристик устойчивости.

V_D – расчетная предельная скорость.

V_{REF} – скорость захода на посадку со всеми работающими двигателями.

V_{APP} – расчётная скорость на посадке согласно РЛЭ.

$V_{у\ пред}$ – предельная величина вертикальной скорости самолета в момент касания ВПП.

$V_{у\ доп}$– допустимая величина вертикальной скорости в момент касания ВПП.

$L_{кас}$–расстояние от точки касания до порога ВПП.

$L_{нач.з.п.}$–расстояние от порога ВПП до начала зоны приземления.

$L_{кон.з.п.}$– расстояние от порога ВПП до конца зоны приземления.

Зона приземления – участок ВПП за ее порогом, предназначенный для первого касания ВПП приземляющимися самолетами.

Порог ВПП – начало участка ВПП, использующийся для посадки самолетов.

$\Delta_{выр}$ – характерное для нормальной эксплуатации изменение скорости с момента начала выравнивания до момента касания ВПП.

$V_{блок.сигн.}$– скорость блокировки сигнализации.

M_{FC} – максимальное число М для характеристик устойчивости.

M_{MO} ($M_{max\ э}$) – максимальное число М при эксплуатации самолета.

M_D – расчетное предельное число М.

$H^{min}_{преп}$ – минимальная безопасная высота пролета над препятствием при наборе высоты, крейсерском полёте, снижении.

$n^{э}_{y\ min}$ – минимальная нормальная эксплуатационная перегрузка.

$n^{э}_{y\ max}$ – максимальная нормальная эксплуатационная перегрузка.

$n^{расч}_{y\ min}$ – минимальная нормальная расчётная перегрузка.

$n^{расч}_{y\ max}$ – максимальная нормальная расчётная перегрузка.

$n^{p}_{y\ max}$ – максимальная нормальная перегрузка, реализуемая в маневре при отказе.

$n^{p}_{y\ min}$ – минимальная нормальная перегрузка, реализуемая в маневре при отказе.

$n_{z\ пред}$ – предельная боковая перегрузка в момент касания ВПП.

α– угол атаки.

β – угол скольжения.

γ – угол крена.

ϑ – угол тангажа.

α_{SW} – угол атаки, при котором срабатывает сигнализация о приближении сваливания.

α_{SR1} – угол атаки, при котором начинается сваливание в рассматриваемой конфигурации.

$\gamma_{опр}$ – угол крена, при котором начинает работать ограничитель предельных режимов.

$\gamma_{опр.\ пред}$ – максимально возможное, кратковременно допустимое значение угла крена при работе ограничителя предельных режимов.

$\gamma_{кас.\ земли}$ – угол крена, при котором происходит касание крыла самолета поверхности земли или ВПП.

По ряду характеристик можно выделить следующие области значений критериев, соответствующих особым ситуациям различной степени опасности.

Изменение характеристик в пределах эксплуатационных ограничений или регламентируемых допустимых значений рассматривается как незначительное и соответствует усложнению условий полета либо отсутствию особой ситуации.

Изменение характеристик, приводящее к достижению или превышению предельных ограничений, соответствует аварийной или катастрофической ситуации.

Промежуточной области между эксплуатационными и предельными ограничениями соответствует сложная ситуация.

В настоящей методике представлены в общем виде области изменения характеристик движения самолета, соответствующее различным видам особых ситуаций. Также даны количественные значения некоторых критериев. Для каждого типа самолета соответственно могут использоваться настоящие количественные значения или определяться с учетом аэродинамических характеристик.

Таблица 11 содержит критерии оценки особых ситуаций, связанные с траекторным движением самолета.

Таблица 12 содержит критерии оценки особых ситуаций, связанные с параметрами движения самолета относительно центра масс, характеристиками устойчивости и управляемости.

Таблица 11. Критерии оценки особых ситуаций, связанные с траекторным движением самолета

Этап полета	**Определяющие характеристики**	**Особые ситуации**		
		Нормальный полет или усложнение условий полета	**Сложная ситуация**	**Аварийная ситуация / Катастрофическая ситуация**
Взлет	Дистанция прерванного взлета, $L_{пр.\ взл.}$	$L_{пр.\ взл.} \leq$ РДПВ-15%	РДПВ-15%$< L_{пр.\ взл.} \leq$ РДПВ	$L_{пр.\ взл.} >$ РДПВ
	Дистанция разбега, $L_р$	$L_р \leq$ РДР-200м	РДР-200м$< L_р \leq$ РДР	$L_р >$ РДР
	Дистанция взлета, $L_{взл}$	$L_{взл.} \leq$ РДВ-200м	РДВ-200м$< L_{взл.} \leq$РДВ.	$L_{взл.} >$РДВ
	Боковой увод на ВПП, $Z_{бок}$	$Z_{бок} \leq Z_{пред} - 5м$	$Z_{пред} - 5м < Z_{бок} \leq Z_{пред}$	$Z_{бок} > Z_{пред}$
	Скорость в момент отрыва, V_{LOF}	$V_{LOF} \leq V_{ВППпред}$-10kt	$V_{ВППпред}$ -10kt$< V_{LOF} <$ $V_{ВППпред}$	$V_{LOF} <$Vmu или $V_{LOF} \geq V_{ВППпред}$
	Скорость на 1-ом, 2-ом участках взлета, V	$V_{2MIN} \leq V < V_{FE}$	$V_{SW} \leq V < V_{2MIN}$ или$V_{FE} \leq V < V_F$	$V \geq V_F$ или $V_{SR1} < V \leq V_{SW}$
	Минимальное расстояние до поверхности ограничения препятствий, Δ	Δ>35ft	0< Δ ≤35ft	Δ ≤ 0
	Энергонагруженность тормозов, $A_т$	$A_т \leq A_{т\ пред}$		$A_т > A_{т\ пред}$
	Нормальная перегрузка, n_y (по условиям прочности)	$n^э_{y\ min} \leq n_y \leq n^э_{y\ max}$	$n^{расч}_{y\ min} \leq n_y < n^э_{y\ min}$ $n^э_{y\ max} < n_y \leq n^{расч}_{y\ max}$	$n_y < n^{расч}_{y\ min}$ $n_y > n^{расч}_{y\ max}$
	Градиент на 1-ом сегменте взлёта, GRAD(V_{LOF})	GRAD(V_{LOF}) ≥ 0.8	0.8 >GRAD(V_{LOF}) > 0	GRAD(V_{LOF}) ≤ 0
	Градиент на 2-ом сегменте взлёта, GRAD(V_2)	GRAD(V_2) ≥ 2.4	2.4> GRAD(V_2) > 0	GRAD(V_2) ≤ 0
	Градиент на финальном сегменте взлёта, GRAD(V_{FTO})	GRAD(V_{FTO}) ≥ 1.2	1.2 >GRAD(V_{FTO}) > 0	GRAD(V_{FTO}) ≤ 0
Набор высоты, крейсерский полёт, снижение (в	Скорость полета, V	$V_{LS} \leq V \leq V_{MO}$	$V_{SW} < V < V_{LS}$ или $V_{MO} < V < V_{FC}$	$V_{SR1} < V < V_{SW}$ или $V_{FC} \leq V \leq V_D$
	Число М полета	$M \leq M_{MO}$	$M_{MO} < M \leq M_{FC}$	$M > M_{FC}$

Этап полета	Определяющие характеристики	Особые ситуации		
		Нормальный полет или усложнение условий полета	**Сложная ситуация**	**Аварийная ситуация / Катастрофическая ситуация**
крейсерской конфигурации)	Располагаемая дальность полета	Обеспечивается завершение полета на аэродроме назначения	Требуется выполнение посадки на ближайшем пригодном аэродроме	Требуется выполнение немедленной посадки (независимо от наличия аэродрома)
	Возможная высота установившегося полета, $H_{пол}$	$H_{пол} \geq H^{min}_{преп}+2000ft$	$H^{min}_{преп}+2000ft < H_{пол} \leq H^{min}_{преп}$	$H_{пол} < H^{min}_{преп}$
	Нормальная перегрузка, n_y (по условиям прочности)	$n^э_{y\,min} \leq n_y \leq n^э_{y\,max}$	$n^{расч}_{y\,min} \leq n_y < n^э_{y\,min}$ $n^э_{y\,max} < n_y \leq n^{расч}_{y\,max}$	$n_y < n^{расч}_{y\,min}$ $n_y > n^{расч}_{y\,max}$
Заход на посадку	Скорость полета, V	$V_{REF} \leq V < V_{FE}$	$V_{SW} \leq V < V_{REF}$ или $V_{FE} \leq V < V_F$	$V_{SR1} < V < V_{SW}$ или $V_{FC} \leq V \leq V_D$
	Минимальное расстояние до поверхности ограничения препятствий, Δ	$\Delta > 35ft$	$0 < \Delta \leq 35ft$	$\Delta \leq 0$
	Нормальная перегрузка n_y (по условиям прочности)	$n^э_{y\,min} \leq n_y \leq n^э_{y\,max}$	$n^{расч}_{y\,min} \leq n_y < n^э_{y\,min}$ $n^э_{y\,max} < n_y \leq n^{расч}_{y\,max}$	$n_y < n^{расч}_{y\,min}$ $n_y > n^{расч}_{y\,max}$
Посадка	Посадочная дистанция, $L_{пос}$ (При отказах обнаруживаемых ниже высоты принятия решения)	$L_{пос} \leq$ РПД-15%	РПД-15% $< L_{пос} \leq$ РПД	$L_{пос} >$ РПД
	Скорость в момент касания ВПП, $V_п$	$(V_{APP}-\Delta_{выр}) < V_п < V_{APP}+10kt$	$V_{APP}+10kt \leq V_п < V_{ВПП\,пред}$ $(V_{APP}-\Delta_{выр}) > V_п > V_{SR1}$	$V_п > V_{ВПП\,пред}$ или $V_п \leq V_{SR1}$
	Вертикальная скорость при касании ВПП, $V_{укас}$	$\lvert V_{укас}\rvert \leq \lvert V_{удоп}\rvert$	$\lvert V_{удоп}\rvert < \lvert V_{укас}\rvert \leq \lvert V_{у\,пред}\rvert$	$\lvert V_{укас}\rvert > \lvert V_{у\,пред}\rvert$
	Боковая составляющая перегрузки при касании ВПП, n_z	$\lvert n_z\rvert \leq \lvert n_{z\,доп}\rvert$	$\lvert n_{z\,доп}\rvert < \lvert n_z\rvert \leq \lvert n_{z\,пред}\rvert$	$\lvert n_z\rvert > \lvert n_{z\,пред}\rvert$

Этап полета	Определяющие характеристики	Особые ситуации		
		Нормальный полет или усложнение условий полета	**Сложная ситуация**	**Аварийная ситуация / Катастрофическая ситуация**
	Боковое смещение на ВПП и боковое отклонение точки касания от оси ВПП, $L_{касс}$	$Z_{бок} \leq Z_{пред} - 5м$	$Z_{пред} - 5м < Z_{бок} \leq Z_{пред}$	$Z_{бок} > Z_{пред}$
	Расстояние от точки касания до входного торца ВПП, $L_{кас}$	$L_{нач.з.п.} \leq L_{кас} \leq L_{кон.з.п.}$	Пор. ВПП$\leq L_{кас} < L_{нач.з.п}$	$L_{кас} <$ Пор. ВПП
	Энергонагруженность тормозов, $A_т$	$A_т \leq A_{тэксп}$	$A_{тэксп} < A_т \leq A_{т\ пред}$	$A_т > A_{т\ пред}$
Уход на второй круг	Скорость полета, V	$V_2 < V < V_{FE}$	$V_{SW} < V \leq V_2$ или $V_{FE} \leq V < V_F$	$V_{SW} > V > V_{SR1}$ или $V \geq V_F$
	Нормальная перегрузка, n_y (по условиям прочности)	$n^э_{y\ min} \leq n_y \leq n^э_{y\ max}$	$n^{расч}_{y\ min} \leq n_y < n^э_{y\ min}$ $n^э_{y\ max} < n_y \leq n^{расч}_{y\ max}$	$n_y < n^{расч}_{y\ min}$ $n_y > n^{расч}_{y\ max}$
	Минимальное расстояние до поверхности ограничения препятствий при наборе высоты, Δ	Δ>35ft	0< Δ ≤35ft	Δ ≤ 0
	Градиент набора высоты, GRAD	GRAD ≥ 2.1	2.1 >GRAD> 0	GRAD ≤ 0

Таблица 12. Критерии оценки особых ситуаций, связанные с параметрами движения самолета относительно центра масс, характеристиками устойчивости и управляемости

Этап полета	Определяющие характеристики	Особые ситуации		
		Нормальный полет или усложнение условий полета	**Сложная ситуация**	**Аварийная ситуация / Катастрофическая ситуация**
Все этапы полета	Угол атаки, α	$\alpha < \alpha_{SW}$	$\alpha_{SW} < \alpha < \alpha_{SR1}$	$\alpha \geq \alpha_{SR1}$
Все этапы полета	Угол скольжения, β	$\beta < \beta_{доп}$	$\beta_{доп} \leq \beta < \beta_{пред}$	$\beta \geq \beta_{пред}$

Этап полета	Определяющие характеристики	Особые ситуации		
		Нормальный полет или усложнение условий полета	**Сложная ситуация**	**Аварийная ситуация / Катастрофическая ситуация**
Набор, крейсерский полёт, снижение, заход на посадку	Угол крена, в переходном процессе после отказа (невмешательство летчика 5сек, автоматизированный и автоматический режимы)	$\gamma \leq \gamma_{опр}(35°)$	$\gamma_{опр}(35°) < \gamma \leq \gamma_{опр.пред}$	$\gamma > \gamma_{опр\ пред}$
Взлёт, посадка, уход на 2-ой круг	Угол крена, в переходном процессе после отказа а) H> 50ft б) H> 30ft в) H = 0	$\gamma \leq \gamma_{опр}(31°)$ $\gamma \leq \gamma_{опр}(18°)$ $\gamma \leq \gamma_{опр}(4°)$	$\gamma_{опр}(31°) < \gamma < \gamma_{кас.\ земли}(45°)$ $\gamma_{опр}(18°) < \gamma < \gamma_{кас.\ земли}(30°)$ $\gamma_{опр}(4°) < \gamma < \gamma_{кас.\ земли}(12°)$	$\gamma \geq \gamma_{кас.\ земли}(45°)$ $\gamma \geq \gamma_{кас.\ земли}(30°)$ $\gamma \geq \gamma_{кас.\ земли}(12°)$

ШАГ 7. Идентификация требований по безопасности

Выделяют два типа требований по результатам ОФО: *качественные* и *количественные* требования по безопасности.

Количественные требования по безопасности должны быть сформулированы для каждого отказного состояния и заключается в допустимой не превышающей вероятности в зависимости от степени опасности в соответствии с Таблицей 8.

Качественные требования по безопасности должны быть сформулированы для каждой функции и заключаются в требуемом уровне гарантии разработки данной функции (FDAL) в зависимости от наиболее строгой степени опасности из всех отказных состояний данной функции в соответствии с Таблицей 9.

ШАГ 8. Определение метода верификации требований по безопасности

На данном этапе определяются методы, с помощью которых будут подтверждаться количественные требования по безопасности, сформированные на предыдущем шаге. Рисунок 41 содержит алгоритм определения метода верификации количественных требований по безопасности.

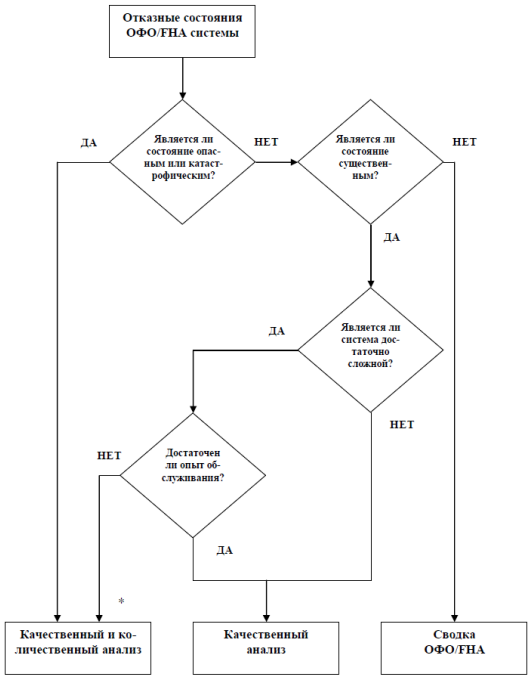

Рисунок 41. Алгоритм выбора метода верификации

Выходными данными ОФО являются:

– Перечень отказных состояний системы;
– Перечень качественных и количественных требований по безопасности;
– Методы верификации выявленных требований по безопасности.

4.5 Современный подход к анализу дерева отказов

Анализ дерева отказов (АДО/FTA) – дедуктивный анализ отказов, который сосредотачивается на одном специфическом нежелательном событии и последовательно определяет причины, которые могут привести к данному событию. Анализ начинается с опасного события уровня ОФО и систематического определения всех вероятных единичных отказов и их комбинаций всех функциональных блоков системы на последующем (более низком) уровне детализации, которые могут привести к данному событию. Анализ продолжается последовательно вглубь конструкции до обнаружения первичных (базовых, наиболее низких) событий. Первичное событие может быть, как отказом собственного компонента, так и интерфейсного оборудования. Первичными событиями могут быть как элементы аппаратного обеспечения, так и программного обеспечения, однако в количественном анализе оценивается только отказы аппаратного обеспечения (т.к. их можно прогнозировать).

АДО как правило выполняется графически и получил наименование из-за ветвей, в виде которых изображается. Такая форма позволяет достичь наглядности причин отказов как для разработчиков, так и для сертифицирующих органов.

С помощью АДО обеспечивается:

- помощь при выполнении ПОБ и ОБ специалистами по надежности и безопасности и рассмотрении сертифицирующими органами архитектуры системы;
- распределение бюджетов допустимой вероятности (формирование требований к вероятности отказов на нижестоящем уровне) на этапе ПОБ;
- расчет вероятности отказных состояний, идентифицированных в ОФО (на этапе ОБ);

- определение допустимого времени технического обслуживания скрытых отказов;

Рисунок 42 содержит упрощенный жизненный цикл АДО.

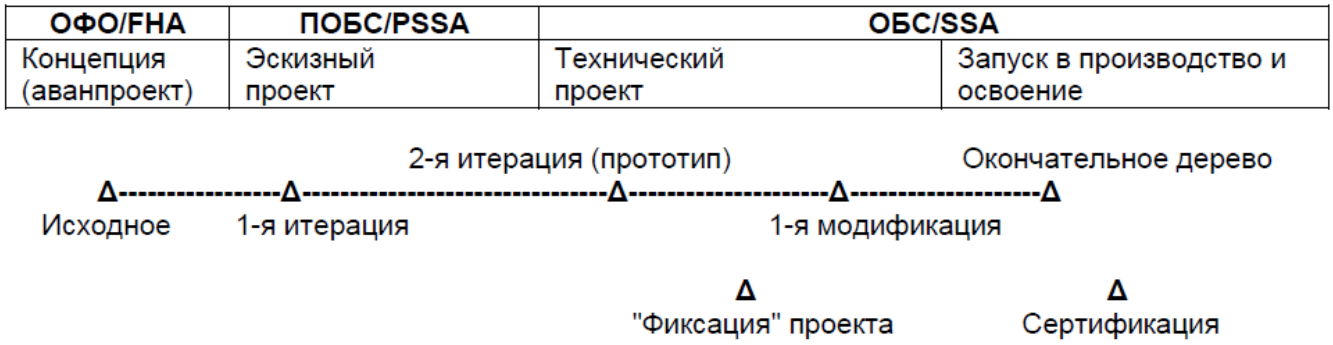

Рисунок 42. Упрощённый процесс жизненного цикла АДО

В приведенном примере:

- "Исходное" АДО выполняется как часть процесса ОФО/FHA для определения комбинации отказов системы и распределения бюджетов вероятностей по системам;
- "1-я итерация" может включать изменения дерева неисправности, обусловленные пересмотром или уточнением исходных требований к изделию. Данная стадия служит для определения требований безопасности, опираясь только на знание предполагаемой архитектуры системы. На этом этапе осуществляется распределение допустимой вероятности возникновения отказов нижестоящего уровня и требуемого уровня гарантии разработки;
- "2-я итерация (прототип)" включает изменения дерева неисправности на базе информации по результатам детальной разработки аппаратуры и/или программного обеспечения. Она проводится на этапе разработки, когда: 1) в первичные события АДО внесена информация по интенсивности отказов; 2) рассчитывается вероятность события верхнего уровня; 3) эта вероятность отказа сравнивается с соответствующим требованием из ОФО (как составная часть процесса верификации). Эта версия дерева неисправности становится частью вспомогательной документации,

необходимой для успешного завершения этапа программы, называемого "Фиксацией проекта";

- "1-я (производственная) модификация" включает изменения дерева неисправности, основанные на изменениях аппаратных средств или программного обеспечения вследствие разрешения проблем, выявленных при испытаниях прототипа;
- "Окончательное дерево" создается специалистом по надежности и безопасности с учетом всех изменений аппаратуры или программного обеспечения по результатам испытаний. Эта версия дерева входит в итоговый отчет ОБ, готовящейся для завершения этапа "Сертификация".

Деревья отказов состоят из двух типов символов: символы логики и символы событий. Логические символы демонстрируют логическую связь событий между собой согласно законам булевой алгебры. Основными логическими символами являются Булевы логические "И" и "ИЛИ". Символ "И" используется, если отказ «верхнего уровня» возникает при возникновении всех отказов «нижнего уровня», а порядок их возникновения не влияет на результат. Символ "ИЛИ" используется, когда отказное событие происходит, если истинно хотя бы одно из нескольких входных условий нижнего уровня. В ряде частных случаев также могут использовать комбинаторные символы: «K из N» и «Приоритетное И». Символ «K из N» выбирается, когда отказное событие верхнего уровня происходит, только когда K входных нижних условий из общего количества N нижних условий истинны. Символ «И с приоритетом» используется, если отказ «верхнего уровня» проявляется в случае определенного порядка возникновения отказов «нижнего уровня».

Чаще всего символы событий представляют собой прямоугольник, треугольник, круг и ромб. Событие «прямоугольник» описывает выход логического символа и является постулированием конкретного отказа, приводящего к событию верхнего уровня. Символ «треугольник» применим в больших по объему деревьях и служит для идентификации переноса информации между листами. «Круг» и «ромб» являются вариантами «базовых» события. Круг используется для «базовых» событий, являющихся внутренними для рассматриваемой системы. «Ромб» используется для

событий, которые далее не анализируются по различным причинам, как правило вызванным незначительным влиянием на событие верхнего уровня, недостатком информации на момент разработки дерева или указывающим на необходимость доработок конструкции или самого дерева.

Границами АДО (до какого уровня детализации должно быть построено дерево) определяется как правило уровнем разрабатываемого изделия. Пример границ представлен в таблице 13.

Таблица 13. Пример границ АДО

Уровень разрабатываемого изделия	**Граница АДО**	**Источник для события верхнего уровня АДО**
Воздушное судно	Блок-схема воздушного судна	ОФО функций самолета
Система	Блок-схема системы	ОФО системы, а также ОФО функций самолета, а также АДО самолета
Изделие	Функциональная блок-схема изделия	АДО системы
Функциональный компонент изделия	Схема изделия, Функциональные элементы ПО	АДО изделия

Конструирование дерева неисправности осуществляется в ходе следующих шагов:

1. Выделяется отказное состояние «верхнего» уровня, соответствующее выявленному функциональному отказу в ходе ОФО;

2. Определяются промежуточные уровни дерева отказа. Данные уровни строятся с использование булевой алгебры возникновения событий. На каждом последующем уровне определяются все возможные причины в комбинациях «ИЛИ» и «И» для выявления всех возможных причин вышестоящего уровня;

3. Промежуточные уровни углубляются через все уровни иерархии системы до тех пор, пока не будут определены все возможные причины их возникновения. Такие конечные причины далее будут называться «базовыми» событиями, они могут

быть вызваны программными сбоями, аппаратными отказами или механическими повреждениям, а также быть собственными или внешними по отношению к рассматриваемой системе;

4. Выполняется количественный анализ. На этапе ПОБ бюджетируются заданные в ОФО допустимые значения вероятности отказов до нижнего уровня (сверху-вниз), а на этапе ОБ рассчитывается вероятность возникновения функционального отказа на основе данных по интенсивности каждого отдельного вида отказа – «базового» события (на этапе ОБ).

Логический символ определяет, как будет выполняться расчет на основе следующих базовых правил вычисления вероятности:

1. Вероятность события *A* обозначается как *P(A)*;

2. Вероятность возникновения двух событий *A* и *B* одновременно обозначается как *P(AB);*

3. Вероятность возникновения одного из двух событий *A* или *B* обозначается как *P(A+B);*

4. Если два события *A* и *B* являются независимыми событиями с вероятностями *P(A)* и *P(B)* соответственно, то вероятность возникновения данных двух событий одновременно определяется значением:

$$P(AB) = P(A) \cdot P(B) \qquad (8)$$

5. Если три события *A, B* и *C* являются независимыми событиями с вероятностями *P(A), P(B)* и *P(C)* соответственно, то вероятность возникновения данных трех событий одновременно определяется значением:

$$P(ABC) = P(A) \cdot P(B) \cdot P(C) \qquad (9)$$

6. Аналогично рассматриваются четыре и более независимых событий, соединенных по схеме «И»;

7. Если два события *A* и *B* являются независимыми событиями с вероятностями *P(A)* и *P(B)* соответственно, то вероятность возникновения одного из двух событий определяется значением:

$$P(A+B) = P(A) + P(B) - [P(A) \cdot P(B)] \qquad (10)$$

8. Если три события *A, B* и *C* являются независимыми событиями с вероятностями *P(A), P(B)* и *P(C)* соответственно, то вероятность возникновения одного из трех событий определяется значением:

$$P(A+B+C) = P(A) + P(B) + P(C) - [P(A) \cdot P(B)] - [P(A) \cdot P(C)] - [P(B) \cdot P(C)] - [P(A) \cdot P(B) \cdot P(C)] \quad (11)$$

9. Аналогично рассматриваются четыре и более независимых событий, соединенных по схеме «ИЛИ»;

10. Если два события являются несовместными (исключают возможность возникновения одного из них при возникновении другого), вероятность событий, соединенных по схеме «ИЛИ» упрощается до следующего:

$$P(A+B) = P(A) + P(B), \text{ при этом } P(AB) = 0 \quad (12).$$

Расчет количественного значения вероятности отказного события верхнего уровня дерева неисправности выполняется с помощью определения сечений отказа и содержит следующие шаги:

- Определение минимальных наборов/сечений дерева неисправности;
- Определение интенсивностей базовых отказов (как правило, с помощью имеющейся на предприятия статистики изделий-аналогов или справочных материалов);
- Определение времени воздействия отказа (для скрытых отказов – период технического обслуживания, позволяющего определить данный отказ);
- Непосредственное выполнение математических расчетов вероятности возникновения отказа верхнего уровня.

При расчетах чаще всего принимается экспоненциальный закон распределения отказов, и, соответственно, вероятность возникновения каждого первичного события принимает вид:

$$P(t) = 1 - e^{-\lambda t}, \text{ где}$$

P(t) – искомая вероятность первичного события в момент времени *t*;

λ – интенсивность отказа (первичного события), определяемая с помощью справочных материалов;

t – интервал времени воздействия отказа.

Вероятность события верхнего уровня определяются с помощью вышеуказанных формул для схем «И», независимых «ИЛИ» событий и несовместных «ИЛИ» событий [66].

Расчетная вероятность возникновения отказных состояний напрямую влияет на процесс сертификации и безопасность полета. При этом велик риск «человеческого фактора» в ходе выполнения АДО, т.к. специалист по надежности и безопасности может ошибиться в ходе выполнения АДО, некорректно указав причины возникновения того или иного отказа. В худшем случае это может привести к тому, что фактически непреходящая по вероятности отказа система будет реализована и пущена в эксплуатацию. Таким образом, одной из основных проблем выполнения АДО на текущий момент является высокий риск человеческой ош ибки в следствие отсутствия достаточной коммуникации между специалистами-разработчиками систем и специалистами, выполняющими АДО.

4.6 Разработка методики модельно-ориентированного подхода к выполнению анализа дерева отказов

4.6.1 Цели и проблематика выполнения Анализа дерева отказов

Ранее было определено, что Анализ дерева отказов – дедуктивный анализ отказов, который сосредотачивается на одном отказном состоянии и является методом определения причин этого состояния. Сложные интегрированные системы, используемые в современных самолетах, а также регулярное обновление алгоритмов их работы и контроля, могут приводить к обесцениванию труда специалиста по надежности и безопасности, вынужденного проводить анализ для потенциально неверных алгоритмов работы системы.

Расчеты, выполняемые в ходе АДО, являются одним из самых распространённых способов как (1) бюджетирования требования с уровня системы на уровень компонентов (на этапе PSSA), так и (2) верификации заданных в ОФО требования (на этапе SSA). Ошибки, допущенные на данном этапе влияют как на задачу требований к комплектующим изделиям, так и приводят к некорректным расчетам итоговой вероятности возникновения отказного состояния.

Во избежание такой проблемы встает задача по интеграции вопросов разработки и оценки безопасности в единую среду. Данная задача решается также с использованием инструментов МОПОБ, а именно интеграцией инструментов по разработке и оценке безопасности (например, MATLAB Simulink и ANSYS medini analyze, которые рассматриваются в настоящей методике). Реализованная логика переходов между состояниями системы позволит автоматизировать процесс выполнения АДО. Такой подход позволит обеспечить перекрёстный контроль результатов работ специалиста по безопасности и специалиста по системной разработке.

4.6.2 Методика модельно-ориентированного подхода к Анализу дерева отказов

Разработанная методика выполнения АДО представлена в виде алгоритма на рисунке 43.

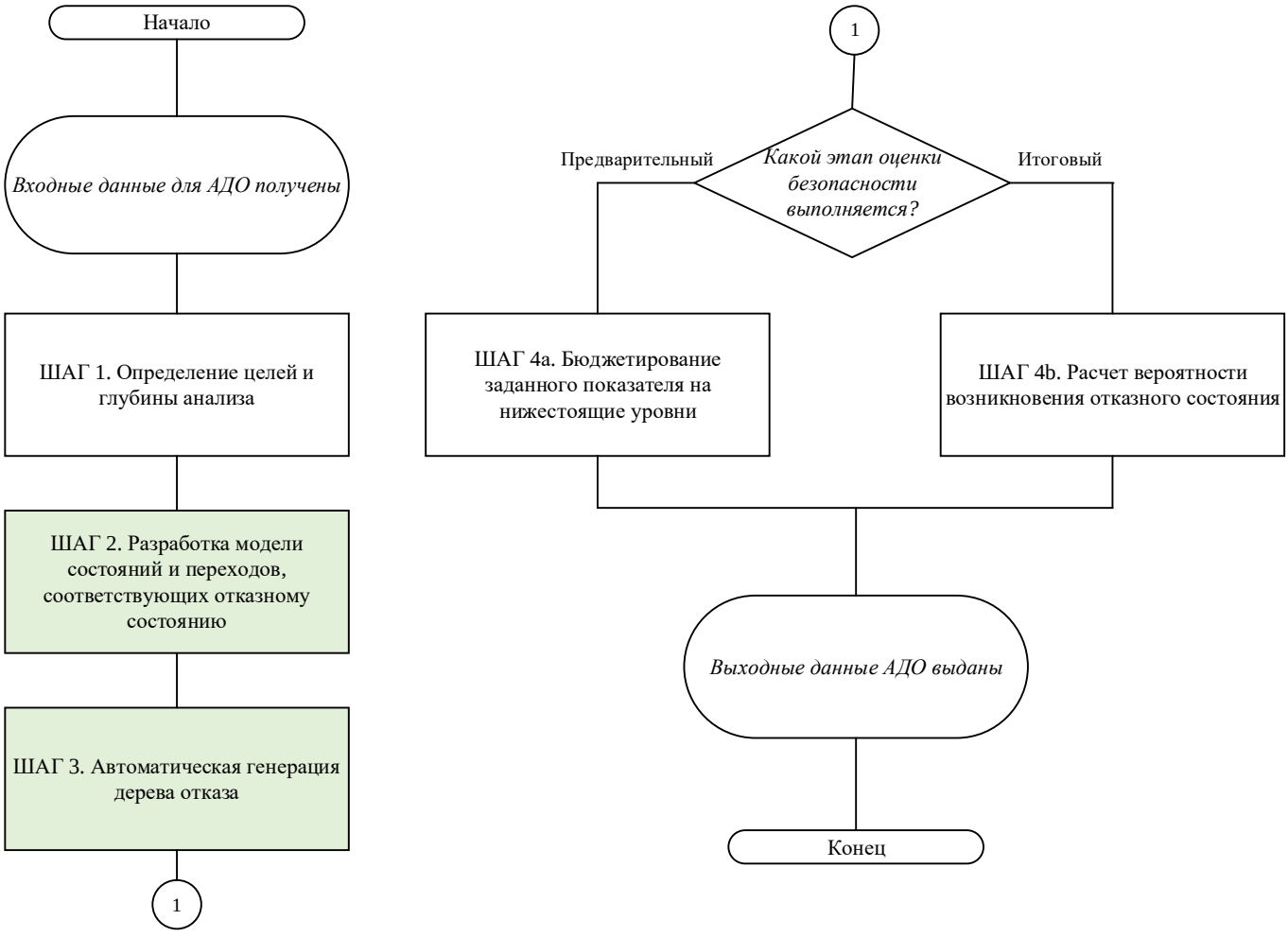

Рисунок 43. Алгоритм модельно-ориентированного подхода к ОФО

Входными данными для выполнения АДО являются:

– Результаты ОФО/ПОБ на вышестоящем уровне иерархии;

– Функциональные блок-схемы системы.

Шаг 1. Определение целей и глубины анализа

Цель анализа зависит от этапа, на котором выполняется анализа. На этапе предварительной оценки безопасности достигаются следующие цели:

– распределение вероятности отказа верхнего уровня, т.е. выполнение бюджетирования;

– определение требований к архитектуре системы для обеспечения заданного уровня отказобезопасности;

– определение уровней гарантий разработки;

На этапе оценки безопасности выполняется подтверждение того, что требования и цели безопасности были достигнуты.

Глубина анализа или его границы должны быть определены. Можно выделить следующие уровни выполнения анализа:

– самолет;

– система;

– подсистема;

– функциональный блок подсистемы.

Границы и задачи выполняемые на каждом из этих уровней представлены в таблице 14.

Таблица 14 – Уровень анализа деревьев отказов

Уровень анализа	**Граница анализа**	**Выполняемый анализ**
Самолет	Функциональная блок-схема самолета	Предварительная оценка безопасности: Распределение бюджетов вероятностей и критичностей отказов по различным системам выполняющих совместно самолетную функцию. Оценка безопасности:

Уровень анализа	Граница анализа	Выполняемый анализ
		Определение последствий отказов и их вероятностей, влияющих на самолет по результатам оценки безопасности уровня системы.
Система	Функциональная блок-схема системы	Предварительная оценка безопасности: Распределение бюджетов вероятностей и критичностей отказов на подсистемы. Оценка безопасности: Использование интенсивностей отказов подсистемы для оценки вероятности возникновения рассматриваемых событий.
Подсистема	Функциональная блок-схема подсистемы	Предварительная оценка безопасности: Распределение бюджетов вероятностей и критичностей отказов по функциональным блокам системы Оценка безопасности: Использование интенсивностей отказов функциональных блоков (т.е. интенсивность отказов процессора, генераторов, памяти и т.д.).
Функциональный блок	Схемы блока (электрические, гидравлические и другие)	Предварительная оценка безопасности: Распределение бюджетов вероятностей и критичностей отказов по функциональным блокам системы. Распределение уровней гарантий конструирования на аппаратное обеспечение и программное обеспечение. Оценка безопасности: Использование интенсивностей отказов конкретных элементов (т.е. интенсивность отказов приемника сигналов по ARINC 429), что позволяет оценить конкретных отказы и их влияние.

Шаг 2. Разработка модели состояния и переходов, соответствующих отказному состоянию

Разработка модели состояния и переходов, соответствующих отказному состоянию, ведется на основе метода конечных автоматов в MATLAB Simulink/Stateflow. Диаграмма Stateflow может содержать последовательную и комбинаторную логику в форме диаграмм переходов состояний, блок-схем, таблиц переходов состояний и таблиц истинности. Диаграмма переходов состояний является графическим представлением конечного автомата.

Шаг 3. Автоматическая генерация дерева отказов

ANSYS medini analyze поддерживает автоматическое создание деревьев отказов из моделей MATLAB Simulink / Stateflow. Для каждого выходного порта модели Simulink выбирается каждый путь, ведущий к этому порту. Таким образом создается модель АДО в ANSYS medini analyze.

Шаг 4. Операции с количественными показателями АДО

Шаг 4а. Бюджетирование заданного показателя на нижестоящие уровни

Распределение бюджетов вероятности на компоненты нижестоящего уровня в АДО применяются на этапе предварительной оценки безопасности и могут выполняться как консервативно, так и произвольно.

В случае использования консервативного подхода, бюджет вероятности распределяется равномерно между компонентами нижестоящего уровня в зависимости от оператора-соединения событий: для событий, соединенных оператором «ИЛИ», берется среднее арифметическое значение; для событий, соединенных оператором «И» берется корень n-ой степени, где n – количество событий, соединенных оператором И. В первых редакциях такой подход наиболее приемлем в связи со своей простотой и предрасположенностью к автоматизации. Однако, на более поздних этапах разработки может привести к тому, что одна часть реального оборудования не будет удовлетворять заданным бюджетам, а другая часть будет иметь достаточный запас для ужесточения требований. Это будет проявляться, например, при сравнении механических и электронных систем, т.к. надежность механических компонентов значительно превышает надежность электронных

компонентов. В таком случае используется второй подход с произвольным распределением бюджетов вероятности.

В случае использования подхода с произвольным распределением, бюджет вероятности распределяется между компонентами таким образом, чтобы учесть физическую сущность потенциальных причин отказов оборудования.

Шаг 4b. Расчет вероятности возникновения отказного состояния

Расчет вероятности возникновения отказного состояния ведется на основе реальных значений надежности оборудования и конкретных видов отказов, которые могут произойти в соответствующих компонентов уровня. Расчет вероятности производится на этапе оценки безопасности.

Для расчета вероятности возникновения отказного состояния следует определить набор минимальных сечений. Минимальное сечение – это наименьшая комбинация причин отказов, достаточных для наступления нежелательного события.

При формировании минимальных сечений особое внимание должно уделяться отсутствию одинаковых причин в различных ветках, что может привезти к ошибочным расчетам. В связи с этим рекомендуется для таких случаев избегать ссылок на другие деревья, которые внесены в структуру дерева как неразрабатываемые события. Лучше перенести всю структуру поддерева в анализируемое дерево. Это позволит избежать ош ибок расчета.

Пример, в котором имеется одинаковые события представлен ниже на рисунке 44.

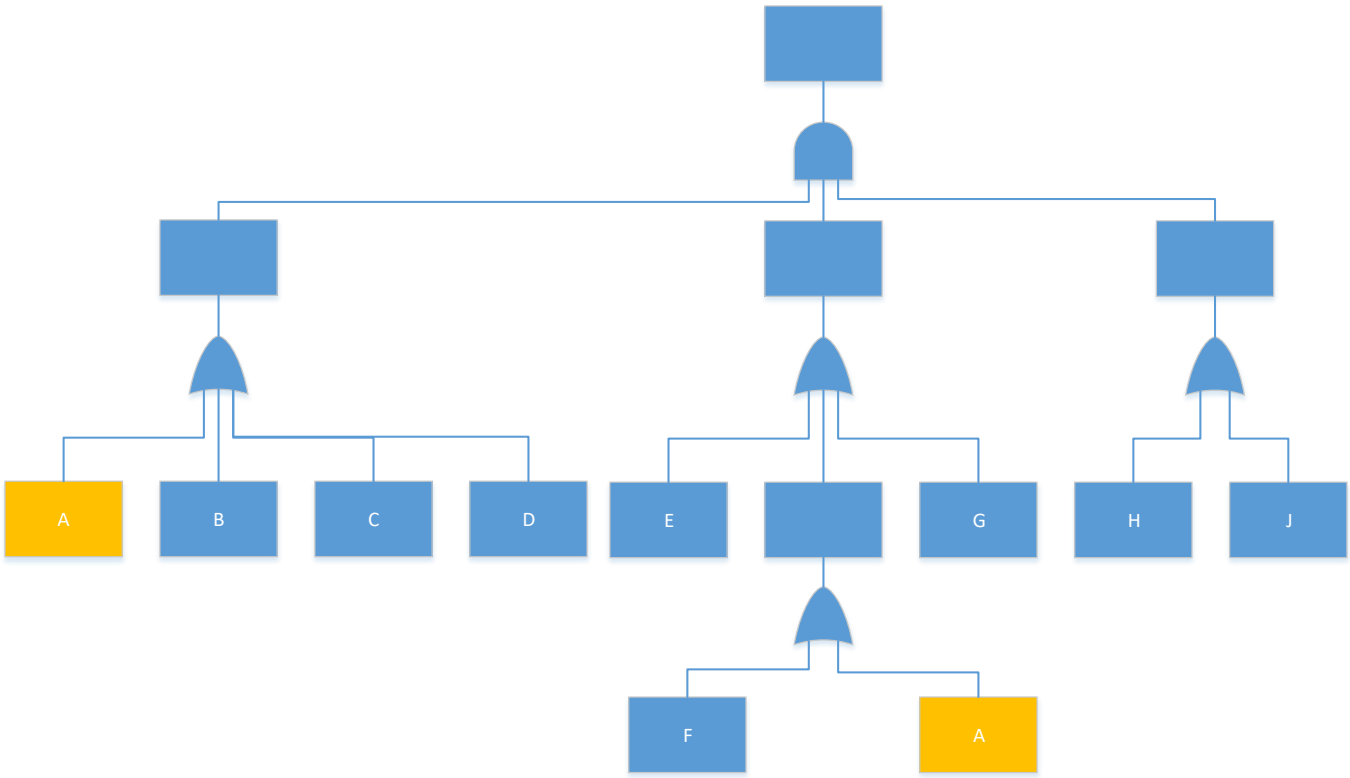

Рисунок 44. Определение минимальных сечений

Обозначив *P(A), P(B), P(C), P(D), P(E), P(F), P(G), P(H), P(J)* как *A, B, C, D, E, F, G, H, J* соответственно, вероятность верхнего события можно записать как: *(A+B+C+D)*(E+F+A+G)*(H+J)*. Раскрывая скобки получим:

AEH+AFH+AAH+AGH+BEH+BFH+ABH+BGH+CEH+CFH+ACH+CGH+AEJ +AFJ+AAJ+AGJ+BEJ+BFJ+ABJ+BGJ+CEJ+CFJ+ACJ+CGJ+DEJ+DFJ+ADJ+DGJ

При этом часть из этих комбинаций не являются минимальными сечениями, так как событие *A* повторяется. Для исключения лишних событий можно воспользоваться следующими правилами:

1. *A+A=A.*
2. *A*A=A.*
3. *A+AK=A.*
4. *AAK=AK.*

Тогда перечень комбинаций может быть уменьшен до следующего:

AEH+BEH+BFH+BGH+CEH+CFH+CGH+AJ+BEJ+BFJ+BGJ+CEJ+CFJ+CG J+ DEJ+DFJ+DGJ.

Эти комбинации являются минимальными сечениями. Перестроенное дерево, в котором исключен повтор события *A*, можно представить как изображено на рисунке 45).

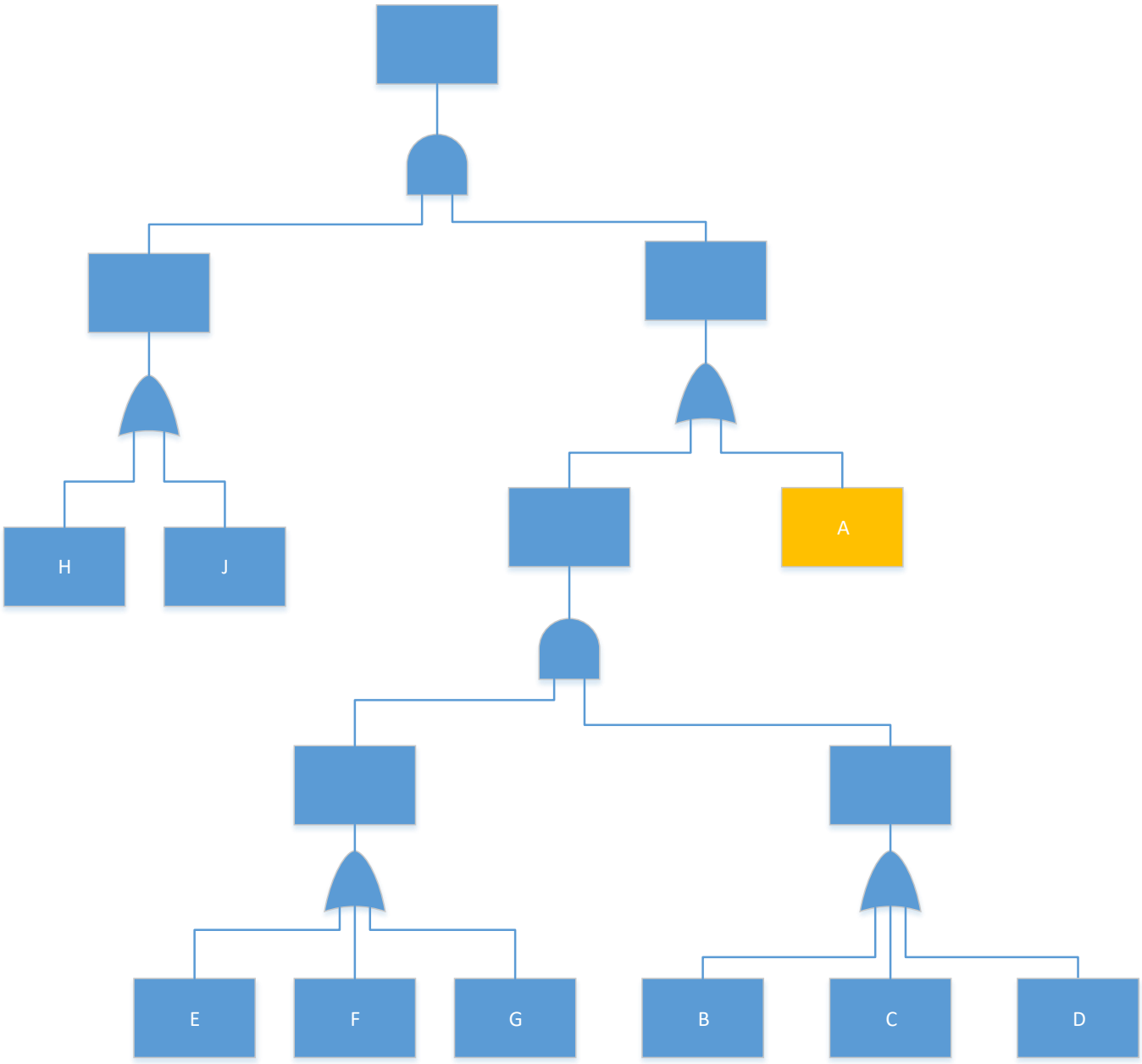

Рисунок 45 – Преобразованное дерево для определения минимальных сечений

Дальнейшее вычисление вероятности возникновения события верхнего уровня выполняется по формулам (8) – (12).

Выходными данными АДО являются:

– Перечень количественных требований по безопасности (на этапе PSSA);

– Расчетные значения вероятности отказных состояний (на этапе SSA).

4.7 Современный подход к анализу видов и последствий отказов

Анализ видов и последствий отказов (АВПО/FMEA) является систематическим исследованием видов отказа системы, изделия, функции или компонента и определением последствий на более высоких уровнях детализации. Выделяют два вида АВПО/FMEA: функциональный и компонентный. Функциональный АВПО применим в основном на этапе ПОБ и для сложного электронного оборудования. На этапе ОБ и для простых компонентов применим компонентный АВПО.

АВПО/FMEA выполняется на выбранном уровне (система, изделие и т.д.) постулированием видов отказа конкретных конечных компонентов на рассматриваемом уровне.

Для каждого из компонентов (для компонентного АВПО) и функционального блока (для функционального АВПО) определяются конкретные относящиеся виды отказа.

Функциональный АВПО/FMEA проводится на любом уровне иерархии системы. Допустимый уровень разукрупнения зависит от структуры анализируемой системы и целей выполняемого анализа, которые могут отличаться на различных стадиях проектирования. При исследовании уровня иерархии «система», а также на более низких уровнях, декомпозиция может привести к определению множества взаимосвязанных блоков, выполняющих единую функцию системы. Такие блоки будем называть функциональными. Для каждого функционального блока должны быть изучены внутренние и интерфейсные функции относительно работы системы.

Дальнейшим действием является идентификация нарушений функций функциональных блоков. Эти нарушения функций функциональных блоков определяются схожим образом как процессе выполнения ОФО, независимо от конкретного применения блоков и как эта функция физически может отказать.

Компонентный АВПО/FMEA аналогичен, по сути, с функциональным, но учитывает вместо анализа на уровне функций конкретные виды отказов всех

компонентов системы. Виды отказов, определяемые в ходе компонентного АВПО, могут быть справочными или взятыми по результатам испытаний.

Независимо от применимого подхода к АВПО, каждому виду отказа назначается интенсивность отказа исходя из расчетов надежности и справочных материалов [67].

На первый взгляд может показать, что сам по себе АВПО не сложен и все возможные методики разработаны достаточно давно (АВПО применяется с 1940х годов). Однако с ростом сложности и интеграции систем, возникает проблема влияния человеческого фактора.

Специалист по надежности и безопасности, выполняющий анализ, не всегда может адекватно оценить отказ и определить его последствия [68]. Данная проблема особенно актуальна для современных сложных блоков комплексов бортового оборудования гражданских самолетов, выполненных на основе электронных элементов аппаратуры.

4.8 Разработка методики модельно-ориентированного подхода к выполнению Анализа видов и последствий отказов

4.8.1 Цели и проблематика выполнения Анализа видов и последствий отказов

На текущий момент Анализ видов и последствий отказов выполняется вручную экспертами по оценке безопасности, что наряду с очевидным преимуществом, таким как использование обширного опыта экспертов, имеет и недостатки, а именно – высока вероятность совершить ош ибку при ручных расчетах, пропустить при анализе какие-либо функции или компоненты, либо, что случается наиболее часто, не отразить должным образом изменения конструкции в результатах АВПО.

Применение МОПОБ позволит значительно снизить вероятность таких погрешностей за счет использования автоматизации определения конфигурации анализируемого компонента и формализации описания возможных последствий отказов.

Автоматизация определения конфигурации заключается в том, что в ходе проектирования возможно внесение изменений в архитектуру конструкции – добавление новых компонентов, изменение состава и взаимосвязей функциональных блоков, изменение состава элементов с одновременной привязкой к выполнению анализа видов и последствий отказов, которую позволяют установить и отслеживать современные программные инструменты для модельно-ориентированного проектирования и оценки безопасности. Такие инструменты позволяют отслеживать изменения в автоматическом режиме, что позволяет избежать пропуска ответственного компонента или функционального блока при выполнении АВПО.

Формализация определения последствий отказов заключается в том, что полностью перенесенная логика функционирования, контроля и распространения отказов (с учетом их вероятности) в модельный вид позволит уйти от экспертного решения о последствиях отказов и перейти к формальному обоснованию последствий. Метод конечных автоматов является удобным способом моделирования описанных процессов является. Современные инструменты, использующие принципы МОПОБ, позволяют моделировать последствия методом конечных

автоматов в собственных приложениях или же могут получать результаты из сторонних программ автоматизировано.

Также к проблематике выполнения АВПО на текущий момент следует отнести, что не все разработчики оборудования учитывают влияния воздействия одиночных ионизирующих частиц (ВОИЧ) на надежность радиоэлектронного оборудования.

Атмосферное излучение – это общий термин, который относится ко всем типам ионизирующего излучения, включая нейтроны, проникающие или генерируемые в атмосфере Земли. Основными источниками атмосферного излучения являются солнечное и галактическое излучение [69]. Первичные космические лучи высокой энергии (то есть внегалактические, галактические и солнечные космические лучи) непрерывно поступают на Землю и взаимодействуют с атомами в атмосфере Земли, создавая вторичные частицы высокой энергии.

Из различных созданных вторичных частиц нейтроны высокой энергии являются основной причиной так называемых последствий воздействия одиночных ионизирующих частиц (ВОИЧ) в электронных устройствах летательных аппаратов. Этот термин охватывает последствия ряда различных сбоев и видов отказов, вызванных этим явлением [69]. Эти воздействия могут оказывать негативное влияние на безопасность электронного бортового оборудования и самолета в целом.

Оборудование современных самолетов во многом состоит из электронных компонентов. Различаются простые (резисторы, диоды, конденсаторы и т.д.) компоненты и сложные (микроконтроллеры, ПЛИС). Отдельно можно выделить сверхсложные компоненты (многоядерные процессоры). Все они выполняют различные функции, как критичные, так и не критичные по безопасности.

Для нейтронов, а также всех других вторичных частиц в атмосфере высота, широта и энергия являются основными параметрами, помогающими нам понять частоту проявления ВОИЧ:

• максимальная скорость потока на высоте около 60 000 футов – так называемый максимум Пфотцера, и

• общее изменение потока нейтронов (диапазон энергий от 1 до 10 МэВ) с высотой.

На рисунке 46 представлена плотность потока нейтронов, изменяющаяся в зависимости от высоты. Изменение широты атмосферных нейтронов определяется главным образом магнитным полем Земли. Общее изменение атмосферного потока нейтронов (диапазон энергий от 1 до 10 МэВ) с широтой показано графически на рисунке 47 [69].

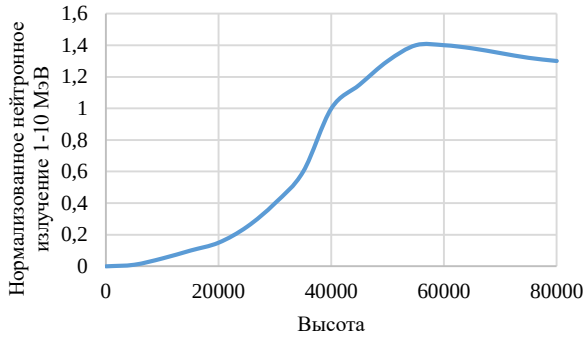

Рисунок 46. Плотность потока нейтронов, изменяющаяся в зависимости от высоты

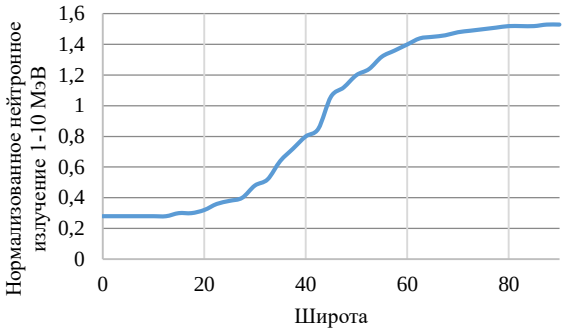

Рисунок 47. Изменение атмосферного потока нейтронов в зависимости от широты

Современные гражданские лайнеры, летающие на высотах порядка 40 000 футов и без ограничений по широтам, попадают под воздействий радиационных частиц, в связи с чем необходимо анализировать влияние этих частиц на надежность и безопасность.

Количественные характеристики, связанные с надежностью, рассчитываются с использованием математических методов, представленных ниже. Качественные характеристики, связанные с безопасностью, основаны на количественных расчетах, но представляют собой техническую оценку (в данном случае в форме АВПО) конкретного эффекта типа ВОИЧ.

4.8.2 Методика модельно-ориентированного подхода к Анализу видов и последствий отказов

Разработанная методика выполнения АВПО представлена в виде алгоритма на рисунке 48.

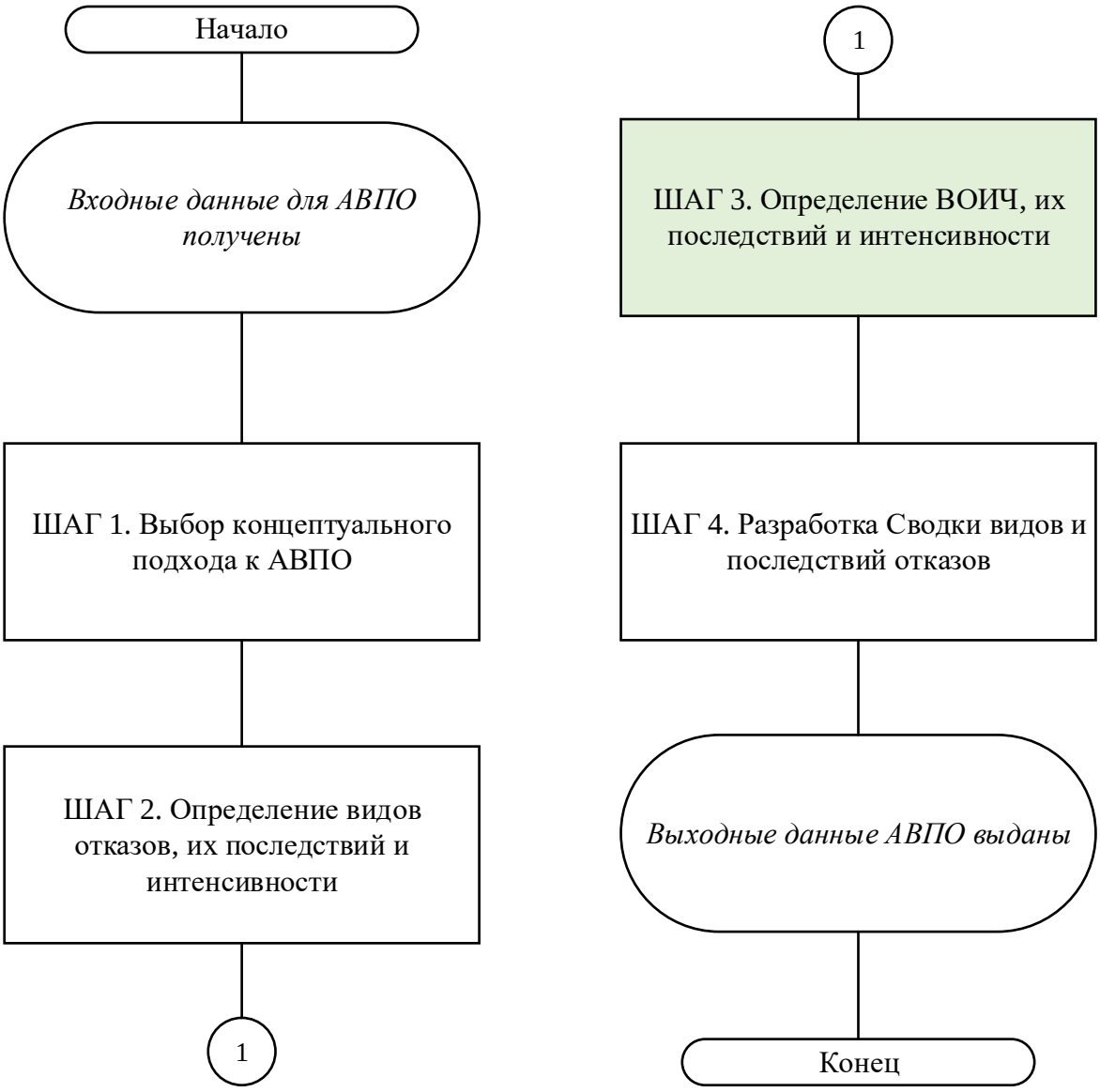

Рисунок 48. Алгоритм модельно-ориентированного подхода к АВПО

Входными данными для выполнения АВПО являются:

- Расчетно-конструкторская документация (включая спецификации изделия, чертежи, алгоритмы и т.д.);
- Анализ надежности каждого компонента в составе изделия.

Шаг 1. Выбор концептуального подхода к АВПО

Выделяют два основных подхода к АВПО – функциональный (как правило используется для сложного электронного оборудования, такого как ПЛИС и микропроцессоры) и компонентный (обычно использующийся для простых

механических и электрических компонентов). Как к функциональному, так и к компонентному АВПО применим количественный подход к выполнению анализа, при котором для каждого вида отказа определяется значение его интенсивности либо на основе данных из истории предыдущей эксплуатации, либо из справочников с данными интенсивности отказов, например, таким как MIL-HDBK-217 [70], MIL-HDBK-338 [71], RAC «Nonelectronic Parts Reliability Data» [37], Rome Laboratory «Reliability Engineer's Toolkit» [72] и отечественный справочник ЭРИ-2006 [6].

При выполнении FMEA следует учитывать, что компонент системы, для которого проводится анализ, имеет разноуровневое строение – сам компонент, его функциональные блоки (ФБ) и элементы аппаратуры, входящие в функциональный блок, как представлено на Рисунке 49.

Рисунок 49. Общее представление уравнений иерархии изделия при выполнении АВПО

Функциональный метод АВПО применяется на этапе ПОБ, а также для сложных компонентов на любом этапе.

Компонентный метод АВПО применяется на этапе ОБ.

Шаг 2. Определение видов отказов, их последствий и интенсивности

Общая схема (алгоритм) АВПО функциональным методом включает следующие операции:

1. идентифицируют все функции, выполняемые функциональными блоками (ФБ);
2. для каждой функции ФБ определяют перечень возможных нарушений функции ФБ (НФФБ) методом, аналогичным определению отказных состояний в ОФО (полная потеря/частичная потеря/самопроизвольное выполнение/ошибочное выполнение);
3. определяются последствия НФФБ для рассматриваемых и интерфейсных ФБ из которых должна быть очевидна связь с событием из ОФО;
4. для каждого нарушения функции ФБ оценивают возможные последствий этого нарушения, которые берутся из перечня отказных состояний ОФО. Если в ОФО отсутствует подходящее в качестве последствий отказное состояние, то данное отказное состояние должно быть включено в следующую редакцию ОФО;
5. на основании событий ОФО определяется степень опасности;
6. определяются возможные методы обнаружения НФФБ в виде допущений к внутреннему контролю и взаимодействующих систем. Данные допущения должны быть провалидированы в ходе дальнейшей разработки.

Процессы выполнения компонентного АВПО состоит из следующих действий:

1. все компоненты в сборке изделия анализируются для выявления возможных конкретных видов отказов: механических (разрушения, заклинивания) и электрических (пробой, обрыв, уход за нормы ТУ);
2. для определенных в предыдущем действии видов отказов анализируются последствия на уровне сборки и изделия в целом. Могут использоваться материалы функционального АВПО или ОФО. Последствия отказов должны быть хорошо задокументированы, в том

числе включая информацию по способам обнаружения отказов или утверждения, что отказ является скрытым. Далее эта информация должна быть подтверждена моделированием или испытаниями;

3. в зависимости от определенных на предыдущем шаге последствий отказов, указываются уровни критичности данных видов отказов. Четкая и ясная связь с ОФО позволяет использовать валидированные значения;

4. указанные действия выполняются для каждого из уровней иерархии изделия: простой компонент (резистор, пружина и т.д.), функциональный узел, функциональный блок, система. Каждый из уровней определяется на основе результатов предыдущего, более низкого уровня;

5. те отказы, степень опасность которых превышает допустимые значения в соответствии с определенными требованиями, включают в перечень особо ответственных элементов, контроль которых в ходе эксплуатации позволяет проводить регулярные регламентные работы для определения исправности оборудования и демонстрации их летной годности.

Шаг 3. Определение ВОИЧ, их последствий и интенсивности

На сложные и сверхсложные компоненты могут воздействовать ионизирующие частицы, представленные в таблице 15.

Таблица 15. Типы ВОИЧ с описанием

Тип ВОИЧ	**Описание типа ВОИЧ**
Радиационно-индуцированный сбой в одном бите (Single Event Upset)	Изменение состояния в бите или регистре, или фиксация состояния в устройстве, когда излучение, поглощаемое устройством, является достаточным для изменения логического состояния бита. Обычно данный тип ВОИЧ проявляется в виде переходных импульсов в логических схемах или в виде изменения битов в ячейках памяти или регистрах. Короткий

Тип ВОИЧ	Описание типа ВОИЧ
	импульс тока воспринимается микросхемой как импульсная помеха, и, если его амплитуда достаточно велика, он может привести к переключению элемента, стоящего за пораженным транзистором. Комбинационные и аналоговые схемы в момент прохождения импульса тока выдают неверный результат, а запоминающие элементы переключаются навсегда. Таким образом, наиболее уязвимой частью микропроцессора является кэш-память: ее на кристалле много, и сбои в ней не проходят сами по себе.
Радиационно-индуцированный сбой в нескольких битах (Multiple Bit Upset)	Постоянное совершенствование технологических процессов привело к созданию очень плотных ячеек памяти, которые хранят информацию с меньшей емкостью и низким напряжением. Следовательно, требуется меньше заряда, чтобы произвести один или несколько сбоев в памяти. Энергия, откладываемая в кремнии электронного компонента одной ионизирующей частицей, приводит к тому, что в одном и том же слове происходит изменение в более чем одном бите [73].
Радиационно-индуцированный сбой в нескольких ячейках (Multiple Cell Upset)	ВОИЧ, которое включает в себя одновременный сбой двух или более ячеек в интегральной схеме. Примечание: обычно отказавшие ячейки физически соседствуют, но не всегда.
Защелкивание транзистора (тиристорный эффект) (Single Event Latchup)	Запуск паразитной цепи PNPN в КМОП элементе, что приводит к состоянию, когда паразитный фиксированный ток превышает ток удержания. Это состояние поддерживается при подаче питания. Результатом будет формирование короткого замыкания

Тип ВОИЧ	Описание типа ВОИЧ
	между землей и питанием, потеря работоспособности пораженного элемента и резкий рост тока потребления, способный привести к защелкиванию пораженного элемента и функциональному отказу. Тиристорный эффект может вызвать блокировку цепи и / или сбой устройства. Может вызывать или не вызывать постоянный сбой, но требует включения / выключения питания для возврата интегральной схемы к нормальной работе, если она не повреждена.
Эффект пробоя подзатворного диэлектрика (Single Event Gate Rupture)	Происходит в затворе компонента с изолированным затвором, когда поглощаемый устройством заряд излучения достаточен для его разрушения. Отказ проявляется с разрушением затвора компонента.
Радиационное выжигание (Single Event Burnout)	Происходит, когда запитанное электронное устройство или его часть выжигается в результате поглощения энергии, вызванного ВОИЧ.
Переходный процесс (Single Event Transient)	Ложный сигнал или напряжение, вызванное вкладом заряда одной частицей, которая может распространяться по цепи в течение одного тактового цикла.
«Жесткий» сбой (Single Event Hard Error)	«Жесткие» сбои в устройствах, таких как память, принимают форму «замороженных» битов. Сбой называется «жестким», т.к. устройство больше не работает должным образом, даже после сброса питания и повторного включения.
Одиночное событие прерывания функции (Single Event Functional Interrupt)	Взаимодействие между радиационной частицей и полупроводниковым устройством, которое приводит к прерыванию функции устройства (потенциально требующему сброса), например, из-за повреждения

Тип ВОИЧ	Описание типа ВОИЧ
	внутреннего канала управления сложного устройства, такого как микропроцессор.

Из данной таблицы видно, что воздействие атмосферного излучения на бортовые системы или оборудование может привести к различным последствиям (как временным, так и постоянным).

На данный момент аспекты влияния различных типов ВОИЧ на надежность оборудования уже достаточно хорошо изучены [74], и интенсивность различных типов ВОИЧ можно прогнозировать [75].

Упрощенный метод расчета интенсивности ВОИЧ для конкретного типа ВОИЧ заключается в умножении площади поперечного сечения полупроводника, на который воздействует частица для этого типа ($см^2$) на интегральный поток нейтронов; например, 6000 н/см2 в час (энергия > 10 МэВ). При расчете интенсивности ВОИЧ для устройств с меньшей геометрией, на которые могут влиять нейтроны с более низкой энергией, поток нейтронов с энергией от 1 до 10 МэВ добавляется к 6000 $н/см^2$ в час. Поток $6000н/см^2$ в час является номинальным значением для высоты 40 000 футов (12,2 км) и широты 45° и может быть рассчитан для разных высот и широт. Примеры расчета интенсивности ВОИЧ:

$$\lambda_{ВОИЧ} = 6000\left[\frac{н}{см^2}\right] \times S_{ППСПП}\left[см^2\right] \quad (13)$$

Используя *(13),* интенсивность ВОИЧ может быть рассчитана для каждого сложного и сверхсложного компонента, подвергшегося воздействию излучения. Кроме того, можно консервативно предположить, что заданная интенсивность ВОИЧ является интенсивностью каждого типа ВОИЧ, т.е. все события равновероятны.

Шаг 4. Разработка Сводки видов и последствий отказов

Сводка отказов с уровня программных и аппаратных отказов

АВПО программных и аппаратных отказов является наиболее фундаментальным анализом по сравнению с остальными уровнями абстракции. Это объясняется, что на данном уровне рассматривается атомарная структура изделия, без обобщений. Если по результатам данного анализа будет выявлено, что отсутствуют виды отказов, приводящие к катастрофическим последствиям, то цели АВПО всего изделия достигнуты (однако это не исключает необходимости обобщения и представления на более высоких уровнях иерархии для упрощения смежного анализа дерева отказов и в интересах сертификации). С другой стороны, если будет обнаружен вид отказа, который приводит к катастрофической ситуации, то архитектура изделия должна быть переделана таким образом, чтобы митигировать последствия данного вида отказа, несмотря на степень готовности рассматриваемого и смежного оборудования.

Для сокращения объема отчетной документации на более высоких уровнях иерархии, результаты АВПО программных и аппаратных средств сводятся в Сводку видов и последствий отказов, основываясь на одинаковых последствиях. При этом интенсивности видов отказов складываются. Пример реализации процесса представлен на рисунке 50.

Рисунок 50 Пример перехода от программных и аппаратных АВПО к СВПО

Сводка отказов с уровня отказов функциональных блоков

АВПО функциональных блоков является наиболее удобным анализом для системных аналитиков безопасности по сравнению с остальными уровнями абстракции. Это объясняется тем, что на данном уровне рассматриваются очевидные отказные состояния, не требующие детального понимания физики нарушения аппаратуры, но при этом отказы не абстрактные, а привязаны непосредственно к тем функциям, которые выполняются оборудованием. Последствия на более высоком уровне и причины на более низком уровне поддаются анализу и выявлению причинно-следственных связей поведения item в случае отказов.

Для сокращения объема отчетной документации на более высоких уровнях иерархии, результаты АВПО функциональных блоков сводятся в Сводку видов и последствий отказов, основываясь на одинаковых последствиях. При этом интенсивности видов отказов складываются. Пример реализации процесса представлен на рисунке 51.

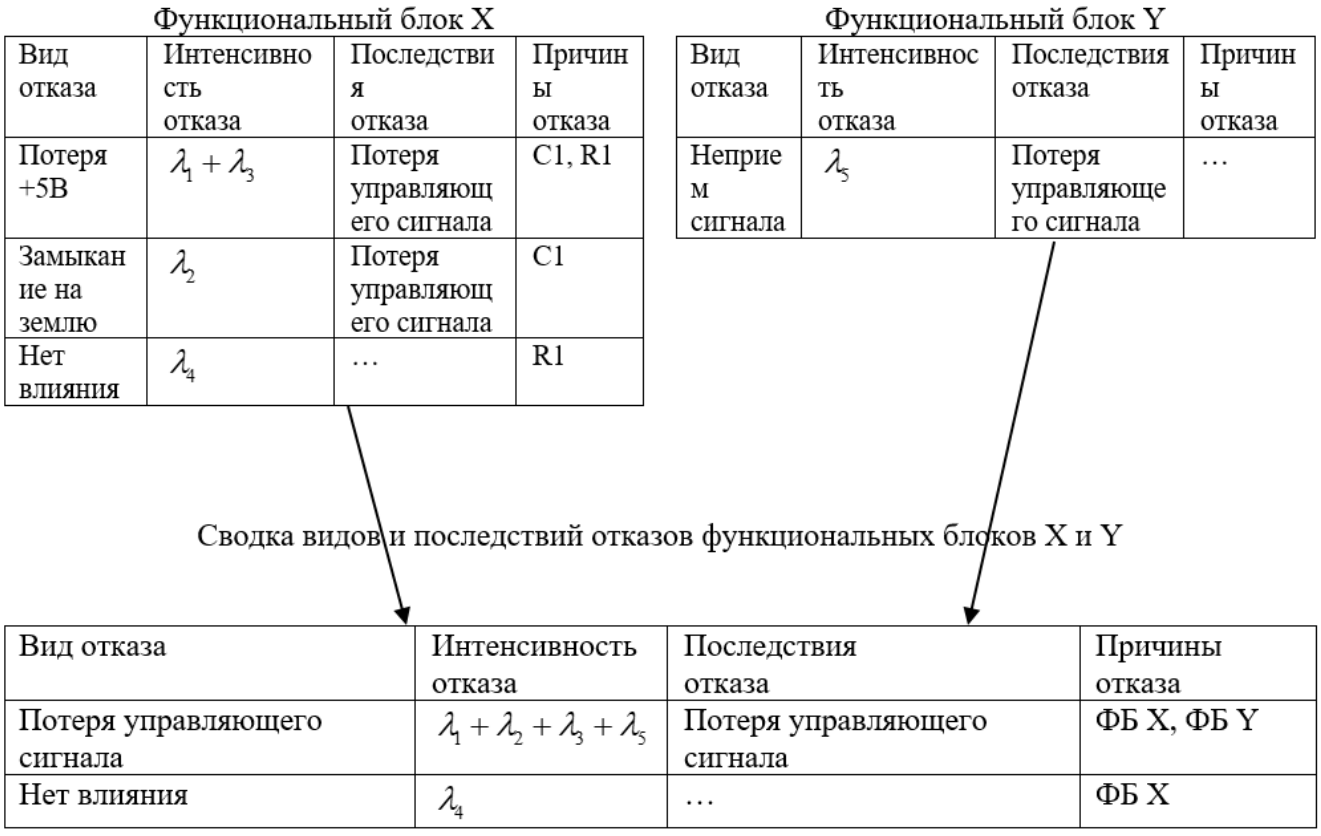

Рисунок 51. Пример перехода от АВПО функциональных блоков к СВПО

Сводка отказов с уровня отказов изделий

АВПО уровня изделий является наиболее приемлемым анализом для аналитиков безопасности уровня самолета или самолетной системы по сравнению с остальными уровнями абстракции. Это объясняется тем, что на данном уровне рассматриваются конкретные отказные состояния, не требующие детального знания конструкции изделий, при этом отказы привязаны непосредственно к тем функциям, которые выполняются данным изделием и может быть исследовано влияние на отказные состояния, определенные в ходе выполнения Оценки функциональных опасностей. Последствия на более высоком уровне и причины на более низком уровне поддаются анализу и выявлению причинно-следственных связей поведения системы в случае отказов.

Для сокращения объема отчетной документации, результаты АВПО изделия объединяются в Сводку видов и последствий отказов, основываясь на одинаковых последствиях, для дальнейшего использования в анализе дерева отказов и для взаимодействия с сертификационными органами. При этом интенсивности видов отказов складываются. Пример реализации процесса представлен на рисунке 52.

Изделие X

Вид отказа	Интенсивность отказа	Последствия отказа	Причины отказа
Потеря управляющего сигнала	$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_5$	Потеря управления поверхностью	ФБ X, ФБ Y
Нет влияния	λ_4	Нет влияния	ФБ X

Изделие Y

Вид отказа	Интенсивность отказа	Последствия отказа	Причины отказа
Ложный управляющий сигнал	λ_6	Кратковременное колебание	…
Нет влияния	λ_7	Нет влияния	…

Сводка видов и последствий отказов изделий X и Y

Вид отказа	Интенсивность отказа	Последствия отказа	Причины отказа
Потеря управления поверхностью	$\lambda_1 + \lambda_2 + \lambda_3 + \lambda_5$	Снижение маневренности по крену	ФБ X, ФБ Y
Кратковременное колебание	λ_6	Возмущение в движении по крену	
Нет влияния	$\lambda_4 + \lambda_7$	Нет влияния	ФБ X

Рисунок 52. Пример перехода от АВПО изделий к СВПО

Выходными данными АВПО являются:

- Перечень базовых событий для АДО;
- Подтверждение соответствия изделием требованиям АП-25.1309.

4.9 Применение модельно-ориентированного подхода к оценке безопасности комбинированного метода кворум-контроля

Оценка функциональных опасностей и анализ видов и последствий отказов играют меньшую роль в контексте функции комбинированного метода кворум-контроля. Тем не менее, степень опасности отказов и их подтверждение в соответствии с указанной методикой представлено в Главе 2. Влияние ВОИЧ также учитывается в расчетах вероятности, представленных ранее. Ключевую роль в применении МОПОБ к комбинированному методу кворум-контроля выполняет Анализ дерева отказов.

В данном разделе будет разработан автомат в использованием средств MATLAB *Stateflow* и преобразован в дерево отказов с использованием средств ANSYS medini analyze.

Опишем рассматриваемый случай. Пусть имеется некая трехканальная система со встроенной системой контроля. Встроенные системы контроля трехканальных систем, широко применяющиеся в авиационной промышленности, способны работать до второго отказа, т.к. при отказе одного из каналов, отказавший исключается из формирования достоверного сигнала; при отказе второго канала (особенно в случае ложного сигнала по данному каналу) встроенные системы контроля не способны определить, какой из каналов отказал. В таком случае, как правило, переходят на таблично заданные коэффициенты или резервные средства получения информации. Таким образом могут быть идентифицированы три состояния:

1) Все три канала системы исправны;
2) Один канал в состоянии «отказ» и два исправны;
3) Три канала в состоянии «отказ».

Также предполагая наличие кратковременных сбоев (например, редиационно-индуцированных [76]), будем считать, что по результатам каждого такта работы встроенной системы контроля все три канала будут заново проходить проверку исправности. Проверка исправности работоспобности каждого отдельно взятого канала будет определяться путем попарного сравнения значений всех каналов. В тех случаях, когда все полученные разности меньше некоего значения ε, будет приниматься исправность всех каналов. В тех случаях, когда в двух полученных разностях значение больше значения ε, канал, участвующий в обоих проверках, будет считаться отказавшим. Результирующий интегральный сигнал будем рассчитывать, как среднее арифметическое значений исправных каналов.

Представим описанную логику в виде автомата, реализованного в MATLAB Stateflow, как представлено на рисунке Рисунок 53.

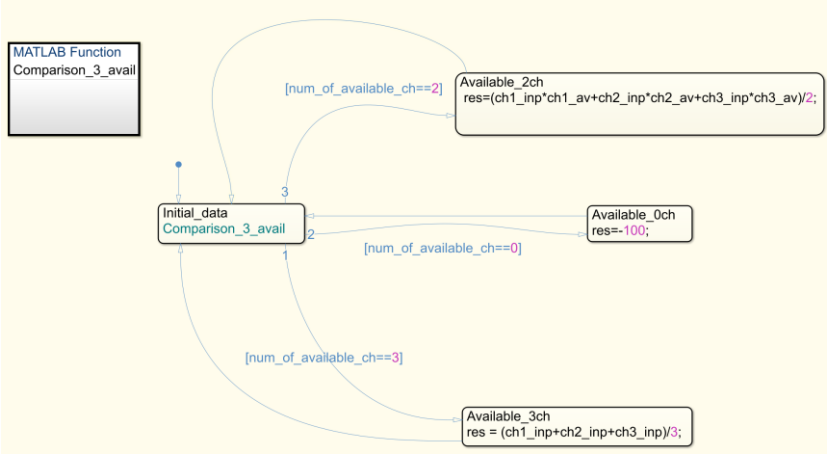

Рисунок 53. Реализация логики примера в MATLAB Stateflow

На рисунке использованы следующие переменные:

num_of_available_ch – количество доступных каналов (не находящихся в состоянии «отказ»);

ch1_inp (ch2_inp, ch3_inp) – входное значение *i*-го канала;

ch1_av (ch2_av, ch3_av) – признак исправности *i*-го канала, определяющийся функцией *Comparison_3_avail;*

res – выходное значение интегрального сигнала по результатам работы встроенной системы контроля.

Результатом работы является преобразование данной логики в Анализ дерева отказов, который представлен на рисунке 54.

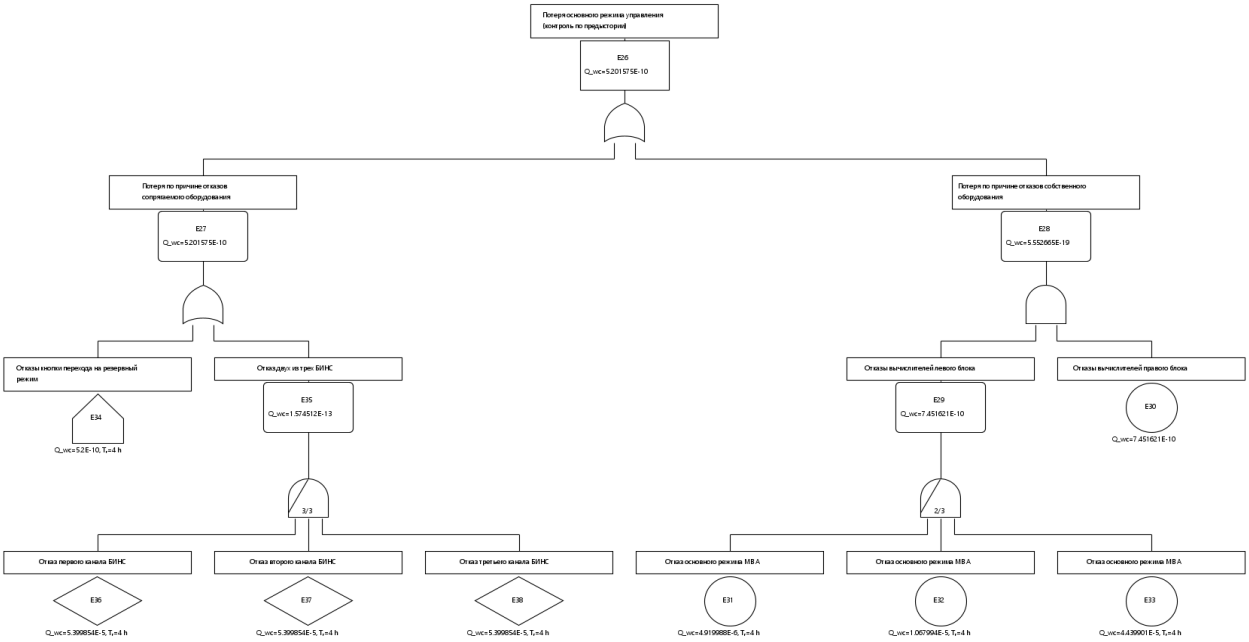

Рисунок 54. Реализация дерева в ANSYS medini analyze

Выводы по главе 4

1. Описаны основные принципы модельно-ориентированного подхода к оценке безопасности, заключающиеся в доработке существующих инструментов и языков программирования под задачи оценки безопасности и анализа надежности изделий.

2. Выявлены основные препятствия и проблемы использования МОПОБ на текущий момент:

- текущие стандарты, требующие выполнение мероприятий процесса оценки безопасности, не требуют использования МОПОБ;
- отдельно взятые работы, посвященные МОПОБ, решают частные задачи и не связаны между собой методологически и инструментально;

3. Предложена модернизация применимого системного подхода к оценке безопасности, описанного в нормативной документации с учетом внедрения МОПОБ.

4. Разработана Stateflow модель переходов состояний для комбинированного метода кворум-контроля, на основе которой получена структура и расчет Анализа дерева отказов.

ЗАКЛЮЧЕНИЕ

Целью работы являлось разработка повышение безопасности полетов за счет снижения вероятности преждевременного перехода на резервный режим КСУ.

Первичный анализ архитектур КСУ показал, что основная проблема является в том, что переход на резервный режим КСУ происходит при отказах во взаимодействующем оборудовании: БИНС и СВС. Проблематика вызвана тем, что большая часть методов контроля работает исправно вплоть до второго отказа. Таким образом, сохраняются исправные источники сигналов БИНС и СВС, однако они не используются для продолжения работы в основном режиме в том числе из-за некоторых комбинаций отказов, приводящих к невозможности определить, какой из источников формирует корректные сигналы. Дополнительные ошибки вкладывают ошибки измерения, выраженные гауссовским законом распределения плотности вероятности.

В ходе работы были изучены существующие методы кворум-контроля резервированных сигналов бортового оборудования на примере сигналов БИНС и СВС. Было выявлено, что существуют различные методики, связанные с внедрением дополнительных наземных корректирующих устройств, а также использование элементов искусственного интеллекта. Несмотря на перспективность данных методик, они не всегда могут быть реализованы на борту реальных гражданских воздушных судов. При использовании корректирующих устройств, невозможно обеспечить корректную работу при прерываниях получения сигнала от данного наземного корректирующего устройства, а методы искусственного интеллекта на текущий момент не могут быть внедрена в проекты гражданской авиации из-за особенностей сертификации гражданской авиационной техники, а также подверженности к кибератакам. В связи с этим анализ существующих методов основывался на «классических» методах: вычисление среднего арифметического значения, вычисление медианного значения, контроль по предыстории.

Сравнение методов кворум-контроля осуществлялось по следующим основным видам отказов и их комбинациям:

1. Мгновенный отказ в одном канале;
2. Постепенный отказ в одном канале;
3. Мгновенный отказ в двух каналах;
4. Постепенный отказ в двух каналах;
5. Мгновенный отказ в одном канале с последующим постепенным отказом в другом канале;
6. Постепенный отказ в одном канале с последующим мгновенным отказом в другом канале.

В первой главе было обнаружено, что метод вычисления среднего арифметического дает неисправный результат уже при отказе в одном канале, а метод вычисления медианного значения и контроля по предыстории исправно работают вплоть до второго отказа, при этом при различных комбинациях видов отказов, разные методы показывают лучшие варианты. Таким образом было показано, что «классические» методы не обеспечивают требуемый уровень безопасности в части вероятности перехода на резервный режим КСУ, а перспективные методы сложны в реализации, имеют сложности с сертификацией и также не гарантируют корректность получаемых результирующий значений. Исходя из этого встала задача разработки методики кворум-контроля, решающей эти проблемы.

Во второй главе были сформулированы требования к разрабатываемой методике, основываясь на методах Лорцзака и неравенства Чебышева. С использованием неравенства Чебышева определяются аномальные значения анализируемого временного ряда и определяется весовой коэффициент предыстории. Вторым весовым коэффициентом метода Лорцзака является коэффициент близости сигналов. Алгоритмическое обеспечение методики заключается в внедрении дополнительных условий «флагов доступности» каждого из каналов взаимодействующей системы для повышения показателя контролепригодности. Реализованная методика обеспечила лучшие показатели как по вероятности, так и по функционированию, т.к. удалось предотвратить переход на резервный режим КСУ вплоть до третьего отказа сопрягаемого оборудования. Сравнение результатов различных методик представлено в таблице

Параметр	Среднее арифметическое	Медианное значение	Контроль по предыстории	Комбинированная методика
Вероятность перехода на резервный режим КСУ	$2{,}53 * 10^{-4}$	$1{,}49 * 10^{-8}$	$1{,}49 * 10^{-8}$	$5{,}21 * 10^{-10}$
Функционирование	Вплоть до первого отказа	Вплоть до второго отказа	Вплоть до третьего отказа, за исключением ситуации, когда сначала происходит постепенный отказ, а затем мгновенный	Вплоть до третьего отказа при рассмотренных любых комбинациях отказов

Т.к. реализованная методика показала положительные результаты с точки зрения вероятности и работы при отказах, в Главе 3 был разработан стенд полунатурного моделирования и проведены испытания при различных конфигурациях самолета на взлете и посадке. По результатам 288 испытаний в автоматическом и ручном режиме управления было выявлено, что предложенный метод контроля при всех комбинациях отказов не приводит к ситуации хуже БС/УУП, в то время как все остальные методы приводят к КС ситуациям в различных опытах.

Т.к. по результатам испытаний доводы, сделанные в Главе 2, оправдались, то следующим шагом стала оценка безопасности данного метода в соответствии с требованиями сертификации гражданской авиационной техники. В Главе 3 проанализированы методы оценки безопасности и даны предложения по их модернизации с учетом активного внедрения различных модельно-ориентированных методов. Так в процесс Оценки функциональных опасностей было предложено внедрить этап валидации степени опасности, в Анализ видов и последствий отказов учет моделей отказов, вызванных воздействием радиационного излучения, а Анализ дерева отказов предложено было автоматизировать за счет разработки Stateflow-диаграмм. Применительно к оценке безопасности предложенного метода была разработана диаграмма перехода между состояниями и на основе ее сгенерировано дерево, подтверждающее указанные выше вероятности.

Список использованных источников

[1] АР МАК, Руководство Р4754а по разработке воздушных судов гражданской авиации и систем, Москва, 2016, 131 с.

[2] Б.С. Алёшин, С.Г. Баженов, Ю.И. Диденко, Ю.Ф. Шелюхин. Системы дистанционного управления магистральных самолетов — М. : «Наука», 2013. — 292 с.

[3] Герон С. В., Фрид А. И. Голосование в N-кратно резервированных системах //Вестник Уфимского государственного авиационного технического университета. – 2007. – Т. 9. – №. 2. – С. 42-49.

[4] Гавриленко Ю. В. и др. Сравнительный анализ мажоритарного и статистического контроля при оценке качества функционирования БИНС //НАВИГАЦИЯ И УПРАВЛЕНИЕ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ. – 2013. – С. 82.

[5] Гришко А. К. Анализ надежности структурных элементов сложной системы с учетом интенсивности отказов и параметрической девиации //Модели, системы, сети в экономике, технике, природе и обществе. – 2016. – №. 3 (19). – С. 130-137.

[6] Надежность Э. Р. И. справочник //М.: МО РФ. – 2006. – Т. 641.

[7] Mahar D., Fields W., Reade J. Failure Mode/Mechanism Distributions-FMD 2016. – 2016.

[8] Кутдусов Ф. Х., Рублев Т. А. Адаптивный мажоритарный элемент в системах автоматического управления //Исследовано в России. – 2005. – Т. 8. – С. 1248-1252.

[9] Lorczak P. R., Caglayan A. K., Eckhardt D. E. A theoretical investigation of generalized voters for redundant systems //[1989] The Nineteenth International Symposium on Fault-Tolerant Computing. Digest of Papers. – IEEE, 1989. – 21-23 June 1989, Chicago, IL, USA – С. 444-451.

[10] Savelev A., Lituev N., Olidaev E. Functional hazards assessment of an integrated flight control system validation using model-based design //IOP Conference

Series: Materials Science and Engineering. – IOP Publishing, 2020. – Т. 868. – №. 1. – С. 012006.

[11] Beer A. et al. Model-based quantitative safety analysis of Matlab Simulink/Stateflow models //Model-Based Development of Embedded Systems. – 2013. – С. 60-69.

[12] Zhang H. et al. Dynamic reliability by using simulink and stateflow //Chemical Engineering Transactions. – 2013. – Т. 33. – С. 529-534.

[13] Cui C. C., Li G. Q. Translate the Stateflow Models into Alloy for Safety Analysis //Applied Mechanics and Materials. – Trans Tech Publications Ltd, 2014. – Т. 490. – С. 1702-1705.

[14] Jiang N., Li G., Liu B. Model-based safety analyses of embedded system using stateflow //2016 11th International Conference on Reliability, Maintainability and Safety (ICRMS). – IEEE, 2016. – С. 1-6.

[15] Bartocci E. et al. Localizing faults in Simulink/Stateflow models with STL //Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (part of CPS Week). – 2018. – С. 197-206.

[16] Chen L., Jiao J., Fan J. Fault propagation formal modeling based on stateflow //2015 First International Conference on Reliability Systems Engineering (ICRSE). – IEEE, 2015. – С. 1-7.

[17] Bourbouh H. et al. Automated analysis of Stateflow models //21st International conference on logic for programming, artificial intelligence and reasoning (LPAR 2017). – 2017. – Т. 46. – С. 144-161.

[18] Wang B., Zhao T. Safety simulation applying Stateflow technology //Journal of Beijing University of Aeronautics and Astronautics. – 2011. – Т. 37. – №. 11. – С. 1415-1420.

[19] Leveson N. G., Stolzy J. L. Safety analysis using Petri nets //IEEE Transactions on software engineering. – 1987. – №. 3. – С. 386-397.

[20] Atluri V., Huang W. K. A Petri net based safety analysis of workflow authorization models //Journal of Computer Security. – 2000. – Т. 8. – №. 2-3. – С. 209-240.

[21] Talebberrouane M., Khan F., Lounis Z. Availability analysis of safety critical systems using advanced fault tree and stochastic Petri net formalisms //Journal of Loss Prevention in the Process Industries. – 2016. – Т. 44. – С. 193-203.

[22] Hei X. et al. Automatic transformation from UML statechart to Petri nets for safety analysis and verification //2011 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering. – IEEE, 2011. – С. 948-951.

[23] Sheldon F. T., Greiner S., Benzinger M. Specification, safety and reliability analysis using Stochastic Petri Net models //Tenth International Workshop on Software Specification and Design. IWSSD-10 2000. – IEEE, 2000. – С. 123-132.

[24] Adamyan A., He D. Failure and safety assessment of systems using Petri nets //Proceedings 2002 IEEE International Conference on Robotics and Automation (Cat. No. 02CH37292). – IEEE, 2002. – Т. 2. – С. 1919-1924.

[25] Zareiee M., Dideban A., Orouji A. A. Safety analysis of discrete event systems using a simplified Petri net controller //ISA transactions. – 2014. – Т. 53. – №. 1. – С. 44-49.

[26] Leveson N. G., Stolzy J. T. Analyzing safety and fault tolerance using time petri nets. – 1984.

[27] Sunanda B. E., Seetharamaiah P. Modeling of safety-critical systems using petri nets //ACM SIGSOFT Software Engineering Notes. – 2015. – Т. 40. – №. 1. – С. 1-7.

[28] Reza H. et al. A safety analysis method using Fault Tree analysis and Petri Nets //2009 Sixth International Conference on Information Technology: New Generations. – IEEE, 2009. – С. 1089-1094.

[29] Liu T. S., Chiou S. B. The application of Petri nets to failure analysis //Reliability Engineering & System Safety. – 1997. – Т. 57. – №. 2. – С. 129-142.

[30] Kabir S., Papadopoulos Y. Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: A review //Safety science. – 2019. – Т. 115. – С. 154-175.

[31] Padberg J. Safety properties in Petri net modules //Journal of Integrated Design and Process Science. – 2004. – Т. 8. – №. 4. – С. 65-78.

[32] Хопкрофт Д. Э., Мотвани Р., Ульман Д. Введение в теорию автоматов, языков и вычислений. – 2008.

[33] Schneeweiss W. G. Fast fault-tree evaluation for many sets of input data //IEEE transactions on reliability. – 1990. – Т. 39. – №. 3. – С. 296-300.

[34] Smith D. J., Simpson K. G. L. The Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2015 Edition) and Related Guidance. – Butterworth-Heinemann, 2020.

[35] Amari S. V., Akers J. B. Reliability analysis of large fault trees using the Vesely failure rate //Annual Symposium Reliability and Maintainability, 2004-RAMS. – IEEE, 2004. – С. 391-396.

[36] Лушпа И. Л. О надежности механических компонентов //Труды Международного симпозиума «Надежность и качество». – 2018. – Т. 1. – С. 117-118.

[37] Arno R. G. Nonelectronic Parts Reliability Data. – Reliability Analysis Center, Rome Air Development Center, 2016.

[38] Tyrone L., Jones T. Handbook of reliability prediction procedures for mechanical equipment //Naval Surface Warfare Center West Bethesda. – NSWC-11, 2011.

[39] Михеев А. А., Демина Л. В. Практика разработки доказательной документации по установлению соответствия ВС требованиям раздела А-0 Авиационных правил, Часть 25 //Научный вестник ГосНИИ ГА. – 2018. – №. 23. – С. 122-128.

[40] Елисеева Т. А., Плахотникова Е. В. Оценка надежности систем автоматического управления методом анализа дерева неисправностей (FTA) //СОВРЕМЕННЫЕ МАТЕРИАЛЫ, ТЕХНИКА И ТЕХНОЛОГИЯ. – 2013. – С. 184-188.

[41] Елисеева Т. А. Повышение качества экспертной оценки при проведении анализа видов, последствий и критичности отказов (АВПКО) технических систем //Известия Тульского государственного университета. Технические науки. – 2015. – №. 6-1. – С. 342-349.

[42] Благовещенский Д. И., Сафонов А. С., Ушаков М. В. Современные подходы к оценке надежности изделия на ранних этапах жизненного цикла изделия

//Известия Тульского государственного университета. Технические науки. – 2016. – №. 8-2. – С. 228-234.

[43] Вавилов В. Е. и др. МЕТОДЫ АНАЛИЗА ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ ЭЛЕКТРОМЕХАНИЧЕСКИХ СИСТЕМ //ЭЛЕКТРОТЕХНИЧЕСКИЕ КОМПЛЕКСЫ И СИСТЕМЫ. – 2021. – С. 168-172.

[44] Смирнов Н. Н., Кротов С. А. Подход к формированию модели отказобезопасности воздушного судна //Научный вестник Московского государственного технического университета гражданской авиации. – 2015. – №. 219 (9). – С. 27-32.

[45] Кротов С. А. К вопросу о контроле отказобезопасности функциональных систем воздушных судов в процессе эксплуатации //Научный вестник Московского государственного технического университета гражданской авиации. – 2013. – №. 11 (197). – С. 79-84.

[46] Liang H. et al. System Safety Analysis of a Full Authority Digital Engine Control System //2017 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC). – IEEE, 2017. – С. 543-548.

[47] Fusaro R., Viola N. Preliminary reliability and safety assessment methodology for trans-atmospheric transportation systems //Aircraft Engineering and Aerospace Technology. – 2018. – Т. 90. – №. 4. – С. 639-651.

[48] Wang Y. et al. Safety assessment process optimization for integrated modular avionics //IEEE Aerospace and Electronic Systems Magazine. – 2019. – Т. 34. – №. 11. – С. 58-67.

[49] Pasa G. D., de Santiago Júnior V. A. Aircraft Navigation Systems Safety Assessment via Probabilistic Model Checking //Computational Science and Its Applications–ICCSA 2021: 21st International Conference, Cagliari, Italy, September 13–16, 2021, Proceedings, Part IV 21. – Springer International Publishing, 2021. – С. 465-480.

[50] Zhang M. et al. Reliability technology using FTA, FMECA, FHA and FRACAS: A review //2021 IEEE International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC). – IEEE, 2021. – С. 282-291.

[51] Sun R. et al. A Safety Analysis Method of Airborne Software Based on ARP4761 //Journal of Physics: Conference Series. – IOP Publishing, 2020. – Т. 1673. – №. 1. – С. 012045.

[52] Zalewski J., Kornecki A. Trends nad challenges in the aviation systems safety and cybersecurity //TASK Quarterly: scientific bulletin of Academic Computer Centre in Gdansk. – 2019. – Т. 23.

[53] Bleu-Laine M. H. et al. A model-based system engineering approach to normal category airplane airworthiness certification //AIAA Aviation 2019 Forum. – 2019. – С. 3344.

[54] Hu Z. et al. A complexity analysis approach for model-based system engineering //2020 IEEE 15th International Conference of System of Systems Engineering (SoSE). – IEEE, 2020. – С. 000501-000506.

[55] Jeyaraj A. K., Tabesh N., Liscouet-Hanke S. Connecting Model-based Systems Engineering and Multidisciplinary Design Analysis and Optimization for Aircraft Systems Architecting //AIAA AVIATION 2021 FORUM. – 2021. – С. 3077.

[56] Bendarkar M. V. et al. A model-based aircraft certification framework for normal category airplanes //AIAA Aviation 2020 Forum. – 2020. – С. 3096.

[57] Кашфутдинов Б. Д. Модельно-ориентированный подход к проектированию системы стабилизации летательного аппарата //РЕШЕТНЕВСКИЕ ЧТЕНИЯ. – 2020. – С. 25-26.

[58] Татаринцев В. А., Васильев А. В. ПРОЕКТИРОВАНИЕ ТЕХНИЧЕСКИХ СИСТЕМ НА ОСНОВЕ МОДЕЛЬНО-ОРИЕНТИРОВАННОГО ПОДХОДА. – 2020.

[59] Станкевич Ф. В. Сравнительный анализ языков архитектурного моделирования ArchiMate и SysML //Молодежь и современные информационные технологии: сборник трудов XI Международной научно-практической конференции студентов, аспирантов и молодых ученых, г. Томск, 13-16 ноября 2013 г. – Томский политехнический университет, 2013. – С. 386-388.

[60] Brunel J. et al. Performing safety analyses with AADL and AltaRica //Model-Based Safety and Assessment: 5th International Symposium, IMBSA 2017, Trento, Italy,

September 11–13, 2017, Proceedings 5. – Springer International Publishing, 2017. – С. 67-81.

[61] Shao N., Zhang S., Liang H. Model-based safety analysis of a control system using Simulink and Simscape extended models //MATEC Web of Conferences. – EDP Sciences, 2017. – Т. 139. – С. 00219.

[62] Munk P., Nordmann A. Model-based safety assessment with SysML and component fault trees: application and lessons learned //Software and Systems Modeling. – 2020. – Т. 19. – №. 4. – С. 889-910.

[63] Gonschorek T. et al. Integrating Safety Design Artifacts into System Development Models Using SafeDeML //Model-Based Safety and Assessment: 6th International Symposium, IMBSA 2019, Thessaloniki, Greece, October 16–18, 2019, Proceedings 6. – Springer International Publishing, 2019. – С. 93-106.

[64] Prosvirnova T. et al. The AltaRica 3.0 project for model-based safety assessment //IFAC proceedings volumes. – 2013. – Т. 46. – №. 22. – С. 127-132.

[65] Литуев Н. А., Савельев А. С., Неретин Е. С. Разработка комплекса моделирования для валидации оценки функциональных опасностей комплексной системы управления с использованием методов модельно-ориентированного проектирования //Crede Experto: транспорт, общество, образование, язык. – 2020. – №. 3. – С. 50-59.

[66] ГОСТ Р. Р 27.302-2009 Надежность в технике (ССНТ). Анализ дерева неисправностей //Электронный фонд правовой и нормативно-технической документации АО «Кодекс» URL: http://http://docs. cntd. ru/document/1200081358 (дата обращения: 25.07. 2020). – 2011.

[67] ГОСТ Р. Р 27.310-95 «Анализ видов, последствий и критичности отказов». – 1995.

[68] Banghart M., Babski-Reeves K., Bian L. Human induced variability during failure mode effects analysis //2016 Annual Reliability and Maintainability Symposium (RAMS). – IEEE, 2016. – С. 1-7.

[69] Riemer B. W., Dela Cruz C., Williams T. Report from the Inaugural Meeting on the Opportunities at the SEEMS Facility June 11-12, 2019. – Oak Ridge National Lab.(ORNL), Oak Ridge, TN (United States), 2020. – №. ORNL/TM-2019/1441.

[70] US Department of Defense. MIL-HDBK-217F (NOTICE 2), Military Handbook Reliability Prediction of Electronic Equipment //Defense Technical Information Center: Alexandria. – 1995.

[71] Handbook M. Electronic reliability design handbook //MIL-HDBK-338, DoD. – 1988.

[72] Dudley B., Morris S., Feduccia A. The rome laboratory reliability engineer's toolkit. – 1993.

[73] Dutta A., Touba N. A. Multiple bit upset tolerant memory using a selective cycle avoidance based SEC-DED-DAEC code //25th IEEE VLSI Test Symposium (VTS'07). – IEEE, 2007. – С. 349-354.

[74] DiBari R. What reliability engineers should know about space radiation effects //2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS). – IEEE, 2013. – С. 1-2.

[75] Pickel J. C. Single-event effects rate prediction //IEEE Transactions on Nuclear Science. – 1996. – Т. 43. – №. 2. – С. 483-495.

[76] Зебрев Г. И. Радиационные эффекты в кремниевых интегральных схемах высокой степени интеграции //М.: НИЯУ МИФИ. – 2010. – С. 148.

[77] Марчук В. И., Токарева С. В. Способ обнаружения аномальных значений при анализе нестационарных случайных сигналов //Известия Южного федерального университета. Технические науки. – 2008. – Т. 80. – №. 3. – С. 66-72.