МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество
АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

кафедра Космическая техника и технологии

«Допущен к защите»
Заведующий кафедрой Ашпбаев Куанпш Арингожаевич, PhD
(Ф.И.О., ученая степень, звание)
_____ «_____» _____ **20__ г.**
(подпись)

ДИПЛОМНАЯ РАБОТА

На тему: Разработка модели и методики функциональной безопасности программных средств космического назначения

Специальность : 5В074600 - Космическая техника и технологии

Выполнил (а): Ибрагимова М.Р КТТТ-14-1
(Фамилия и инициалы) группа

Научный руководитель: Исмаил Е.Е, к.т.н, профессор
(Фамилия и инициалы, ученая степень, звание)
_____ «05» июня 2018 г.
(подпись)

Рецензент: Инчин К.А.С, к.т.н. доцент.
(Фамилия и инициалы, ученая степень, звание)
_____ «5» июня 2018 г.
(подпись)

Нормоконтролер: Ашпбаев К.А., PhD
(Фамилия и инициалы, ученая степень, звание)
_____ «5» июня 2018 г.
(подпись)

Консультанты:

по экономической части:
Аренбаева Ж.Г., к.э.н, профессор
(Фамилия и инициалы, ученая степень, звание)
_____ «5» июня 2018 г.
(подпись)

по безопасности жизнедеятельности:
Бекбасаров Ш.Ш, д.т.н, старший преподаватель
(Фамилия и инициалы, ученая степень, звание)
_____ «28» мая 2018 г.
(подпись)

Алматы 2018 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Институт Космической инженерии и телекоммуникации
Специальность Космическая техника и технологии
Кафедра 5В074600 Космическая техника и технология

ЗАДАНИЕ

на выполнение дипломная работа

Студент Ибрагимова Мунира Рустамовна
(фамилия, имя, отчество)

Тема работы Разработка модели и методики функциональной безопасности программных средств космического назначения

утверждена приказом по университету № 199 от «27» 12 2017 г.

Срок сдачи законченной работы «06» июня 2018 г.

Исходные данные к работе (требуемые параметры результатов проектирования (исследования) и исходные данные объекта)

Разработка модели функциональной безопасности для программных средств космического назначения
Разработка модели оценки функциональной безопасности программных средств космического назначения
Разработка методики выполнения оценки функциональной безопасности программных средств космического назначения.

Перечень вопросов, подлежащих разработке в дипломной работе, или краткое содержание дипломной работы:

1) Анализ особенностей разработка требований к оценке функциональной безопасности программных средств космического назначения
2) Разработка модели оценки функциональной безопасности программных средств космического назначения
3) Разработка методики оценки функциональной безопасности программных средств космического назначения.
4) Выбор методов оценки функциональной безопасности программных средств космического назначения.
5) Принципы оценки экономической эффективности программных средств
6) Охрана труда и техника безопасности на рабочем месте.

Перечень графического материала (с точным указанием обязательных чертежей)

1. Анализ особенностей и разработка требований к оценке функциональной безопасности ПСКН
2. Разработка модели функциональной безопасности для ПСКН
3. Разработки методики оценки функциональной безопасности ПСКН
4. Разработки методики выполнения оценки функциональной безопасности ПСКН

Рекомендуемая основная литература

1. ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств.
2. Исмаил Е.Е. Характеристики качества программных средств космического назначения: монография. Saarbrücken: Изд-во LAP LAMBERT Academic Publishing, 2015-213с. ISBN: 978-3-659-79520-6
3. Липаев В.В., Экономика производства сложных программных продуктов - М.: 2008.
4. Липаев В.В. Выбор и оценивание характеристик качества программных средств. Методы и стандарты. - М.: 2001.

Консультанты по работе с указанием относящихся к ним разделов

Раздел	Консультант	Сроки	Подпись
БЖД	Бекбасаров Ш.Ш.	25.05.2018	
Экономическая часть	Аренбаева М.Т	25.05.2018	
Рецензия	Инчин А.С	01.06.2018	
Нормоконтроль	Амирбаев Ж.А	01.06.2018	
Основная часть	Исмаил Е.Е	03.06.2018	

Г Р А Ф И К
подготовки дипломной работы

№ п/п	Наименование разделов, перечень разрабатываемых вопросов	Сроки представления руководителю	Примечание
1	Введение	25.01.2018	
2	Анализ особенностей разработка требований к оценке функциональной безопасности ПСКН	25.01.2018.	
3	Разработка модели оценки функциональной безопасности ПСКН	22.03.2018	
4	Разработка методики оценки функциональной безопасности ПСКН	28.03.2018	
5	Экономическая часть	16.05.2018	
6	Основы безопасности жизнедеятельности	16.05.2018	
7	Заключение	18.05.2018	

Дата выдачи задания «____»_____20___ г.

Заведующий кафедрой _____ _____
(подпись) (Фамилия и инициалы)

Руководитель _____ Иванов Е.Е
(подпись) (Фамилия и инициалы)

Задание принял к исполнению

_____ _____
(подпись студента) (Фамилия и инициалы)

Аннотация

Данная дипломная работа выполненна на актуальная тема: «Разработка модели и методики оценки функциональной безопасности программных средств космического назначения». Тема основывается тем фактом и сложностям объектов, ракетно-космической техники и обусловлена многообразием решаемых ими задач научного, социально-экономического и оборонного характера. Основная цель дипломная работа — это разработка методов оценки функциональной безопасности программных средств космического назначения-выполнено.

Аңдатпа

Дипломдық жұмыс «Ғарыш саласына арналған бағдарламалық құралдарының функционалдық қаупсіздігін бағалау модель мен әдістемесін әзірлеу» тақырыбына байланысты атқарылган.Атқарылған жұмыс қазіргі уақытта күрделі ғарыштық-зымырандық құрылғыларға техникалық есептеулер мен алға койылған міндеттерді ғылыми, әлеуметті-экономикалық және қорғаныс мінездемелері тұрғысына сәйкестендіріліп көп салалалы бағыттарға негізделген. Дипломдық жұмыстың негізгі мақсаты бұл құрылғылардың тексеру әдістерін анықтау болды. Ал алға қойылған мақсат орындалған.

Annotation

This thesis works is carried out on the current topic: «Development of a model and of a technique for evaluating the functional safety of software for space purposes». The theme is based on the facts and complexities of objects, rockets and spaces technology and is caused by the variety of scientifics, socioeconomics and defensives tasks they solve. The main purpose of the thesis work is the development of methods for assessing the quality of software for space applications-performed.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....8
1 Анализ особенностей и разработка требований к оценке функциональной безопасности ПСКН.....10
1.1 Проблемы обеспечения функциональной безопасности программных средств.....14
1.2 Анализ факторов, определяющих функциональную безопасность программных средств 18
1.3 Общие требования к оценке функциональной безопасности ПСКН 20
1.4 Основные задачи оценки функциональной безопасности ПСКН.....24
2. Разработка модели оценки функциональной безопасности ПСКН.....27
2.1 Разработка модели функциональной безопасности для ПСКН 28
2.2 Разработка модели оценки функциональной безопасности ПСКН...31
2.3 Основные процедуры оценки функциональной безопасности ПСКН 32
3. Разработка методики оценки функциональной безопасности ПСКН .34
3.1 Выбор методов оценки функциональной безопасности ПСКН.....35
3.2 Разработка требований к функциональной безопасности ПСКН.....37
3.3 Разработка методики выполнения оценки функциональной безопасности ПСКН.....39
4. Экономический раздел 41
4.1. Принципы оценки экономической эффективности программных средств.....41
4.2 Основные показатели экономической эффективности программных средств.....41
4.3 Анализ и расчет затрат на разработку ПСКН 42
5 Безопасность жизнедеятельности.....48
5.1 Охрана труда и техника безопасности на рабочем месте.....48
5.2 Техника безопасности при работе с электрическими приборами 51
5.3 Расчет искусственного освещения 52
5.3 Пожарная безопасность.....55
ЗАКЛЮЧЕНИЕ 59
Список использованных источников 61

ВВЕДЕНИЕ

Понятия и характеристики функциональной безопасности систем близки к понятиям надежности, поэтому далее в тексте для сокращения, часто под термином «функциональная безопасность» будет подразумеваться и «надежность». Основное различие состоит в том, что в показателях надежности учитываются все реализации опасных отказов, а в характеристиках функциональной безопасности регистрируются и учитываются только те отказы, которые привели к столь большому или катастрофическому ущербу, который отразился на безопасности системы и информации для потребителей. Статистически таких отказов может быть в несколько раз меньше, чем учитываемых в значениях надежности. Однако методы, влияющие факторы и реальные значения показателей надежности ПП могут служить ориентирами при оценке функциональной безопасности критических систем. Поэтому способы оценки и испытаний функциональной безопасности, могут базироваться на методах, определения надежности функционирования комплексов программ и баз данных.

Любое программное обеспечение, в первую очередь, должно отражать основную цель их жизненного цикла в проекте, его экономическую, техническую, научную или социальную эффективность. Эту эффективность системы можно охарактеризовать как количественную или качественную, как набор полезных функций и особенностей ПК, других существующих программных комплексов, их отличий, а также эффективности и потенциальных источников факторов. В результате он должен быть как структурированным, так и вспомогательным, а также целью и целым рядом целевых применений и потребителей, а также целью набора пользователей.

Эффективность системы программного приложения определяется уровнем удовлетворения потребностей отдельных лиц - потребителей и потребителей, которые часто измеряются по экономическим категориям: затраты, затраты на рабочую силу, ранее существовавшие расходы и т. Д. Функциональность ПС- это общее резюме эффективности стандартизованных общих качественных характеристик. качество функциональности может быть выполнено и условия, в которых он существенно зависит (в том числе безопасность), и другие структурные характеристики типичны для удовлетворения потребностей пользователя и ПС. С этим связаны задачи.

Номенклатура и значения всех показателей качества дизайна определяются основными функциями программного обеспечения и в определенной степени влияют на выполнение этих функций. Таким образом, выбор и дизайн функциональной достоверности ПС, подробное и правильное описание его свойств являются исходными исходными данными для обозначения требуемого качества всех стандартизованных стандартов.

Цель дипломной работы состоит в разработке методики и модели функциональной безопасности программных средств космического назначения.

Объектом исследования данной работы являются программные средства космического назначения.

Для достижения цели работы поставлены следующие задачи:

1.Изучение предметной области ПСКН;

2.Рассмотреть основные требования к оценке функциональной безопасности ПСКН;

3.Провести анализ методов оценки функциональной безопасности ПСКН;

4.Выбрать и обосновать методы оценки функциональной безопасности ПСКН;

5.Сделать выводы;

Теоретической базой для дипломной работы является литература по проектированию, реализации и управлению программными средствами, нормативно-правовые документы, учебная и периодическая литература.

1 Анализ особенностей и разработка требований к оценке функциональной безопасности ПСКН

Обязательные требования к продукции, производству и эксплуатации определены Законом РК «О техническом регулировании». В нем, в частности, введено понятие безопасности продукции – «состояние, при котором отсутствует недопустимый риск (вероятность) связанный с причинением вреда жизни и здоровью граждан, имуществу физических и юридических лиц, государственному или муниципальному имуществу, окружающей среде...». Вот основные понятия: технические регламенты, техническое регулирование, стандартизация, сертификация, сертификация, аккредитация, оценка соответствия и т.д., А также их цель, принципы и процедуры для их практического применения.

В статье представлены системы обработки информации и управления в реальном времени, а также программное обеспечение (ПС) и базы данных баз данных (ЭВМ), все из которых рассматриваются и учитываются с точки зрения безопасности, электронных компьютеров (компьютеров). Кроме того, безопасность продукции, производственные процессы и функционирование системы зависят от условий их эксплуатации и требований заказчика и технической документации из-за небезопасных отказов и неблагоприятных последствий.

В критических системах, в которых результаты обработки информации и контрольные действия напрямую определяют работоспособность и качество функционирования сложных систем управления в чрезвычайных ситуациях, системы оружия, космические объекты, аварии и катастрофы не являются редкостью из-за недостаточной безопасности программного обеспечения. Существует множество примеров смерти дорогостоящих спутников или катастрофических ситуаций с использованием сложных динамических объектов (Марс-1-1976, Ариан-5-1997, Апполон-13-1978 и т. Д.), А также больших финансовых и материальных потерь в авиации , в военных системах и на транспорте из-за относительно простых ошибок в программах. В наиболее тяжелых случаях ущерб был измерен стоимостью жизни и здоровьем людей или большими материальными потерями. В то же время у них был вполне объяснимый характер и источники, влияние которых можно было бы сократить путем углубленного анализа, выявления дефектов и исправлений программ или информации базы данных.

Существующие достижения в области теории и практики управления безопасностью сложных промышленных продуктов, как правило, неизвестны и не используются специалистами, которые создают и используют военные системы на основе программного обеспечения. Это во многих случаях определяет недостатки и сбои в применении ПС, конфликты между клиентами и разработчиками из-за неопределенности их ценностей безопасности и

конкурентоспособности создаваемых ПС на мировом рынке. Формализация и оценка реальной безопасности программного обеспечения и систем часто зависит от интуиции и умения их разработчиков, клиентов и пользователей. В результате проекты ПС не соответствуют первоначальному, заявленному обозначению и первоначальным спецификациям требований к характеристикам безопасности и качества, не вписываются в согласованные графики и бюджет развития.

В требованиях технических заданий и реализованных проектах сложных систем и ПС, связанных с безопасностью, систематически умалчиваются и/или недостаточно формализуются понятия и метрики безопасности программного продукта и выдаваемой информации, какими характеристиками они должны описываться, как их следует измерять и сравнивать с требованиями, отраженными в контракте, техническом задании или спецификациях. Кроме того, некоторые из характеристик функциональной безопасности часто вообще отсутствуют в требованиях заказчика и согласованных документах на систему и ПС, что приводит к произвольному их учету или к пропуску при испытаниях. Этому способствует ограниченность ресурсов, необходимых для достижения и оценивания в процессах жизненного цикла комплексов программ, требуемых и реализованных значений безопасности, а также недостаточная формализация и документирование всего процесса их выбора и анализа. Непрерывно возрастающая сложность и вследствие этого уязвимость систем и ПС от случайных и предумышленных негативных воздействий выдвинули ряд рассматриваемых ниже проблем, связанных с безопасностью систем, использующих программные средства, в разряд важнейших–стратегических, определяющих принципиальную возможность и эффективность их применения. При этом выделились области анализа и обеспечения информационной безопасности, связанные, в основном, с защитой от предумышленных, негативных воздействий на информационные ресурсы систем, и функциональной безопасности, обусловленной отказовыми ситуациями и потерей работоспособности систем и ПС вследствие проявления непредумышленных, случайных дефектов программ, данных, аппаратуры и внешней среды. Проблема обеспечения информационной безопасности функционирования ИС в процессе разработки и эксплуатации возникла и развивается вследствие возрастания сложности и ответственности задач использования информационных ресурсов и увеличения их уязвимости от предумышленных, внешних воздействий, с целью незаконного использования или искажения информации и программ, которые по своему содержанию предназначены для применения ограниченным кругом лиц.

В требованиях технических задач и реализованных проектов сложных систем и ПС, связанных с безопасностью, концепции и показатели безопасности программного продукта и раскрываемой информации систематически скрыты или недостаточно формализованы, какие характеристики они должны описывать, как они должны быть измеряется и

сравнивается с требованиями, отраженными в контракте, круге ведения или спецификациях. Кроме того, некоторые функциональные функции безопасности часто не доступны вообще в соответствии с требованиями заказчика и согласованными документами для системы и ПС, что приводит к их произвольной записи или к пропуску в тестах. Этому способствуют ограниченные ресурсы, необходимые для достижения и оценки жизненного цикла программных комплексов, требуемые и внедренные значения безопасности, а также отсутствие формализации и документирования всего процесса их отбора и анализа. Постоянно возрастающая сложность и, как следствие, уязвимость систем и ПС от случайных и преднамеренных негативных влияний выдвинула ряд проблем, рассмотренных ниже, связанных с безопасностью систем, использующих программное обеспечение, в категорию наиболее важных- стратегических, определяющих принципиальная возможность и эффективность их применения. В то же время были выявлены области анализа и информационной безопасности, в основном связанные с защитой от преднамеренных негативных воздействий на информационные ресурсы систем и функциональная безопасность, вызванная сбоями и потерей эффективности систем и ПС в связи с появлением непреднамеренных , случайные дефекты программ, данных, оборудования и окружающей среды. Проблема обеспечения информационной безопасности функционирования ИС в процессе развития и эксплуатации возникла и развивается из-за все возрастающей сложности и ответственности за задачи использования информационных ресурсов и повышения их уязвимости от преднамеренных внешних воздействий для целей злоупотребления или искажения информации и программ, которые предназначены для их использования ограниченным кругом лиц.

Основное внимание в современной теории и практике средств безопасности информационных систем сосредоточено на защите от вредоносного уничтожения, искажения, кражи и использования программных средств и информации о базе данных. Для этого разработаны и активно развиваются проблемно-ориентированные методы и средства защиты от несанкционированного доступа, от различных типов вирусов и закладок, от утечки информации по каналам электромагнитного излучения и т.д. Это подразумевает присутствие лиц, заинтересованных в несанкционированном доступе к конфиденциальной или полезной информации в системах с целью ее незаконного использования. Для решения этой проблемы были созданы и активно развиваются методы, инструменты и стандарты обеспечения информационной безопасности - защита программ и данных от преднамеренных негативных внешних воздействий. Проблема обеспечения функциональной безопасности в случае случайных, дестабилизирующих воздействий и отсутствия вредоносного воздействия на системы, ПС или базы данных существенно отличается от задач информационной безопасности. При анализе функциональной безопасности учитываются опасные сбои, приводящие к потере работоспособности системы, несчастным случаям и

катастрофам. При таких влияниях внешняя функциональная емкость систем не может быть полностью разрушена, но полная реализация указанных функций и требований к качеству информации для потребителей невозможна. В системах, рассмотренных ниже, безопасность их функционирования определяется проявлениями дестабилизирующих факторов, которые наносят большой ущерб:

•технические сбои внешнего оборудования и искажения исходной информации от объектов внешней среды и от пользователей систем и обрабатываемой информации;

•случайные сбои, сбои и физическое уничтожение аппаратных компонентов и компонентов компьютерных систем и средств связи;

•дефекты и ошибки в комплексах программ и данных обработки информации;

•пробелы и недостатки в средствах для обнаружения опасных сбоев и быстрого восстановления рабочего состояния систем, программ и данных.

В реальных сложных системах, связанных с безопасностью, катастрофические последствия и сбои в работе с большим ущербом возможны в отсутствие враждебных лиц, заинтересованных в таких нарушениях работоспособности систем и подстанций. Пагубные и катастрофические последствия таких отказов в ряде областей применения систем могут превышать результаты злонамеренных эффектов от результатов, иметь их собственный характер, характеристики и характеристики. Поэтому они требуют самостоятельного изучения и адекватных методов и средств обеспечения безопасности. В некоторых системах отказы, влияющие на функциональную безопасность, могут быть вызваны нарушением информационной безопасности, преднамеренным уничтожением или искажением информации в базах данных. Тщательная спецификация и оценка функциональной безопасности систем, программных продуктов и информации, обрабатываемой для потребителей, являются ключевым фактором обеспечения их эффективного и адекватного использования. Это может быть достигнуто путем выявления, идентификации и предоставления соответствующих характеристик с учетом целей использования и функциональных задач ПС и систем. При анализе характеристик функциональной безопасности целесообразно различать два класса систем и их ПС. Первый класс состоит из систем, которые имеют встроенные сложные программы жестких правил реального времени, автоматизированного управления внешними объектами или процессами. Время, необходимое для реагирования на ситуации сбоя таких систем, обычно рассчитывается в секундах или доли секунды, а процессы восстановления должны быть в достаточной степени автоматизированы в течение этого времени (бортовые системы в авиации, в некоторых видах оружия и транспортных средствах).

Системы второго класса используются для управления процессами и обработки бизнес-информации из внешней среды, в которой активно участвуют специалисты (административные, банковские, кадровые военные

системы). Допустимое время отклика на опасные сбои в этих системах может быть минутным, а операции восстановления могут быть доверены администраторам безопасности.

1.1 Проблемы обеспечения функциональной безопасности программных средств

Концепции и характеристики функциональной безопасности систем близки к понятиям надежности. Основное различие заключается в том, что индексы надежности учитывают все реализации опасных сбоев и в характеристиках функциональной безопасности, должны регистрироваться и учитываться только эти сбои, что привело к столь большому катастрофическому ущербу, который повлиял на безопасность системы , информация для потребителей или объектов управления. По статистике, такие отказы могут быть в несколько раз меньше, чем те, которые считаются значениями надежности. Тем не менее, методы, влияющие на факторы и реальные значения показателей надежности ПС могут служить ориентиром при оценке функциональной безопасности критических систем. Поэтому методы оценки и тестирования функциональной безопасности могут быть основаны на концепции измерения надежности функционирования программных комплексов и база данных.

Ущерб от дефектов и ошибок в программах и данных может быть кумулятивным и проявляться в систематических сбоях, каждый из которых влияет на надежность, но не является катастрофой с большим ущербом, который влияет на безопасность системы. Накопление таких сбоев с течением времени может привести к последствиям, которые нарушают функциональную безопасность систем и их применение. Таким образом, понятия надежности и функциональной безопасности сложных систем и подстанций сходятся. С более или менее одинаковыми источниками угроз и их проявлениями эти концепции можно разделить на величину последствий и ущерба в случае сбоев. Проблемы неопределенности в концепции функциональной безопасности конкретных систем, включая программное обеспечение, должны учитываться клиентами, пользователями и разработчиками на протяжении всего их жизненного цикла. Чем сложнее система и чем выше требования безопасности, тем более неопределенны функции и характеристики их безопасности и качества. Неопределенности начинаются с требований клиентов, которые при формулировании технических условий и спецификаций не полностью формализуют и в принципе не могут обеспечить содержание всего набора функций, характеристик и их значений безопасности, которые должны быть в конце проекта и презентации конечного продукта для клиента. Эти требования итеративно формируются, детализируются и уточняются по соглашению между всеми участниками проекта из-за естественных ограничений данных

первичного источника и их изменений под воздействием объективных и субъективных влияний различных процессов на последующих этапах ЖЦ.

Всегда не полностью, с необходимой детализацией определены и описаны все характеристики, особенности функционирования и безопасности объектов внешней среды. Эти характеристики в той или иной степени обычно находятся под воздействием управляемой системы и ПС. Сложность, а поэтому и неопределенность их представления, как правило, адекватны сложности всей системы, функциональная безопасность которой должна обеспечиваться в течение ее ЖЦ. Квалификация и субъективные свойства потребителей и пользователей изменяются по мере освоения функциональных возможностей системы и ее работоспособности, что увеличивает неопределенность ее реальной безопасности. Смена и различия персонала, применяющего систему и ПС, дополнительно увеличивает неопределенность значений безопасности и трудности ее прогнозирования с учетом множества субъективных факторов различных специалистов, участвующих в эксплуатации. В процессе проектирования, разработки и всего жизненного цикла основных функциональных задач, операционной среды, аппаратуры ЭВМ эти компоненты с течением времени развиваются и адаптируются, что отражается на необходимости адекватного изменения методов, задач и средств обеспечения их функциональной безопасности. Таким образом, проблемы обеспечения функциональной безопасности сложных систем должны решаться с учетом одновременного динамического развития всех компонентов среды и факторов, непрерывно изменяющихся и воздействующих на результаты их решения. Однако такой сложный, непрерывный, многосвязный процесс трудно реализовать практически и его целесообразно решать поэтапно, возможно с необходимыми итерациями и упрощениями. При этом следует иметь в виду, что всегда могут проявиться отдаленные связи процессов, которые могут существенно повлиять на текущие работы по обеспечению безопасности системы и ПС.

Роль негативных воздействий и их разрушительных последствий быстро возрастает из-за возрастающей сложности разработки и применения современных компьютерных систем и ответственности за решаемые ими задачи. В то же время сложность внешней и операционной среды, в которой функционируют ПС, и ответственность систем, связанных с безопасностью, возрастают. Объективное увеличение сложности реализованных функций в современных системах напрямую приводит к увеличению их объема и сложности создания. Соответственно, увеличение сложности программ увеличивает относительное и абсолютное количество обнаруженных и оставшихся дефектов, что отражается на снижении потенциальной безопасности их функционирования. По мере увеличения сложности задач, решаемых программами, возрастает влияние ошибок, которые могут угрожать катастрофам и катастрофам в системах, выполняющих критические функции управления большими, дорогими и особенно важными объектами или процессами. Упорядоченное, регулируемое проектирование архитектуры,

разработка и обслуживание комплексных подстанций на основе современных технологий позволяет предотвращать и устранять наиболее опасные системы, алгоритмические и программные дефекты и ошибки на ранних этапах жизненного цикла, а также использовать безопасные программные и информационные компоненты, которые неоднократно тестировались в других проектах. Для обеспечения безопасности критических систем необходимы эффективные методы и средства для предотвращения и обнаружения дефектов, а также для подтверждения безопасности использования программ и баз данных, которые быстро защищают их правильное функционирование в случае каких-либо дефектов и сбоев.

Возможности ПС могут быть предоставлены исходными данными, которые используются для их разработки, коррекции и тестирования. Фактические исходные данные могут содержать значения, которые отличаются от спецификаций и приложений и баз данных, используемых во время использования. При таких исходных данных трудно предсказать работу ПС и различные отклонения, которые могут привести к небезопасным сбоям безопасности. Необходимо учитывать основные трудности аналитической оценки и прогнозирования значений функциональной безопасности программного обеспечения, что является проявлением и следствием ошибок программы и данных и ошибок. Это приведет к практическому сбою априорных аналитических вычислений для функциональной безопасности программных комплексов.

Проблема доступа к основным функциональным системам безопасности с программным обеспечением реального времени решается с использованием современных регулируемых технологических процессов и инструментов для обеспечения их жизненного цикла. Они поддерживаются группой международных стандартов, которые определяют состав и процессы удовлетворения требований по функциональной безопасности систем и подстанций. Структуры, последовательности и содержание процессов процесса ЖЦ в этих стандартах широко варьируются, но основные компоненты позволяют выбирать и использовать проекты ПС, соответствующие конкретным функциям безопасности.

Для систематической, скоординированной борьбы с угрозами безопасности ПС необходимо изучить факторы, которые влияют на функциональную безопасность случайных дефектов и ошибок, существующих и потенциально возможных в конкретных системах и программных комплексах. Это позволит целенаправленно разрабатывать методы и средства обеспечения функциональной безопасности критических ПС для различных целей с реалистичным снижением уровня дефектов проектирования и разработки. Проблема в значительной степени решена путем применения современных методов, инструментов и стандартов, которые поддерживают системный анализ, разработку технологий, разработку и обслуживание систем, их программных средств и баз данных.

Прежде всего, для создания защищенных систем и ПС, их назначение, функции и основные характеристики должны быть формализованы. Исходя из этого, должны быть разработаны общие требования к функциональной безопасности и другие характеристики качества ПС, для обработки информации для потребителей, адекватных функций и функций систем. Требования к функциям систем и ПС, а также безопасность их функционирования должны соответствовать доступным ресурсам для их реализации с учетом допустимого ущерба - рисков, связанных с отказами, когда требования не выполняются в полном объеме. Ограниченность ресурсов различных типов для обеспечения функциональной безопасности существенно влияет на технико-экономические показатели, качество и функциональную безопасность всей системы и подстанции. В результате сложность программ и баз данных, а также имеющихся ресурсов для их реализации становятся косвенными критериями или факторами, которые влияют на выбор методов развития, достигнутое качество и безопасность ПС.

Для обеспечения безопасности ПС и полученной информации для потребителей необходимо осваивать и применять современные методы, автоматизированные технологии и инструменты, которые предотвращают или устраняют большинство типов дефектов и ошибок при создании и модификации подстанций и их компонентов, которые обеспечивают безопасность. Все этапы разработки и сопровождения ПС должны поддерживаться методами и средствами проверки и систематического, автоматизированного тестирования модулей и программных компонентов. Тестирование является основным методом устранения дефектов, измерения и определения реальных характеристик программ на любом этапе их жизненного цикла. Наличие достаточно полных стандартов на основе набора требований спецификаций и их поэтапного разложения является необходимой основой для тестирования и измерения реальной безопасности и качества программных комплексов. Ограниченные ресурсы при создании ПС приводят к целесообразности тщательного планирования, оптимизации и применения экономичных и эффективных методов автоматизации пошаговых испытаний в ЖЦ ПС для обеспечения требуемой функциональной безопасности и надежности его определение.

Разработка систем и ПС должна завершать комплексные испытания и сертификацию достигнутой функциональной безопасности и надежности программных систем, обеспечивающих возможность улучшения их характеристик с помощью соответствующих программных корректировок. Повышение функциональной безопасности рекомендуется путем внедрения процедур анализа выявленных дефектов и оперативного восстановления вычислительного процесса, программ и данных (перезапуска) после обнаружения аномалий и сбоев в работе ПС. Этому может способствовать накопление, мониторинг и хранение данных об обнаруженных дефектах, сбоях и сбоях в процессе выполнения программы и обработки данных.

1.2 Анализ факторов, определяющих функциональную безопасность программных средств

Любое программное обеспечение, в первую очередь, должно отражать основную цель их жизненного цикла в проекте, его экономическую, техническую, научную или социальную эффективность. Эффективность этой системы - это набор полезных функций и функций ПК, которые доступны для других программных систем, а также потенциальные источники факторов и эффективности могут быть количественными или качественными. В результате он должен быть отформатирован, создан или приобретен ПС, с требованиями и целями клиента, а также с целью и объемом. Эффективность программного обеспечения системы определяется тем, в какой степени удовлетворены потребности определенных лиц - во многих случаях это оценивается по экономическим категориям, клиентам или пользователям. Прибыль, затраты, труд, вредная профилактика, продолжительность и т. д. Эта эффективность отражена в стандартах, общем описании функционального фитнес-качества ПС.

Эти ПС, а также эти функции могут выполняться в желаемом качестве, в основном в зависимости от того, что (кроме безопасности) других структурных характеристик, но также и для решения потребностей пользователей в зависимости от их функций и задач. Номенклатура и значения всех показателей качества дизайна определяются основными функциями программного обеспечения и в определенной степени влияют на выполнение этих функций. Поэтому выбор и функциональность дизайна ПС, подробное описание и его свойства являются ключевым сырьем, необходимым для обозначения всех других параметров стандартизованного стандартного дизайна.

Стандартизованные, качественные характеристики ПК стандарта ISO 9126 различаются по степени эффективности использования пакетов программного обеспечения для программных целей. Верховные ценности, безусловно, обязаны присваиваться свойствам и атрибутам многофункциональной годности, важным с целью свершения главных хитрых полнее применения ПС.

В современных проектах ПС готовые компоненты других подобных разработок, прототипов и пакетов приложений составляют большую или меньшую долю. Это значительно ускорит вашу работу и уменьшит стоимость создания сложных пакетов программного обеспечения. Вспомогательные разработчики часто являются дилеммой проекта: адаптация, абсолютно новые детали или использование программ безопасности (в том числе безопасности) и компонентов полки для портных (сколько и сколько). В результате при первоначальном экономическом анализе затрат на создание ПС с требуемыми функциями безопасности рекомендуется рассмотреть два альтернативных варианта определения стоимости затрат на разработку:

• Нет подходящих или подходящих компонентов для ПС - прототипов и бесполезного использования;

• Программное обеспечение, основанное на интеграции почти полного набора готовых программных компонентов и информации о базе данных, которые вам не нужны для создания новых компонентов.

При компиляции новой сборки ПС из компонентов некоторым из них может потребоваться создание специальных программ для очистки или взаимодействия с ними. До 80-90% готовых компонентов можно сократить до 3-5 раз в общей сложности на новом ПК. В этом случае, помимо 10-20% новых программных компонентов, необходимы ресурсы для интеграции нового ПС, его квалификационных тестов, тестирования и документации.

При создании выборочных тестов требуются не только тестовые тесты, системы безопасности и системы оценки качества, но и их комплексная отладка.

Поэтому затраты на программные тренажеры и их экономическую эффективность следует учитывать с учетом всего комплекса задач, которые они могут и должны решать в ЖЦ ПС.

Расходы на программное моделирование тестовых данных определяются ресурсами, необходимыми для проектирования и эксплуатации сложных программных пакетов для этих целей, и следующие компоненты:

•затраты на разработку набора программ для имитации информации о внешних объектах и окружающей среды для их эксплуатации;

•затраты на эксплуатацию программ моделирования во время тестирования, тестирования и определения характеристик безопасности и качества испытания ЖЦ;

•Стоимость начальной установки и работы компьютерного моделирования и вспомогательного оборудования, используемого в симуляторе.

Затраты на запуск программ моделирования в основном определяются продолжительностью тестирования, тестирования и измерения характеристик безопасности и качества ПС.

Значения этого времени соответствуют фактическому времени генерации тестовых данных и тестированию программ. Обычно симуляторы используются для тестирования нескольких ПС разных, но близких целей. В результате затраты подразделения на их создание и эксплуатацию быстро снижаются с унификацией имитаторов и расширением сферы их применения для тестирования и оценки качества большого количества подстанций, имеющих тесную функциональную цель. Даже приблизительные оценки этих затрат в большинстве случаев показывают высокую рентабельность программных симуляторов внешней среды, особенно для квалификационных испытаний и оценки характеристик безопасности сложных ПС в реальном времени.

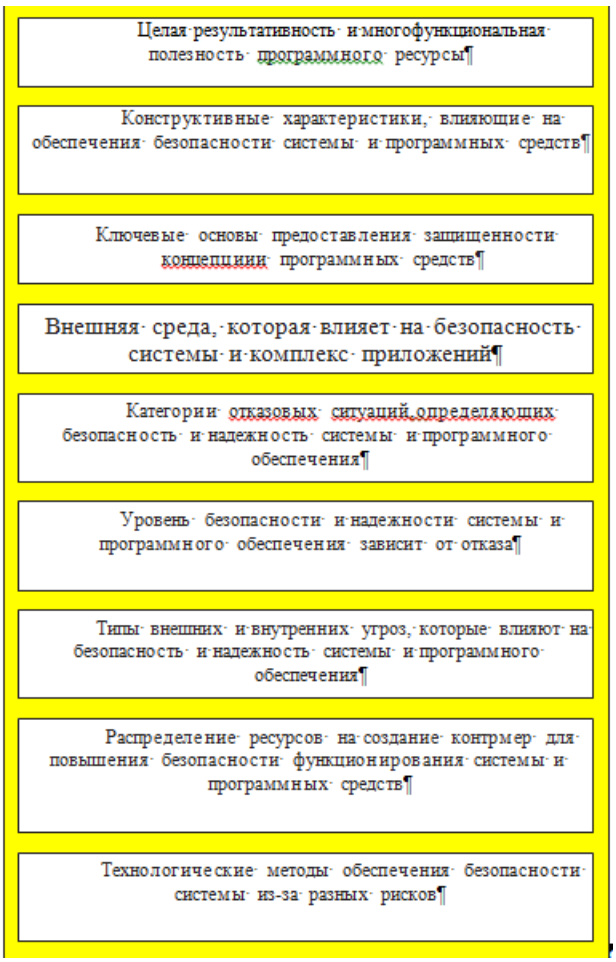

Рисунок-1 показан основной набор факторов и мер для обеспечения функциональной безопасности и систем ПС.

Стандартизованные запасные части все остальные характеристики должны поддерживать тактические цели, выбранные для требований к конструкции. Эти задачи должны быть направлены на обеспечение сбалансированной высокой функциональности ПС путем улучшения свойств структурных характеристик (и безопасности) в контексте ограниченных ресурсов в рамках ЖЦ. С этой целью на основе их эффективности выбираются технические характеристики и характеристики процесса анализа системы, различные факторы, ценности, показатели качества и безопасности. На рисунке 1 показан основной набор факторов и мер для обеспечения функциональной безопасности и систем ПС.

1.3 Общие требования к оценке функциональной безопасности ПСКН

Основные понятия в области функциональной безопасности систем и программного обеспечения характеризуются факторами, связанными с появлением опасных состояний, приводящими к потере эффективности. Если эти события не обнаружены и не устранены специально введенными функциями безопасности в системе, тогда есть опасные сбои и их

последствия. Система, в которую вы хотите ввести функции безопасности, обычно называется системой, связанной с безопасностью. Эти функции необходимы для достижения или поддержания безопасного состояния объекта управления или обработки информации - отдельно или в сочетании с другими системами, связанными с безопасностью, а также с инструментами внешнего смягчения рисков для предотвращения или смягчения последствий опасного события. Примеры включают системы ПС, связанные с безопасностью воздушных судов, системами управления транспортными средствами, электрическими и диспетчерскими системами централизации на железнодорожном транспорте, средствами управления ядерными реакторами и т. Д. Другими словами, любой программный инструмент, отказ которого может повлиять на возникновение чрезвычайной или катастрофической ситуации , последствия которого могут быть тем или иным ущербом, следует рассматривать как связанные с безопасностью. Человек может быть компонентом такой системы, например, получать информацию от программируемого электронного устройства и выполнять действия безопасности на основе этой информации или выполнять действия безопасности с использованием такого устройства.

Термины, используемые далее и связанные с функциональной безопасностью систем и ПС, аналогичны тем, которые содержатся в стандартах ГОСТ 27.002 – 89, IEC 61508, ISO 15408и др. Эти определения базируются на понятии отказа как события, заключающегося в нарушении работоспособного состояния объекта.

Определение отказа является основой для оценки функциональной безопасности и надежности технических систем:

•рабочее состояние- в котором значения всех параметров, характеризующих способность выполнять определенные функции, отвечают требованиям нормативно-технической и проектно-конструкторской документации;

•Нерабочее состояние - в котором значение хотя бы одного параметра, характеризующего способность выполнять указанные функции, не соответствует требованиям нормативной, технической и проектной и проектной документации;

• Сбой ситуации - скрытый сбой, который не может быть обнаружен визуально или рутинными методами и средствами мониторинга и диагностики, но обнаружен с помощью автоматического перезапуска, а также при техническом обслуживании или специальных диагностических методах, которые могут потенциально превратиться в отказ;

• Отказ- событие, связанное с неисправностью системы;

• опасный сбой- событие, состоящее в нарушении работоспособного или защитного состояния с большим ущербом;

• дефекты оборудования, программного обеспечения или данных - негативные события, которые предполагают непреднамеренное отклонение от требований спецификации или документации в их жизненном цикле;

• Ошибки аппаратного обеспечения, программы или данных - случайные, непредсказуемые искажения компонентов или ПС, которые появляются в процессах их анализа или функционирования.

В процессе проектирования в функциональной пригодности можно выделить две группы основных субхарактеристик, которые определяют функциональные и структурные требования и особенности подстанции. При оформлении и выборе функциональных требований можно четко сформулировать в контрактных документах:

•экономические, организационные, технические и социальные стратегические цели всего жизненного цикла системы, ПС и ее компонентов;

•эффективность системы и, в том числе, необходимые технические и экономические показатели применения ПС в системе;

•назначение, внешняя среда, условия для эффективного и безопасного использования ПС;

•функциональные задачи основных компонентов и ПС в целом, а также эффективность системы каждого компонента;

• необходимая и достаточная безопасность применения, качественные характеристики и временные рамки для решения каждой функциональной задачи;

• соответствие ПС и ее компонентов установленным стандартам и нормативным документам для проектирования и применения.

В зависимости от цели ПС функциональная безопасность и некоторые конструктивные характеристики могут стать доминирующей или даже почти полностью определять функциональную пригодность ПС. В большинстве случаев функциональная пригодность во многих случаях зависит от функциональной безопасности, правильности и надежности ПС. Эти характеристики трудно свести к количественным мерам, и часто их необходимо оценивать по наличию свойств и ряда стандартных процедур в ПС или по количеству необходимых ресурсов, которые существенно влияют на функциональную пригодность.

Правильность - способность доставлять правильные или приемлемые результаты пользователям ПС. Стандартами выбора стандартов корректности проектирования могут быть следующие: требования совместимости и особенности комплекса, функции компонентов и программных модулей, а также их структура структуры, взаимодействие и организация правил интерфейса. Требования к разработке ПС должны использоваться как стандарт от высокого модуля, к правильности соответствующих компонентов. Эта концепция обеспечивает справочные (ожидаемые) данные с требуемой точностью рассчитанных значений в соответствии с требованиями спецификаций и спецификаций. Проектирование и разработка программных модулей и макетов использует конкретные структурные критерии для правильности структуры программы, обработки данных и наличия межмодульных интерфейсов. Каждый из полуфинальных критериев может быть охарактеризован несколькими методами измерения качества и степенью

надежности реализованных программ: детерминированным , Стохастическим или в режиме реального времени.

Точные описательные требования могут быть представлены в описании двух основных характеристик, которые должны соответствовать всем программным компонентам и обычно ПС. Первое-характеристики компонентов программного обеспечения требует последовательного исполнения деталей и технических характеристик и проверку вплоть до определенной степени (%), осуществления программ.

Второе требование - выбор стратегий и стратегий использования компонентов ПС, набора программных компонентов и функций, набора маршрутов для выполнения модулей и набора программ для последующего тестирования и тестирования. Необходимое качество и точность результатов по конкретным ограничениям ресурсов. Чтобы определить это значение, нет необходимости регулярно проходить регистрацию для разработки СС, сбора имен, содержания тестируемых программ и маршрутов выполнения, а также мониторинга их общего доступа. Размер выбранной коррекции может быть относительным числом функций и маршрутов для проверки, которые могут быть измерены как процент от общего количества исполняемых файлов. Как показывает опыт, чаще всего, комплекс ПС готовых функции и проверенные маршруты около 50-70% и 90-95%, очень трудно оценить. Для косвенных, специальных автоматики и профессионалов это значение указывает на твердость и длительность теста, что напрямую влияет на функциональность ПС.

Большинство систем безопасности пострадали и потерпели неудачу, поскольку разработчики и клиенты не имеют четкого представления о фактических финансовых, трудовых, временных и других ресурсах, необходимых для реализации контракта. Таким образом, конструкция функциональной безопасности задач подстанции и технического обслуживания в соответствии с требованиями контракта является одной из главных задач всех СС и определить экономические ресурсы, необходимые для создания ЦА.

При планировании проектов ПС разработчик часто является разработчиком, разработчик-разработчик самостоятельно принимает все дизайнерские решения за счет своих ресурсов и рекомендует возместить затраты при покупке рынка. В других случаях существует конкретный потребитель-клиент, который может устанавливать ключевые цели, качество и функции безопасности и предоставлять ресурсы для проекта. Таким образом, существует два сценария экономической целесообразности проектов ПС и их функциональной безопасности:

•разработчик и пакет программного обеспечения и использование разработчика баз данных на протяжении всего жизненного цикла различных секторов заказчика уже давно известен потребителям для выявления и распространения рыночного управления и внешнего заказчик-клиент

массового не является приоритетом для безопасности ПСА и его определяет и устанавливает основные требования, и финансирует проект;

•разработка проекта ПС или БД и его безопасность для разработчика-поставщика для конкретного клиента-использование определенных количеств и определенных ограниченных количеств результатов разработки для клиента, который устанавливает все требования.

1.4 Основные задачи оценки функциональной безопасности ПСКН

Для оценивания свойств функциональной безопасности и надежности систем и ПС необходимо регистрировать,измерять, обобщать и упорядочивать реальные характеристики отказовых ситуаций и их последствия для безопасности.

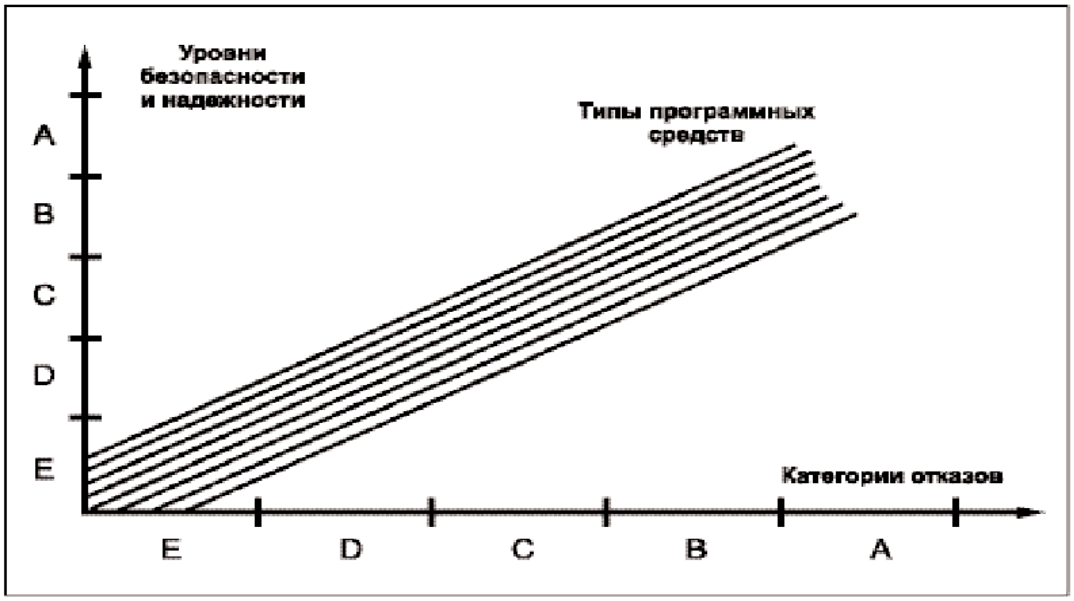

Рис. 2

Рисунок-2.Стандартом установлена следующая классификация отказовых ситуаций.

С этой целью в стандарте ГОСТ Р 51904рекомендуются категории отказовых ситуаций систем и ПС, в зависимости от серьезности их влияния на качество функционирования программ или данных объекта управления. Необходимый для безопасного функционирования уровень качества ПС рекомендуется определять исходя из опасности отказовых ситуаций и возможного при этом ущерба для программ, системы и потребителя. Стандартом установлена следующая классификация отказовых ситуаций (рис. 2)

В соответствии с этим стандартом стандарт СТ Р 51904 входит в категорию открытых системных систем и ПС в зависимости от их функциональности и функциональности управления программой управления объектами. Необеспеченная функция безопасности рекомендуется для явного

и явного выполнения программных, системных и пользовательских потребностей. Следующая классификация корзины (рис. 2) устанавливает стандарт:

•Категория А-Бедствие: Предотвращение несчастных случаев, неблагоприятных последствий, а также системы или пользователей, чтобы предотвратить полное функционирование и функционирование системы или MS, совместимых с требованиями и размером ущерба;

•Категория В -критическая: критическое снижение производительности системы, ее способность использовать и удобоукладываемость или неприемлемое использование возможностей сотрудников при наличии:

•Больший ущерб - очень сложная ситуация или системная нагрузка, которая может вызвать неправильное поведение или неполноту основных функциональных проблем;

•Функциональность и производительность системы ПС или структурные характеристики функциональных недостатков;

•Неблагоприятный или потенциально разрушающий эффект системы или ПК для окружающей среды;

• Категория С- Важно для условий неисправности системы, а также использование функциональной пригодности для продолжения или может произойти, например, в связи с неблагоприятными условиями использования, погрузочных или информационных ресурсов, чтобы справиться с большим искажением условий, приводящих к уменьшению возможности сокращения функциональной способности сотрудников значительно сократить, или работы работников. Эта система приводит к ухудшению;

• Категория D- небольшая ошибка: условия, значительное снижение операции безопасности и использования объекта, но его влияние на надежность и производительность, в пределах их способности к восстановлению нормальной работы, требующей действий персонала может включать в себя, например, в определенных условиях труда увеличение нагрузки, использования или задержек с информацией для персонала;

• Категория Е: практически никакого эффекта, не влияет на производительность и особенности объекта или ошибки, а не увеличивать нагрузку на условия труда персонала.

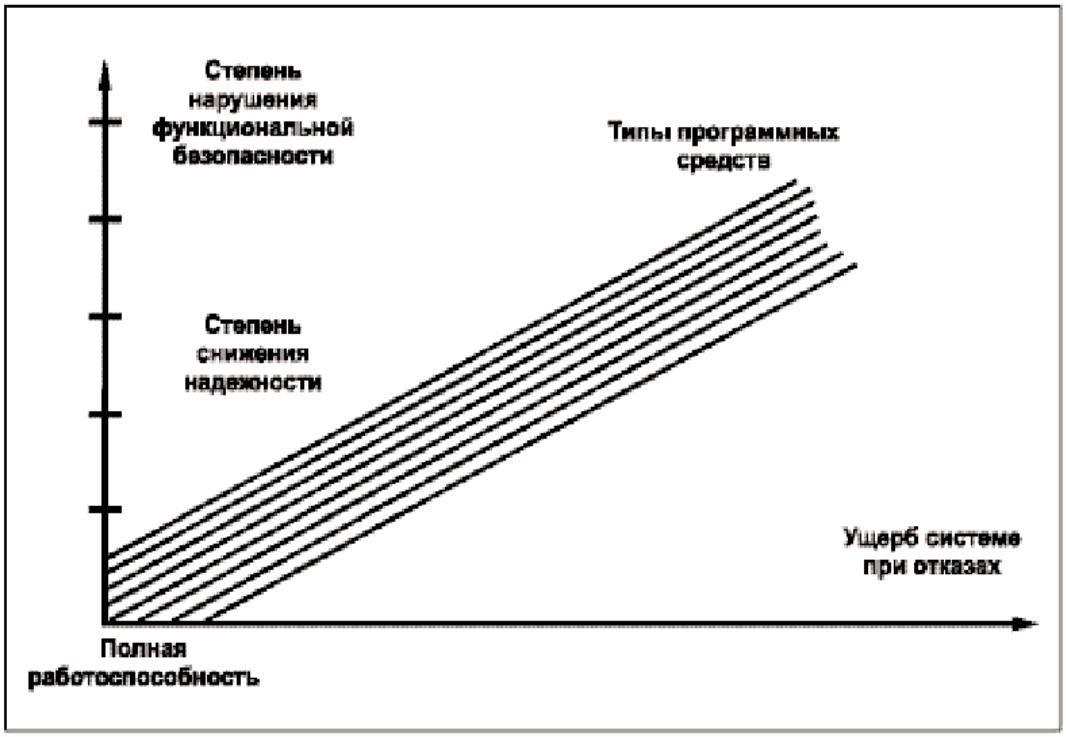

Рис. 3

Рисунок-3. В качестве функционального нарушения безопасности.

Риск отказа состоит в том, что эти пять категорий связаны с потенциальным ущербом, безопасностью и надежностью между концепциями, которые подходят для распределения систем или подстанций, демонстрируя разную степень воздействия. Характеристики первых двух категорий ситуаций высокого уровня следует рассматривать с точки зрения класса безопасности системы. Последние две категории не оказывают практического влияния на эксплуатацию объектов, но относительно менее надежны. Небезопасно рассматривать такие сбои. Третье важное событие - важная категория сбоев. Это требует полного и точного анализа функциональных характеристик, подстанций и сбоев системы, которые влияют не только на надежность, но и на безопасность системы.

Для простоты уровни функциональной безопасности и надежности зависят от линейного отказа и могут незначительно отличаться между различными типами программного обеспечения (см. Рисунок. 2). Эти зависимости могут быть интерпретированы в результате некоторых убытков, возникающих в результате снижения производительности системы или MS. Неисправности в случае неисправности могут быть вызваны снижением надежности во время работы или в худшем случае в качестве функционального нарушения безопасности (рисунок 3). Таким образом, категория, риск повреждения стоимости неспособности восстановить нормальное функционирование системы, сложности и длительности процесса оценки и классификации пиковых уровней и эксплуатационных требований к надежности и безопасности прикладных систем и может рассматриваться в качестве основы для программного обеспечения.

Уровень безопасности и надежности систем и подстанций рекомендуется устанавливать в соответствии с анализом или наиболее вероятными и опасными категориями отказов в обозначенной системе. Уровень качества ПС также зависит от сбоев программы и потенциальных сбоев данных, обнаруженных методами и процессами оценки безопасности.

Это зависит от качества работы, ресурсов и времени сбоя (см. Рисунок 3), чтобы гарантировать, что качество работы соответствует требованиям заказчика:

• Уровень A: Неясная функциональность, безопасность и качество системы, как показано в процессе неблагоприятного воздействия, не приводят к случайному сбою и полностью функциональной системе, которая может привести к неисправности программного инструмента;

• Уровень B: программное обеспечение, которое может привести к опасному состоянию для функциональной пригодности системы с более высоким риском нормального поведения;

• Уровень C: недостаточный риск среднесрочного риска травмирования или потери функциональности и надежности при оценке качества программного обеспечения, его патологическом поведении может иметь серьезные последствия;

• Уровень D: ненормальная система для работы системы и минимальный ущерб системе для незначительных сбоев, что влияет на состояние программного продукта - надежность и надежность функциональности;

• Уровень E: ненормальное поведение и производительность системы практически не влияет на работу сотрудников и их риски, но также может снизить надежность и качество программного обеспечения при использовании программного обеспечения.

2. Разработка модели оценки функциональной безопасности ПСКН

Современная методология оценки качества программных средств (ПС), принятая в семействе международных стандартов ISO/IEC 25000, основана на модели качества и модели оценки качества программного продукта.

Модель качества ПС представляет собой структурированное множество взаимосвязанных характеристик и отношений между ними, образующих базис для спецификации требований к качеству и оценивания качества программного продукта.

Под моделью оценки (измерения) качества понимается спецификация понятий, отношений и правил, используемых для определения методологии измерения качества ПС.

2.1 Разработка модели функциональной безопасности для ПСКН

В соответствие с требованиями стандартов ISO/IEC 25000, для оценки характеристик качества программного продукта, в т.ч. функциональной безопасности, необходимы:

-модель качества характеристики, которая устанавливает подхарактеристики (subcharacteristics), атрибуты, а также показатели (метрики), которые используются для оценки функциональной безопасности программного продукта;

-процесс оценки, который описывает набор действий и задач, которые выполняются при проведении оценки;

-технологическая среда, обеспечивающая поддержку необходимых измерений, применения критериев оценки, а также визуализацию результатов.

Под моделью качества ПО понимается структурированное множество взаимосвязанных характеристик и отношений между ними, образующих базис для спецификации требований к качеству и оценивания качества программного продукта.

Первым шагом в оценке функциональной безопасности является выбор показателей его качества с использованием стандартной модели качества.

Стандарт ISO/IEC 25010 определяет две модели качества ПО:

– модель качества в использовании;

– модель качества продукта.

Качество в использовании - это объединенный эффект достигнутых характеристик качества для пользователей. Модель качества в использовании (рис. 1) определяет 5 характеристик качества, связанных с взаимодействием пользователя с ПО при его применении в заданном контексте:

- продуктивность (Effectiveness),
- эффективность (Efficiency),
- способность к удовлетворению (Satisfaction),
- отсутствие риска (Freedom from risk),
- покрытие контекста (Context coverage).

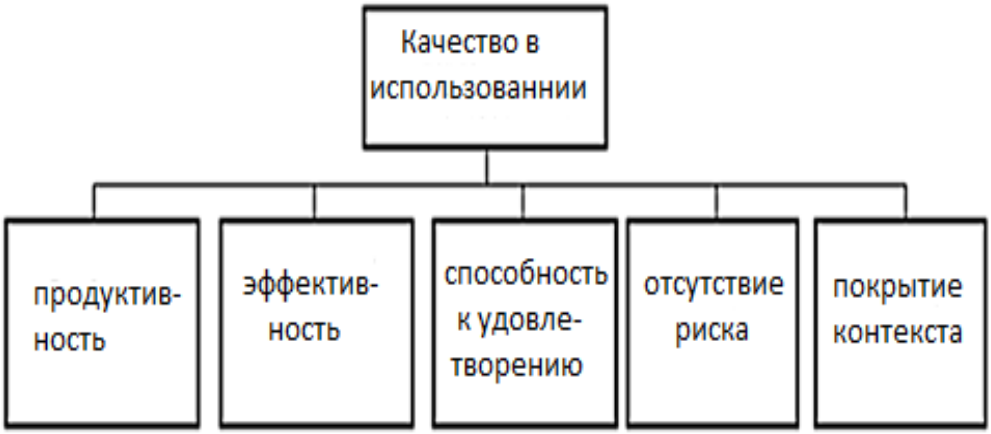

Рисунок 1 – Модель качества ПС в использовании

Модель качества продукта (рис.2) представляет свойства ПО 8 характеристиками:

– функциональная пригодность (Functional suitability),
– производительность (Performance efficiency),
– совместимость (Compatibility),
– удобство использования (Usability),
– надежность (Reliability),
– защищенность (Security),
– сопровождаемость (Maintainability),
– мобильность или переносимость (Portability).

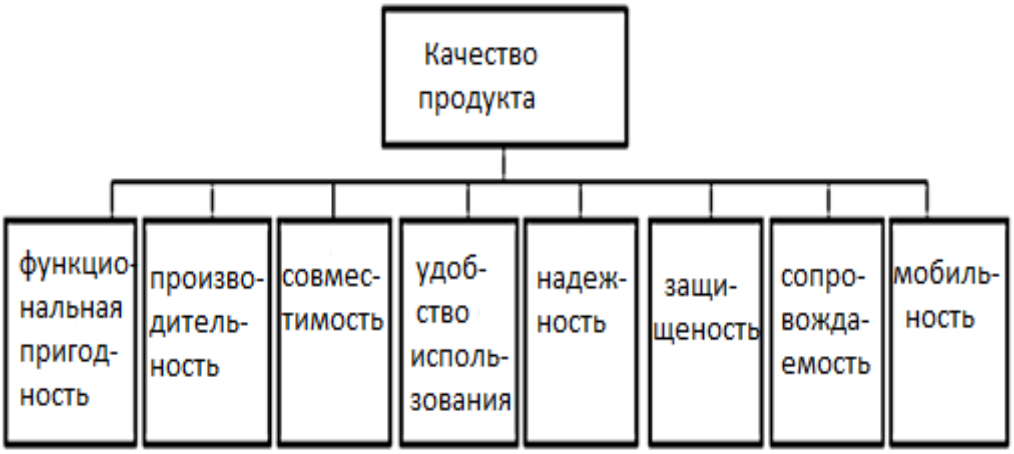

Рисунок 2 – Модель качества программного продукта

Прямое измерение характеристик качества невозможно. Для этого для каждой характеристики качества должна быть построена частная модель качества.

Структура модели характеристики качества ПО представлена на рис. 3.

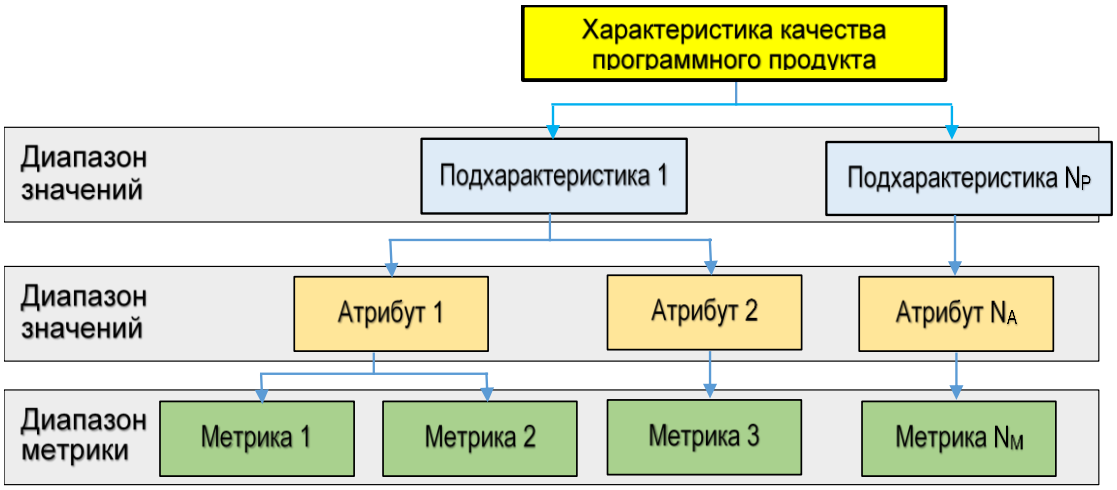

Рисунок 2 – Структура модели характеристики качества ПО

Чтобы создать модель функциональной безопасности ПСКН, необходимо определить атрибуты и показатели, необходимые для измерения этих спецификаций программного обеспечения.

Все возможные функции функциональной безопасности программного обеспечения можно разделить на две группы:

- первое, что напрямую связано с целью и масштабом программного обеспечения и представляет собой ряд особенностей, оцениваемых по конкретным категориям индикаторам;

- Во-вторых, возможна количественная оценка стандартизированных методов.

Программное обеспечение функциональной безопасности является частью используемых качественных характеристик и поэтому оценивается с использованием используемых показателей.

Измерение функциональной безопасности с адекватной точностью и надежностью для сравнения с требованиями ее спецификаций и спецификаций, а измерение должно быть объективным и репродуктивным.

Чтобы количественно определить атрибуты функциональной пригодности, необходимо создать специальные метрики, которые являются количественной мерой, которая позволяет количественно определять конкретные свойства конкретного программного продукта. Метрика характеризуется шкалой и используемым методом измерения.

Основными критериями защиты функционального программного обеспечения являются важность рисков. Риск R (t) в момент времени t, связанный с каким-либо событием, определяется как произведение вероятности P (t) неблагоприятных эффектов D, вызванных этим событием,

$$R(t) = P(t) * D, \quad (1)$$

В дополнение к числовым значениям рисков могут учитываться лингвистические значения (диапазон значений). Результаты анализа риска представлены как матрицы риска

В качестве показателей функции безопасности значения риска принимаются в соответствии с таблицей 1.

Для этих целей можно получить количественную оценку степени соответствия требованиям программного продукта на основе встроенной функциональной модели безопасности. Предлагаемый метод моделирования функциональной безопасности позволяет создавать различные модификации модели, в зависимости от класса класса ПСКН, путем введения или добавления дополнительных атрибутов и соответствующих показателей.

Таблица 1 – Метрики функциональной безопасности

Название	Назначение метрики	Формула и метод вычисления

Риск пользователей	Какова угроза использования ПО для жизни и здоровья пользователя	X=A/B A-количество пользователей, пострадавших вследствие использования ПО; B-общее количество пользователей
Экономический риск	Риск экономического ущерба	X=A/B A-количество случаев причинения экономического ущерба в результате использования ПО; B-общее число случаев использования ПО
Риск повреждения программ и данных	Какова частота повреждения программ и данных	X=A/B A-количество случаев повреждения данных и программ в результате использования ПО; B-общее число случаев использования ПО

2.2 Разработка модели оценки функциональной безопасности ПСКН

В соответствии с современной методологией оценки качества ПС, описанной в базовом международном стандарте ISO/IEC 25040:2011, для оценки качества и измерения его показателей необходимо построить модель оценки (измерения) качества (МОК). Модель оценки качества (измерения) понимается как уточнение понятий, отношений и правил, используемых для определения метода измерения качества контроля качества.

В стандарте ISO/IEC 25040 определены эталонная модель процесса оценки качества программных средств и общие рекомендации по ее применению.

Модель оценки качества (МОК) для конкретного проекта ПС должна основываться на процессе оценки ссылочного качества. МОК должна описать процедуры и процедуры для оценки целей обеспечения качества.

Процесс оценки программного обеспечения для различных целей представляет собой последовательность действий, которые необходимо предпринять для решения оцениваемого объекта в соответствии с конкретным проектом с указанием, планированием, реализацией и ограничениями ограничений. Общая схема оценки качества программного обеспечения показана на рисунке 4.

Необходимо определить входные и выходные данные, ограничения и ресурсы, необходимые для оценки качества программного продукта для

конкретного проекта. Оценка качества ПСКН должна определяться путем определения требований к качеству программного обеспечения с использованием ISO / IEC 25030, определения конкретных целей и критериев оценки.

Процесс оценки качества ПС включает в себя следующие ключевые задачи (процедуры):

1) разработка требований к оценке;
2) разработка специфики оценки;
3) разработка плана оценки (проекта);
4) выполнение оценки;
5) Подготовка и подготовка отчетов об оценке.

2.3 Основные процедуры оценки функциональной безопасности ПСКН

Введите информацию для этой процедуры:

а) необходимость оценки качества программного продукта;

б) уточнить требования к качеству программного продукта;

c) используемые измерительные приборы и методы;

d) Программный продукт, который включает промежуточные продукты, которые оцениваются.

Результаты этого действия:

a) уточнить цели оценки качества программных продуктов;

b) уточнить требования к обеспечению качества программного обеспечения;

c) описание высокоуровневого (общего) плана оценки качества программного продукта.

Эта процедура включает в себя следующие задачи.

- определение цели оценки качества;
- определение оценки;
- требования к качеству подстанций;
- Определение степени тяжести.

Определение целей оценки качества

Целью обеспечения качества является обеспечение соответствия продукта требуемому качеству, которое соответствует установленным и неполным требованиям.

Качество ПС может оцениваться как качество промежуточного программного продукта или конечного качества продукта.

Целью оценки качества промежуточного программного продукта может быть следующее:

-обеспечение качества промежуточных программных продуктов;

-принятие решения о принятии промежуточного субподрядчика;

-оценка текущей мощности проекта разработки ПС;

-принятие решения о завершении цикла жизненного цикла и переход к следующему этапу;

-прогнозирование или предварительная оценка конечного качества программного продукта;

-сбор информации о промежуточных продуктах для мониторинга и контроля процесса разработки;

-разработка программного продукта, разработка и тестирование производительности.

Целью оценки качества программного продукта может быть следующее:

-принятие решения о принятии окончательного продукта;

-определение времени выпуска.

-Сравнение продуктов с аналогичными конкурентоспособными продуктами;

-выбор продуктов из альтернативных продуктов;

-оценка положительных аспектов и пробелов в использовании продуктов, а также их причин;

-Определите способы улучшения качества или замены продукта.

Входными данными для этой процедуры должны быть:

-спецификация детального плана оценки программы;

-уточнение требований к оценке качества программного продукта;

-спецификация требований к качеству программного обеспечения;

-спецификация выбранных показателей качества (оценочные модули);

-уточнить критерии принятия решений о показателях качества программного обеспечения;

-определение критериев для общей оценки качества программного обеспечения;

-определение методов оценки качества программного продукта;

-включая промежуточные продукты, следует оценивать по качеству программного продукта.

Ключевые результаты оценки качества программного обеспечения:

-результаты измерений качества программного продукта;

-результаты оценки качества программного обеспечения.

Основные действия по обеспечению качества программного обеспечения:

-проведение измерений;

Использовать критерии оценки качества ПСКН (сравнение результатов измерений с критериями и требованиями);

- использование общих (интегральных) критериев оценки ПС (расчет комплексных показателей и сравнение с соответствующими критериями и требованиями)

Измерение включает введение набора критериев для выбранных показателей качества программного продукта и его компонентов. Выбранные размеры программного продукта используются для измерения. Результаты измерений - это значения в заданном диапазоне показателей.

Использование критериев ПС для критериев качества - это сравнение установленных критериев (требований) и их измеренных значений для определения их соответствующих пороговых значений.

Общее качество программного обеспечения - это измерение программного обеспечения, используемого для оценки общего качества программного обеспечения, основанного на результатах оценки (измеренных), характеристиках podharakteristik и качественных показателях на основе их взаимопонимания и степени соответствия качеству программного обеспечения.

Результаты оценки:

-В том же самом случае тот же метод, полученный по тому же параметру, представляет собой последовательность измерений между результатами повторного владения (соответствует сходству;

-Изменилась ситуация измерения, и тот же параметр приводит к последовательности измерения свойства между репродуктивными репродукциями (полученными тем же методом, что и один и тот же объект;

-обеспечить необходимый уровень надежности, отвечающий требованиям качества программного продукта;

-определение конкретных пробелов и требований для определения выявления дополнительных оценок, необходимых для определения объема этих недостатков;

-Позволяет определить определенные ограничения или условия использования программного продукта;

-Оценка также позволяет выявлять недостатки и недостатки и оценивать дополнительные потребности.

3. Разработка методики оценки функциональной безопасности ПСКН

Методы теории информации, методы математического описания и исследования информационных процессов, методы передачи, обработки, хранения, поиска и классификации информации, методы теории алгоритмов, теория расчетов, методы контроля качества программного обеспечения, методы надежности программного обеспечения.

При решении проблем диссертации использовались нормативные документы по системному анализу, защите информации, разработке систем защиты программного обеспечения, управлению качеством продукции, а также оценка качества программного обеспечения, защиты информации и других материалов.

Нормативно-методическое и методическое обеспечение технического и экспортного контроля Республики Казахстан, Агентства Республики Казахстан по техническому регулированию и метрологии и других организаций по вопросам нормативно-методического обеспечения процесса обеспечения безопасности и обеспечения качества программных систем

отечественной и зарубежной научно-технической литературы материалов и компьютерной техники.

В ходе дипломногоного исследовании были получены и рекомендованы следующие научные результаты для защиты:

1.Классификация методов оценки качества для применения программных систем общего назначения.

2.Отбор и регистрация ключевых показателей, учитываемых в общей системе обеспечения качества; Особенности систем оценки, связанных с этой оценкой; методы оценки различных показателей качества программного обеспечения и его систем защиты.

3.Методы и рекомендации по разработке высококачественного программного обеспечения на основе неинвазивных алгоритмов.

4.Системная модель «Защищенное программное обеспечение - система защиты программного обеспечения. Анализ функциональности этой модели с учетом функциональных связей между ее структурными элементами.

5.Комплексная модель обеспечения качества систем защиты программного обеспечения.

6.Модель жизненного цикла системы для систем защиты программного обеспечения с улучшенным качеством систем защиты и использование различных механизмов контроля качества на каждом этапе.

7.Методы обеспечения безопасности компьютерных систем на основе существующих принципов качества и безопасности.

3.1 Выбор методов оценки функциональной безопасности ПСКН

Многие методы могут использоваться для обеспечения информационной безопасности в рамках концепции интегрированной безопасности (безопасности и безопасности) современных систем мониторинга.

Выбор методов оценки не гарантирует соответствия требованиям безопасности. Оценщики должны учитывать:

обоснованность и согласованность выбранных методов, языков и инструментальных средств со всем циклом разработки;

используют ли разработчики методы, которые они полностью понимают;

хорошо ли методы, языки и инструментальные средства подходят для исключения дефектов и ошибок, возникающих при разработке.

В каждом стандарте стандартные таблицы содержат рекомендации по уровням соответствия набору требований безопасности. В соответствии с набором требований безопасности вы должны выбрать соответствующие методы. Методология связана с концепцией эффективности. Для всех других сбалансированных факторов методы, описанные HR, более эффективны с точки зрения контроля остаточных дефектов в PP, выявленных при разработке

программного обеспечения, в предотвращении системных нарушений (в архитектуре). Для специальных приложений при планировании безопасности следует указывать соответствующую комбинацию методов и мер. Функциональные этапы IEC 61508-3 начинаются с требований системы безопасности и соответствующей части плана безопасности клиента, которые:

Необходимые функции безопасности и уровни, соответствующие набору требований для объекта или системы:

функции безопасности, назначенные компонентам системы безопасности;

Он рассматривает возможности программного обеспечения в каждом компоненте системы безопасности.

1.Программная архитектура определена для всех функций безопасности, отправленных в ПС.

2.Вместе с разработчиком разработчиком функции архитектуры и программного обеспечения и оборудования считаются безопасными.

3.Начались планы по тестированию и сертификации подстанций.

4.Проектирование, разработка, испытания и испытания подстанций:

планирование безопасности;

уровень соответствия ПС требованиям к безопасности объектов или систем; ПС.

5.Завершите Службу наблюдения ПС, которая должна соответствовать процедурам операционной системы для персонала ПС и описать хорошо разработанное программное обеспечение, предоставленное предоставленным финансовым инструментом.

Вместе с сайтами или системами безопасности программное обеспечение разработчика сертифицировано аппаратным обеспечением 6. Он сертифицирован производителем программного обеспечения или системой безопасности совместно с разработчиком.

7.Дальнейшие выводы ПС System Engineer будут разделены с дальнейшей оценкой всей системы.

8.Если ПС Во время работы некоторые шаги, которые необходимо изменить, требуют повторения.

Для этих шагов необходимо выбрать методы и процедуры безопасности ПС в соответствии с требуемым уровнем соответствия установленным требованиям безопасности системы. Чтобы упростить этот выбор, стандарты были разработаны с использованием множества различных методов и мер в зависимости от четырех уровней соответствия требованиям безопасности. Перекрестные ссылки в таблицах - это меры предосторожности для каждого метода или ссылки на дополнительные источники информации. Примеры пригодности приложения к набору требований безопасности приведены в Приложении и подпадают под действие требований соответствия требованиям безопасности для программного обеспечения, разработанного в IEC 61508-7.

3.2 Разработка требований к функциональной безопасности ПСКН

Объем и распределение доступных компьютерных ресурсов может оказать существенное влияние на общую безопасность системы. Наиболее распространенным видом ресурсов, который следует учитывать при проектировании, являются финансовые и экономические издержки или сложность разработки и функционирования системы безопасности системы. Чтобы разместить эти ресурсы на объектном компьютере, необходимо обеспечить программное обеспечение и потерю информации из внешних и внутренних ресурсов памяти компьютера. Кроме того, необходимо иметь временную резервную копию для работы компьютера - дополнительную производительность компьютера. Обеспечивая функциональную безопасность, также используются следующие типы вычислительных ресурсов:

•Мониторинг и коррекция искажения информации с внешних носителей и источников данных;

•Быстрое обнаружение и обнаружение дефектов в программном обеспечении и обработке данных при использовании ПС для основных целей;

•Обеспечение и поддержание безопасности всех видов безопасности;

•Создание тестовых наборов или проведение тестов для отслеживания работы, целостности и целостности работы ПС во время работы системы;

•Сбор, хранение и мониторинг несанкционированного доступа к информации об обнаруженных событиях, связанных с безопасностью программ и сбоев данных, сбоев и сбоев;

•Внедрение обнаружения и обнаружение неисправностей и быстрый анализ процедур и программ мониторинга и мониторинга (перезапуска) обеспечивает функциональность системы и дефекты после ее обнаружения.

Клиент-клиент в первую очередь заинтересован в безопасности и качестве готовой продукции - системы и программного обеспечения, обычно не заботятся о том, как они достигаются. Конструкция системы и ПС, а также необходимая функциональная безопасность любого продукта могут обеспечить два метода:

продукты, которые неадекватны для безопасности и качества готовой продукции или спецификации поставки или пересмотра только окончательным, окончательным тестированием и проверкой;

Обеспечение функциональной безопасности и обеспечения качества при проектировании, разработке и производстве дефектных технологий и обеспечении высокой безопасности и качества при создании и модификации.

Первый метод может быть очень дорогостоящим для сложных систем, которые могут привести к значительным экономическим потерям из-за затрат на строительство, что не подходит для вступления в брак. процесс разработки адекватен процессу разработки и может быть достигнут только за счет отсутствия системы обеспечения качества без необходимости обеспечения

безопасности, доступа, улучшения продольного процесса и повторного тестирования массового производства.

Второй способ-создание сложных систем, которые являются экономически эффективными из-за высокого качества и недостатков в процессе проектирования, проектирования и производства, что обеспечивает минимальные экономические издержки. Он уменьшает, но не исключает функциональную безопасность и качество контроля качества продукции. Для создания современных высококачественных приложений требуются два метода, в которых основное внимание уделяется использованию регулируемых технологий в безопасных системах. Таким образом, сертификаты безопасности и качества и интегрированные политики резервного копирования должны основываться на проверках и тестах:

-программные технологии, поддерживающие регулируемые системы качества, жизненный цикл программного обеспечения;

-функционирование готовых программных продуктов с полным набором соответствующей документации по техническому обслуживанию.

Качество разработанных систем и программ имеет решающее значение, когда их конечная взаимосвязь зависит от качества их технологии строительства и всего жизненного цикла, а также от необходимости получать конечный продукт с высокими значениями безопасности и качества. Когда показатель качества приближается к этой технологии и приближается к достижению уровня автоматизации процесса разработки, становится ясно, что стоимость разработки резко возрастет. Это привело к существенному изменению методологии и культуры в создании и совершенствовании системы и ПС. ПС Непрерывный рост требований к функциональной безопасности и качеству Способствует созданию и использованию международных стандартов и регулируемой технологии, которая автоматизирует цикл жизненного цикла. очень сложно оценить необходимость принятия очень редкого случая случайных сбоев, в большинстве случаев, для определения сложной сложной системы и сложности программного комплекса и измерения прямой функциональной безопасности. Для этой цели мы подвергаемся высокому риску и могут быть очень дорогими в критических ситуациях, и создание опасных операционных систем должно проводить долгосрочные эксперименты. Кроме того, одна из редких и одна из неисправностей не позволяет оценить статистическую значимость времени между авариями и вероятной величиной в этом случае. Программы функциональной безопасности. Аналитические вычисления и экспертная оценка Полная функциональная безопасность программных модулей и компонентов может выявлять сбои и ошибки в случайном, неожиданном развертывании, усложняя комплексы. Поэтому высокая функциональная безопасность программных продуктов определяется и определяется технологиями обеспечения качества на всех этапах жизненного цикла систем и подстанций. С этой целью стандарты, регулирующие функциональную безопасность систем и программных систем, уделяют

большое внимание технологическим процессам и инструментальным системам для обеспечения безопасности и качества ПС. В IEC 61508 аппаратные и программные системы встроены в функциональные системы безопасности и частично разработаны для обеспечения шестой части требований и третьей части процессов регулирования.

ПС Обеспеченность этапы и процессы структурированы по схеме работ, компонентов и объектов, а также выбора методов для создания безопасных подстанций и внесли свой вклад в рекомендации. Третья часть ISO 15408 посвящена полному набору требований к обеспечению качества при разработке и использовании комплексов систем информационной безопасности. Этот набор требований для обеспечения функциональных возможностей безопасности, с акцентом на реализации функций безопасности, используемых в традиционных методах поддержки сложного жизненного цикла технологий ПС. безопасные системы и программное обеспечение инженерных технологий и процессов, а также ISO 13335 стандарта IEC 60880. Таким образом, значительная часть требований стандартов в процессе создания безопасных систем и программного обеспечения для функциональных стандартов безопасности, но нет описания процессов измерения и локализации а также критерии безопасности программного продукта. Функциональные элементы методов безопасности для защиты физических нарушений, вызванных старением оборудования случайного появления, а также процессы несовершенные конструкции, направленные на защиту системных расстройств. В дополнение к информационной безопасности современной глобальной безопасности, функциональные методы безопасности обеспечивают защиту от кибератак. Кроме того, многие из методов трудно, то есть тот же самый метод, в первую очередь, для защиты случаен функциональность продукта будет необходимо и достаточно механизм безопасности, а во-вторых, обеспечение функциональной безопасности в процессе разработки необходимого и достаточного набора используемых методов. Следовательно, мы будем выделять технические и организационные соглашения о функциональной безопасности.

3.3 Разработка методики выполнения оценки функциональной безопасности ПСКН

Разработка и оценка программного обеспечения и систем функциональной безопасности часто связаны с интуицией, их разработчиками, клиентами и умениями пользователей. Успех теории и практики управления интегрированными программными продуктами в целом не известен или не используется экспертами в разработке и внедрении программных (ПС) систем. В большинстве случаев ПС определяет дефекты и неисправности. Часто проекты подстанции являются подлинными, заявленные

цели и требования безопасности не соответствуют первоначальным требованиям и требованиям к качеству, согласованным с графиком и бюджетом развития. технические характеристики и сложность SS Требования текущих проектов систематически измеряются и сравниваются с требованиями, изложенными в Условиях, ссылках или Спецификациях, как описано в описании характеристик, показаний и недостаточных показателей безопасности и концепций программного обеспечения и не предоставляет информацию. В то же время функции безопасности часто отсутствуют в определенных требованиях клиентов и в согласованных документах ПС. Это влияет на отсутствие формализации и документирования процесса отбора и анализа. Предлагаемый проект направлен на: - анализ и обоснование требований к программному обеспечению функциональной безопасности; - изучение процессов программного обеспечения функциональной безопасности; - оценка их функциональной безопасности и функционального программного обеспечения для обеспечения безопасности при проверке тестирования и тестирования программного обеспечения; - разработка методологии функциональной безопасности сложных программных систем.

4. Экономический раздел

4.1. Принципы оценки экономической эффективности программных средств

Экономическая эффективность программного продукта - это измерение коэффициента потери производительности программного продукта.

Ключевые экономические показатели:

-экономический эффект,

-коэффициент экономической эффективности капитальных вложений,

-срок погашения капитальных вложений.

Экономический результат- результат реализации услуги в виде сбережений в форме сбережений.

Основные источники сбережений для организаций (предприятий) с использованием программного обеспечения:

-улучшение основной деятельности, связанной с использованием программного обеспечения;

-сокращение времени разработки новых программных продуктов за счет лучших эргономических функций;

-сокращение времени компьютера и других ресурсов для запуска и восстановления задач;

Коэффициент экономической эффективности капитальных вложений составляет один тенге в год от производства или использования программных продуктов.

Показателем эффективности инвестиций является период времени, включая стоимость программного обеспечения, период компенсации (отрицательный доход).

4.2 Основные показатели экономической эффективности программных средств

Определение эффективности программного продукта основано на принципах оценки производительности и использования новых технологий. Основные положения разрабатываются на основе разработки и разработки методов определения экономической эффективности использования новых технологий, изобретений и инноваций с учетом специфики программного продукта.

На различных стадиях жизненного цикла программного изделия и в зависимости от целей расчета рассчитываются и документально оформляются следующие виды экономического эффекта: предварительный, потенциальный, гарантированный и фактический.

Предварительный экономический эффект рассчитывается до разработки этих технических предложений и эксплуатационных допущений. Предварительный результат является элементом технико-экономического обоснования разработки программного продукта и используется для планирования и разработки программных продуктов.

Потенциальный экономический эффект рассчитывается на основе технико-экономических характеристик и допущений, которые были достигнуты для максимизации использования программного продукта. Потенциальный результат заключается в оценке эффективности организаций по разработке программного обеспечения.

Гарантированный экономический эффект рассчитывается как гарантированное экономическое преимущество для конкретного сайта реализации и обычно гарантируется для нескольких объектов.

Гарантированный общий экономический эффект рассчитывается, когда программное обеспечение основано на данных о объеме программных продуктов, соответствующих возможностям продукта, продукции и обслуживании, а также на основе фактической продуктовой производительности программного обеспечения (производственных объектов). Гарантированный валовой эффект служит для разработки и утверждения экономически жизнеспособных продуктов для программных продуктов, выбора варианта производства и внедрения программных продуктов.

Фактический экономический эффект рассчитывается на основе данных бухгалтерского учета и сопоставим с затратами и результатами фактического использования программного продукта. Фактический результат рассчитывается из одной программы для внедрения определенных программных продуктов в конкретном учреждении, а также общей экономической эффективности конкретного программного продукта на всех сайтах отчетного периода. Фактический результат используется для оценки эффективности организаций, создающих, внедряющих и использующих программные продукты.

4.3 Анализ и расчет затрат на разработку ПСКН

Цель этого раздела: кратко изложить содержание проекта для обоснования его экономической, целесообразности, реального и основных преимуществ.

Внедрение методологии тестирования программного обеспечения для космических применений значительно упростит и автоматизирует работу

В экономической секции необходимо определить:

1) сложность этапов разработки;
2) расходы для разработчиков;
3) социальные расходы;

4) затраты на разработку и потребление энергии;

Затраты на разработку программного обеспечения разработчика определяются путем умножения сложности разработки методологии тестирования разработчика ЗПр для средней почасовой заработной платы. Мы снимаем затраты на работу разработчика в качестве формулы

$$Çï_{Ð} = Ò * Ñ\times_{Ð}\ , (4.1)$$

где,Т - трудоемкость разработки методики тестирования;

СЧр- средняя почасовая оплата за разработчика, тенге в час.

$$Ñ\times_{Ð} = \frac{Ï_{ïð} + Ï_{Ðóê} + Ï_{Ò}}{Ô_{ÐÂ}},\ (4.2)$$

где, $Ï_{Ðóê}, Ï_{ïÐ}$ $Ï_{Ò}$, - зарплату программиста, зарплату работника и зарплату тестера, среднюю заработную плату программиста:

$Ï_{ïÐ}$= 160000 тенге;

Зарплата тестера:

$Ï_{Ò}$= 80000 тенге;

а руководитель проекта:

$Ï_{Ðóê}$ = 230000 тенге;

$Ô_{ÐÂ}$= Ежемесячные рабочие часы с 8-часовыми рабочими днями и 5-дневной рабочей неделей:

$Ô_{ÐÂ}$=176 часа

Подставляя в формулы значения, получим значения СЧр и ЗПр:

$$Ñ\times_{Ð} = \frac{160000 + 230000 + 80000}{176} = 2670,45 òåí ãå/ ÷àñ,$$

$$Çï_{Ð} = 211,47 * 2215,91 = 564720,06 òåí ãå$$

Расходы на оплату труда программиста на разработку тестирования составят 468598,49 тенге.

Расчет отчислений на социальные фонды.

Единый социальный налог составляет 11 % от заработной платы разработчиков:

$$Ñ_{Í} = Çï_{Ð} * 0,11\ ,(4.3)$$

$$Ñ_{Í} = 564720,06 * 0,11 = 62119,20 òåí ãå$$

Поэтому оплата научного руководителя и программиста за разработку теста составляет 493470,05 тенге.

Расчет затрат на техническую поддержку проекта.

Тестирование средств разработки требует:

Технические средства	Стоимость, тенге
монитор	40000
системный блок	100000
клавиатура	2500
мышь	2000
программный продукт	130000
Windows10 (лицензионный)	40000
Итоги	314500

Программным продуктом является программное обеспечение и соответствующая документация для доставки пользователю. Программный продукт представляет собой программный продукт, определенный в ГОСТ Р ИСО 9126.

Общие затраты на техническую и программную поддержку Sof = 314500 тенге. Основные средства переводятся на товары, которые оцениваются в виде амортизационных отчислений.

Рассчитать стоимость амортизации по следующей формуле:

$$Ç_{à} = Ñ_{áàë} * \frac{Í_{à}}{100}\%, \quad (4.4)$$

где: Сбал -балансовая стоимость компьютер а, тенге/шт;

На-норма амортизации в процентах.

Балансовая стоимость компьютер а определяется по формуле:

$$Ñ_{áàë} = Ñ_{Ðû í} * Ç_{Ï Ð}, \quad (4.5)$$

где:

$Ñ_{Ðû í}$ -рыночная стоимость ПК, в тенге

$Ç_{Ï Ð}$-прочие затраты (на доставку , от 3 до 6% от стоимости ПК).

Берем $Ç_{Ï Ð} = 5\%$ от рыночной стоимости ПК.

Рыночная стоимость компьютера составит 144500 тенге.

Срок службы компьютера составляет 5 лет, поэтому амортизация Н составляет 20%.

$$Ç_{Ï Ð} = 144500 * 0,05 = 7225 òåí ãåå$$

Рассчитываем балансовую стоимость

$\tilde{N}_{áàë} = 144500 + 7225 = 151725 ò\ åí\ ãå,$

Находим по формуле издержки на амортизацию

$Ç_{ïà} = 151725 * 0,2 = 30345 ò\ åí\ ãå$

Издержки на амортизацию составляют 30345тенге.
Рассчитываем действительный фонд времени ПК:
Стоимость амортизации составляет 30 345 тенге.
Мы вычисляем точный временной фонд ПК:

$$Ò_{Ï\,Ê} = N_m * N_{ä} * N_{÷}, (4.6)$$

где: N_m – количество месяцев , срок разработки программного продукта;
$N_{ä}$ - количество рабочих дней в месяце;
$N_{÷}$ - средняя продолжительность рабочего дня (8 часов);

$Ò_{Ï\,Ê} = 3 * 22 * 8 = 528 ÷ àñî\ â,$

Действительный фонд времени в срок разработки программного продукта ПК равен 528 часов.
Теперь, рассчитываем цену машино-часа (тенге):

$$T_{ð} = \frac{Ç_{ïà} + Ç_{Ïî\,ð}}{Ò_{Ï\,Ê}}, (4.7)$$

где: $Ç_{ïà}$ - затраты издержек на амортизацию, тенге в срок;
$Ç_{Ïî\,ð}$ - годовые издержки на прочие и накладные расходы, тенге в срок;
$Ò_{Ï\,Ê}$ - действительный фонд времени ПК, ч асов в срок;
Теперь, подставляя в формулу найденные значения находим цену одного машино-часа:

$$\tilde{N} = \frac{30345 + 7225}{528} = 71,15,$$

Цена одного машино-часа составит 71,15 тенге.
Мы вычисляем стоимость компьютерного времени, пока программное обеспечение обновляется.
Стоимость машинного времени определяется по формуле:

$$Ç_{Ï\,Â} = \tilde{N} * (t_{ïð} * t_{îò}), \ (4.6)$$

где: $\tilde{N}$ - цена машино-часов, рассчитывается;

$t_{ïð}$ - затраты на программирование;

$t_{îò}$ - затраты на отладку программы.

По формуле рассчитываем затраты на оплату машинного времени при написании и отладке программы:

$$Ç_{ÎÂ} = 71,15*(30,30+68,18) = 7006,85 òåíãå$$

Общая стоимость технической поддержки проекта:

$$Ç_{Îò} = Ç_{ïð} + Ç_{îò} + Ç_{ÎÂ}, (4.7)$$

$$Ç_{Îò} = 30345 + 7225 + 7006,85 = 44576,85 òåíãå$$

Рассчитать стоимость электроэнергии по формуле:

$$\tilde{N}_{Ý} = Ç_{Ý} * Ð*(t_{ïð} + t_{îò} + t_{ä}), \ (4.8)$$

где: $Ç_{Ý}$ - стоимость электроэнергии $1 êÂò \div = 26 \ òã$;

$Ð$- мощность, потребляемая ПК (для компьютера в вышеуказанной конфигурации мощность составит 800 Вт;

$t_{ïð}$ -затраты на программирование $t_{ïð} = 30,30$

$t_{îò}$ - затраты на отладку; $t_{îò} = 68,18$

$t_{ä}$ - затраты на подготовку документации $t_{ä} = 21,21$.

$$\tilde{N}_{Ý} = 26*0,8*(30,30+68,18+21,21) = 2489,55 òåíãå$$

Подводя итоги, мы получаем:

Расходы на оплату труда руководителя и программиста, тг	564720,06
Затраты на техническое обеспечение проекта, тг	44576,85
Отчисление социальный налог,тг	62119,20
Затраты на энергоресурсы, тг	2489,55
Итого	673905,66

Диаграмма 4.1. Структура затрат на тестирование программного обеспечения для космических применений

Было достигнуто экономическое обоснование для разработки методологии тестирования программного обеспечения для космических целей: были рассчитаны затраты менеджера и программиста; расходы на техническое обслуживание, включая амортизацию основных средств, другие расходы и стоимость автомобиля; стоимость потребленной электроэнергии.

Стоимость «затрат на разработку программного обеспечения» включает 7% стоимости технической поддержки, заработной платы - 84%, вычетов по социальному налогу - 9% и энергопотребления - 1%.

Таким образом, само программное обеспечение составляет 673905,66 тенге.

Цены на программные продукты определяются по следующей формуле:

$$Ц_{ПП} = С_П + П_П + НДС \quad (4.8)$$

где $Ñ_{ïÐ}$ - себестоимости программного продукта тг;

$Ï$ - прибыл продукта от себестоимость 20-40%, заложим 35%, НДС-налог на добавленную стоимость 12%;

Себестоимость программного продукта $Ñ_{ïÐ} = 673905,66 òåíãå.$

Прибыль продукта:

$$Ö_{ïï} = 116735,66 + 673905,66 = 790640,66 òåíãå$$

Цена программного продукта-790640 тенге.

5 Безопасность жизнедеятельности

5.1 Охрана труда и техника безопасности на рабочем месте

Вопросы безопасности человека необходимо решать на всех этапах жизненного цикла, который заключается в разработке, внедрении или использовании программы.

Более безопасная жизнь человека во многом зависит от оценки опасных, вредных производственных факторов. Изменения в тяжести человеческого тела могут возникать по целому ряду причин. Это может быть любой фактор в рабочей среде, чрезмерный физический и умственный стресс, нейроэмоциональный стресс и другие комбинации этих причин.

Опасные и вредные производственные факторы делятся на следующие группы в зависимости от их происхождения:

физически;

-химические;

-психофизиологические;

-Био разнообразие.

В лабораторной комнате следующие физические факторы могут неблагоприятно влиять на программиста:

-высокая и низкая температура воздуха;

-избыточное загрязнение пылью и газом;

-высокая и низкая влажность;

-болезни рабочего места;

-Чрезмерные нормы шума;

-повышение уровней ионизирующего излучения;

-повышение уровня электромагнитных полей;

-уровень статического электричества;

-опасность поражения электрическим током;

-Экран дисплея отключается.

Микроклимат производственных помещений - это климат интерьера здания, определяемый сочетанием температуры, влажности и влажности воздуха, которые влияют на организм из трех человек.

Несмотря на внешние условия, лаборатория использует нагрев воды в холодную погоду в отопительный сезон для оптимизации влажности, влажности, гигиены и влажности воздуха. Кондиционер - это блок вентилятора, в котором хранятся настройки кондиционирования воздуха в помещении с помощью устройств автоматического управления.В случае, если естественное освещение слабое, на рабочем месте должно применяться также искусственное освещение. Далее будет произведен расчет искусственного освещения.

Источниками помех могут быть общий уровень шума, источники вентиляции, кондиционеры или периферийные устройства для компьютеров

(плоттеры, принтеры и т. Д.). Эффект этого шума в течение длительного времени оказывает негативное влияние на эмоциональное состояние персонала.

Согласно ГОСТ 12.1.003-76 эквивалентный эквивалентный объем ССБТ не должен превышать 50 дБА. Для достижения такого уровня шума рекомендуется использовать настенные росписи, которые создают звук.

В качестве мер по снижению шума вы можете:

- укладка потолков и стен звукоизоляционными материалами (шум уменьшается на 6-8 дБ);
- экранирование рабочих мест (установка секций, диафрагм);
- установка в компьютерном зале минимального оборудования для удаления шума;
- Рациональное расположение зданий.

Электромагнитные поля с сильными характеристиками электрического и магнитного полей вредны для человеческого организма.

Основным источником этих проблем являются мониторы (мониторы), особенно электронно-лучевые трубки, которые относятся к здоровью людей, использующих компьютерные информационные системы на основе персональных компьютеров. Они являются источниками вредных веществ, что отрицательно сказывается на здоровье программиста.

ПЭВМ - источники таких выбросов:

-мягкий рентген; 72

-ультрафиолетовый от 200 до 400 нм;

-видимый 400 - 700 нм,

-инфракрасный инфракрасный порт 700 - близко к 1050 нм;

-3 кГц - радиочастота 30 МГц;

-электростатическое поле.

Ультрафиолетовое излучение менее эффективно, но высокая доза приводит к дерматиту кожи, головной боли и зрению.

Инфракрасное излучение приводит к перегреву тканей человека (особенно глазной линзы), повышенной температуре тела. Напряжение электростатического поля не должно превышать 20 кВ / м.

Поверхностный электростатический потенциал не должен превышать 500 В.

Выполните до пятнадцати минут в течение полутора часов, чтобы работать на компьютере, увеличивая мощность поля и, конечно же, пользуясь защитными экранами. Защитная защита от хорошей решетки или стекла накапливает электростатический заряд. Экран монитора заземлен, чтобы снять заряд.

Максимально допустимая спецификация ЭМП

Наименование параметров	Допустимое значение
Электрическая составляющая	10 В/м

напряженности электромагнитного поля на расстоянии 50 см от поверхности видеомагнитофона	
Напряженность электромагнитного поля по магнитной составляющей на расстоянии 50 см от поверхности видеомонитора	0,3 А/м
Напряженность электростатического поля не должно превышать: для взрослых пользователей	20 кВ/м
Напряженность электромагнитного поля на расстоянии 50 см вокруг ВДТ по электрической составляющей должна быть не более:	
в диапазоне частот 5 Гц – 2 кГц;	25 В/м
в диапазоне частот 2 – 400 кГц	2,5 В/м
Плотность магнитного потока должна быть не более:	
в диапазоне частот 5 Гц – 2 кГц;	250нТл
в диапазоне частот 2 – 400 кГц	25 нТл
Поверхностный электростатический потенциал не должен превышать	500 В

Чтобы предотвратить введение опасного оборудования, все дисплеи должны быть протестированы на соответствие требованиям безопасности (например, Международные стандарты для MRP 2, TCO 99).

Степень опасного и вредного воздействия на человека электрического тока, электрической дуги и электромагнитных полей:

-тип и значение напряжения и тока;

-частота электрического тока;

-текущий путь через тело человека;

-продолжительность действия на организм человека.

Электробезопасность в лабораторных помещениях обеспечивается техническими средствами и защитным оборудованием, а также организационными и техническими мерами.

Давайте рассмотрим основные причины поражения электрическим током на рабочем месте:

1.Повреждение металлических поверхностей (корпус, конец-конец), которые излучают мощность изоляции.

2.Нерегулируемые электроприборы.

3.Нет подготовки персонала по правилам электробезопасности. Статическое электричество хранится в корпусе компьютера во время работы. На расстоянии 5-10 см от экрана интенсивность электростатического поля составляет 60-280 кВ / м, т.е. в 10 раз больше, чем 20 кВ / м. Чтобы уменьшить напряжение, вы можете использовать увлажнители и нейтрализаторы, антистатические полы.

Электробезопасность по ГОСТ 12.1.030.- 81.

Опасное и вредное воздействие на людей, поражающих электрический удар, отражается в виде поражения электрическим током и профессиональных заболеваний.

Электробезопасность в лаборатории обеспечивается техническими средствами и защитным оборудованием, а также организационными и техническими мерами.

5.2 Техника безопасности при работе с электрическими приборами

Через конкретное тело тока через источник питания электропитания к электроприборам и впечатляющий электрический провод. Степень поражения электрическим током определяется током. Степень ущерба в основном обусловлена стрессом, физическим сопротивлением и изоляцией. высокое напряжение и высокий ток, а разрушающий эффект электрического тока может значительно снизить сопротивление. При работе в жаркой атмосфере сопротивление человеческого тела уменьшается. Сотрудник носит обувь, одежду, руки и т. Д. когда это чрезвычайно опасно.

Основные виды поражения электрическим током:

1. Электрическая травма. Каскадные нарушения диафрагмы включают сердечно-сосудистую и респираторную системы, судороги сердечной мышцы и потерю сознания.

2. Электрический ток. Возбуждение живых тканей, проходящих через тело.

3. Электрошок. Он состоит из эффектов центральной токсичности системы. Система кровообращения, метаболизм и даже нейропсихические расстройства.

4. Электрический ток. когда находящиеся под напряжением детали или электрическая дуга подвергаются электрошоку. Самая сложная ситуация - это текущая дуга электрической дуги и человеческого организма. Кроме того, внутренние органы могут гореть.

5. Электрические знаки. Это произошло при транспортировке деталей несущих материалов. Кроме того, кожа плотнее, а материал (металл) хранится в его отверстиях.

В то время должны учитываться другие факторы:

1. Тип горелки. Ток постоянного тока до 300 В пост. Тока более безопасен, чем ток. Непосредственные падения напряжения при 300 В опасны.

2. Текущая продолжительность. Чем дольше тело человека, тем больше изменений в теле, тем меньше сопротивление кожи и, следовательно, ток. В случае повреждения или влаги сопротивление кожи минимально.

3. Текущий путь в организме человека. Если текущий проходит через кратчайший путь и не влияет на важный орган (например, вдоль ладони), поражение будет минимальным. Если поток перемещается от одного к

другому, например, спинной мозг, сердце, дыхательная система и т. Д. будут затронуты. - Победа будет самой высокой.

Текущая частота. Текущая частота в линиях электропередачи составляет 50 Гц. Возрастающая частота будет медленной и немного менее разрушительной. Ток на частоте, превышающей 50 кГц, практически неразрушающий, но в то же время мощность тока должна быть меньше. Эти токи только вызывают тепло из внутренних органов. Это явление используется в физиотерапии.

Защита от напряжения в химических лабораториях не превышает 12 В.

Меры предосторожности при работе с электроприборами.

1.Лаборатория должна иметь общий переключатель для включения и отключения лабораторной сети.

2.Лаборатория должна использовать заводское оборудование. При их использовании вы должны следовать инструкциям паспорта и изготовителя.

3.Электроприборы в лаборатории должны быть обязательными. Целостность земли проверяется лаборантом.

4.Не используйте дефектные инструменты, сломанные изоляторы или отверстия.

Электроприборы (особенно электрические нагреватели) не должны оставаться без присмотра.

6.Все электронагреватели должны быть достаточно теплоизолированы со всех сторон независимо от их емкости.

ПРИМЕЧАНИЕ:

•Смочите руки краном.

•Протрите электроприборы и провода.

Первая помощь при поражении электрическим током.

1.Выключите жертву. Для этого отключите открытый ключ или этот параметр. Если это невозможно, сушите одежду, будьте сильнее и так далее. Используйте.

2.Если жертва сознательна, он должен обеспечить мир до прибытия врача. В случае сомнений дайте первую помощь (чистый, чистый, воздух, аммиак, посыпьте водой и согрейте тело, искусственное дыхание).

5.3 Расчет искусственного освещения

Большее внимание уделяется освещению рабочего пространства оператора, например, как работает свет и организм человека. Правильно лицензированное освещение начинается с высокого нервного функционирования и увеличивает функциональность. Когда нет света, человек работает более эффективно, устает и повышает вероятность совершения неправильного. В зависимости от длины волны свет может быть интересным (розово-красный) или успокаивающим (желто-зеленый). Спектральный состав влияет на производительность труда.

Исследования показали, что в естественном свете производится только 100% человеческого производства, производится только 76% красного и оранжевого. Люди могут потерять свой естественный свет вообще по любой причине или части. В связи с этим компании уделяют большое внимание рабочему пространству оператора и отвечают будущим условиям:

Уровень освещения соответствует традиционным гигиеническим стандартам, установленным для использования самолета по аналогии;

Размерности и освещенности в помещении задается в рабочей плоскости, а пространство между пространствами не резко контрастируется;

Освещает источники света и другие предметы в освещении;

Искусственные комнатные системы освещения используют сочетание естественного света, искусственное освещение, независимо от освещения defektnaturalnogo приближалось их спектральный состав ЛДЦ (лампы дневного света улучшеной цветопередачи), чтобы улучшить флуоресцентные лампы, используемых в помещение.

Из-за размера дискриминации оператора 0,15 мм пространство, необходимое для расчета количества используемых ламп, может быть отнесено к одной категории визуальных работ (высокоточная работа), чтобы обеспечить удовлетворительную удовлетворительную категорию освещения. Из-за того, что разрядность - визуальная работа 1 г, освещение должно быть 400 лк. Чтобы обеспечить этот свет, люминесцентные лампы ЛДЦ -80 просят себе потолок с потолочной лампой, которая оснащена общим освещением (четырехламповые). комната имеет следующие размеры: A 4.85 m = длина, ширина B = 4,3 метра, высота H = 2,5 м, белый потолок, настенный светильник:

Коэффициенты отражения потолка стен пола, соответственно равны ρ

$ï = 70\%, \rho$

$ñ = 50\%, \rho$

$Ï = 30\%$

Для данного помещения уровень рабочей поверхности (стол) над полом

$h_1 = 0,75ì$.

Определим расстояние между рабочей поверхностью (стол) и потолком:

$$h_p = H - h_1, (5.1)$$

$h_p = 2,5 - 0,75 = 1,75ì$

У данного типа на и выгоднейшее отношение.

$$\lambda = \frac{L}{h}, (5.2)$$

λ =1,4

где:

L - расстояние между рядами светильников, м.

H - высота подвеса, м.

h_p –расчетная высота.

Определим расстояние между рядами светильников.

$$L = \lambda * h, (5.3)$$

$L = 1,75*1,4 = 2,45ì$

тогда число рядов светильников будет =2

Расстояние между стенами и верхними лампами определяется по следующей формуле:

$$L = 0,3*L, (5.4)$$

$L = 0,3*2,45 = 0,7ì$.

С учетом значений коэффициента $ðñ$, $ðí$.

При

$$I = \frac{A*B}{h*(A+B)}, (5.5)$$

$$I = \frac{4,85*4,3}{1,75*(4,85+4,3)} = 1,3$$

тогда коэффициент использования светового потока равен $\eta = 0,48$. Номинальный световой поток лампы ЛДЦ-80 равен $F_{Ë} = 2720ëì$.

Следовательно световой поток светильника, равен

$$F_{ÑÂ} = F_{Ë} * n, (5.4)$$

Где:

$n = 4$ число лампа в светильнике.

Тогда:

$$F_{CB} = 2720*4 = 10880ëì$$

Определим необходимое число светильников в ряду по следующей формуле:

$$N_{ë} = \frac{E_{í} * S * Z * K_{Ç}}{n * Ô * \eta}, \ (5.6)$$

где $Z = 1,1$-коэффициент неравномерности освещения;

$K = 1,5$- коэффициент запаса, учитывающий запыление светильников, при условии чистки светильников не реже двух раз в год;

n- число рядов светильников.

Подставим известные значения в формулу (5.5) и определим число светильников в ряду:

$$N_{ё} = \frac{400*1,5*36*1,1}{2*10880*0,48} = 3.$$

Схема расположения светильников на потолке помещения приведена на рисунке 2.1.

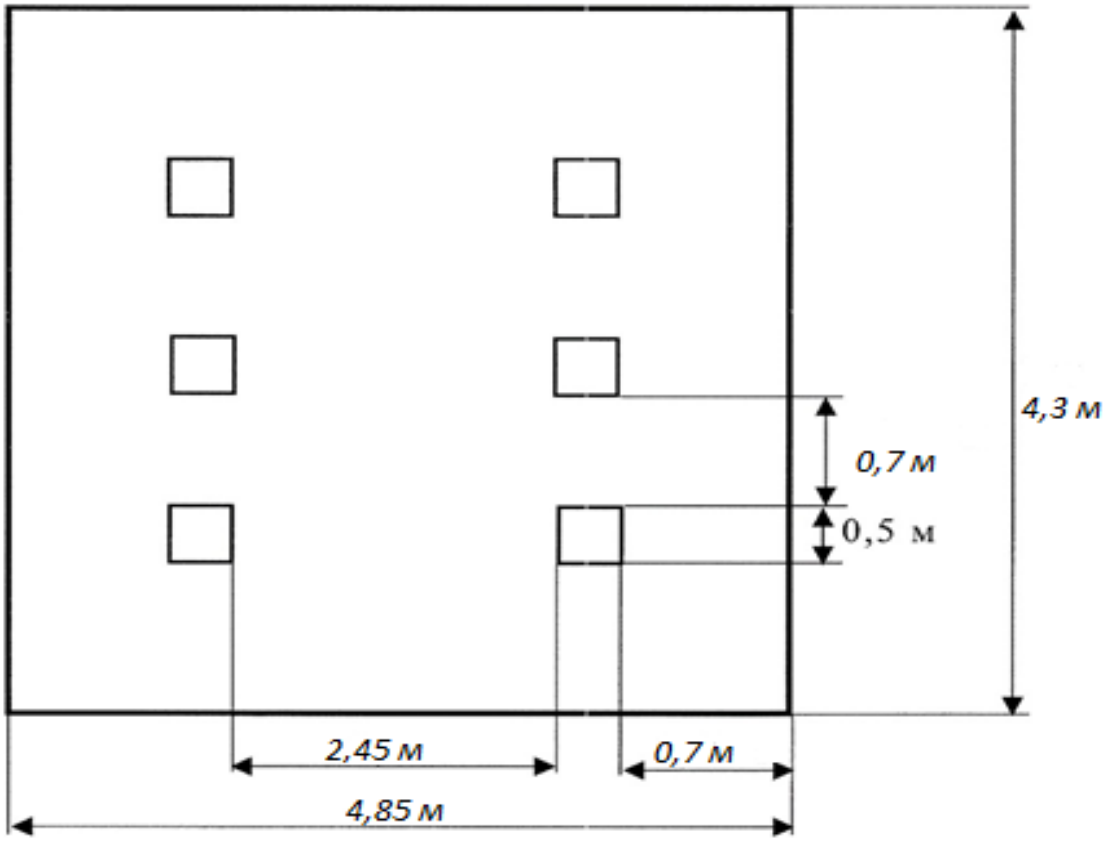

Рисунок 2.1-.План помещения операторской с размещением светильников.

5.3 Пожарная безопасность

Согласно Приложению 2. 2.04.09-84 Компания занимается пожарной безопасностью, функциональным назначением и скоростью сжигания СНиП загрузка легковоспламеняющихся материалов, помещение для участников комнаты в следующей комнате, установка дизельных двигателей, расположенная в первой группе, относящейся к категории В. Категория В, относится к и т.д.

Чтобы закрыть акустические и эстетические строительные материалы, изоляцию стен, дверей, полов, электрических кабелей, сигнальных кабелей,

радиодеталей, кабели подключения к клеточных тел изоляции обмотки, загрязнения и компьютерных элементов для очистки жидкостей и горючих компонентов в домашних условиях.

Источники цепей зажигания для электронных компьютеров, оборудование, используемое для оборудования, кондиционеры и т. д. может быть.

Благодаря дорогостоящему оборудованию в помещении, и многие процессы выполняются в автоматическом режиме, на самом деле вы должны автоматически установить систему пожаротушения с газовым потоком.

Как гасящий огонь агент, используется объединенный состав углекислого углекислотно хладоновый.

Расчетная масса комбинированного углекислотно- хладонового состава md кг, для объемного пожаротушения определяется по формуле:

$$md = k * gn * V, \quad (5.7)$$

где $k = 1,2$- коэффициент компенсации не учитываемых потерь углекислотно-хладонового состава, $gn = 0,4$-нормативная массовая концентрация углекислотно хладонового состава,

V-объем помещения,

$$V = A * B * H, (5.8)$$

где: $À = 4,85ì$ -длина помещения,

$Â = 4,3ì$ B=4,3м-ширина помещения,

$H = 2,5ì$ -высота помещения.

Тогда:

$$V = 4,85 * 4,3 * 2,5 = 52,14ì^3.$$

Следовательно:

$$md = 1,2 * 0,4 * 52,14 = 25,03êã$$

В случае открытых площадок с закрытой площадью от 1% до 10% от площади пола необходимо использовать дополнительные хлорированные углекислые композиции 5 кг на 1 $ì^2$.

Ориентировочное количество цилиндров ε составляет 25 килограммов на 25 литров диоксида углерода на основе 40 литров.

Диаметр диаметра определяется внутренним диаметром главной трубы d_i мм по формуле

$$d_i = 12 * \sqrt{2} = 17 ì\ ì$$

Эквивалентная длинна магистрального трубопровода I_2 определяется по формуле:

$$I_2 = k_1 * I, (5.9)$$

Где $k_1 = 1,2$ -коэффициент увеличения длины трубопровода для компенсации не учитывающих местных потерь, $I = 33M$ -длина трубопровода по проекту тогда,

$I_2 = 1,2 * 33 = 40 ì$.

Площадь сечения выходного отверстия оросителя $À_ç$, $ì\ ì^2$ определяется по формуле:

$$À_ç = \frac{S}{\varepsilon_1}, (5.10)$$

Где: S-площадь сечения магистрального трубопровода, $ì\ ì^2$; ε_1-число оросителей, тогда

$$À_ç = \frac{3,14 * 8,52}{3} = 75 ì\ ì^2$$

Расход углекислотно-хладонового состава Q,кг/с, в зависимости от эквивалентной длины и диаметра трубопровода равна 1,4 кг/с

Расчетное время подачи углекислотно -хладонового состава t, мин, определяется по формуле:

$$t = \frac{md}{60Q}, (5.11)$$

$$t = \frac{43}{60 * 1,4} = 0,5 ì\ èí.$$

Масса основного запаса углекислотно-хладонового состава m, кг, определяется по формуле:

$$m = 1,1 * md(\frac{1 + k_2}{k}), (5.12)$$

где $k_2 = 0,2$-коэффициент учитывающий остаток углекислотно-хладонового состава в баллонах и трубопроводах тогда:,

$$m = 1{,}1 * 25{,}03 * (\frac{1+0{,}2}{1{,}2}) = 27{,}53 \hat{e}\tilde{a}$$

Таким образом из полученных результатов можно сделать вывод, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 2 баллона углекислотно-хладонового состава вместимостью 40 литров, с массой смеси 25 кг и рабочим давлением 12,5 МПа. В помещении установлено 3 оросителя, продолжительность выпуска заряда составляет 0,5 с.

Расстояние между двумя струйными струями в сардакине составляет более 4 метров, а от сопел до стен не более 2 метров.

Автоматические установки для газового пожаротушения имеют автоматические пусковые устройства в соответствии с ГОСТ 12.4.009-83

Основной и распределительный трубопроводы выполнены из стальных труб ГОСТ 8734-75.

Кроме того, есть ручные огнетушители, плакаты, запрещающие использование открытых провокационных сообщений, пожарных экранов и плакатов, курящих курить, так как есть дымовой детектор ионизационного типа, расположенный на потолке на высоте 2,45 м.

ЗАКЛЮЧЕНИЕ

Функциональная безопасность необходима не для всех классов современных систем и прикладных программных средств. Для обеспечения функциональной безопасности целесообразно выявлять и описывать общие характеристики и атрибуты критически оцениваемого критерия в соответствии с требованиями ISO 12182 (Классификация программного обеспечения). Стандарт делится на три различные группы характеристик: внутренние виды; типы среды и типы данных. Для каждого типа отображается список классов, поэтому рекомендуется выбрать подходящие описания для указания конкретных функций конкретной системы или для более широкого использования ПК. Для их функциональной безопасности общее количество трех типов, три из 16 классов и общая спецификация более 100 ПС: - функциональность прикладного программного обеспечения - системы или системы управления технологическим процессом; объем системы - оборудование и процессы и объекты управления объектами; рабочий режим обработка данных в реальном времени; масштаб, ПС- средний или большой объем; представление данных - предмет или объект;

Критика ПС- возможность вызвать высокие, дорогие имущественные или человеческие угрозы жизни; класс пользователей - технические средства и квалифицированные специалисты; стабильность ПС- потенциальное или дискретное изменение; доступность программного продукта для фактического использования в системе ; требуемая производительность: объем памяти - средний или низкий; время отклика быстрый, второй; производительность - небольшая или средняя; высокая безопасность и надежность; компьютерные системы и окружающая среда - микропроцессорное управление и системы реального времени.

Требования к вычислительным ресурсам - высокое, почти полное использование ресурсов для базовых функциональных целей.

Общее представление о характеристиках качества программных средств международным стандартом ISO 9126 рекомендуется отражать тремя взаимодействующими и взаимозависимыми метриками характеристик качества, описывающими: процессы, модификации и внутреннее качество разработки цикла разработки ПС; внешнее качество, отраженное в описании конечного продукта, по спецификациям заказчика.

Эффективность удовлетворения потребностей пользователей с учетом качества и ресурсов, используемых при нормальной эксплуатации. Метрики включают в себя промежуточные компоненты и продукты, включая систему идентификации ПС, а также требования и требования. Необходимые условия для достижения качества использования. Качественные внутренние атрибуты качества внешней среды являются необходимыми условиями для необходимого жизненного цикла и разумного внешнего поведения.

Измерения будут проводиться с точными позициями и качественными субхарактеристиками ПС характеристик и атрибутов трех уровней детализации, которые должны быть выделены для их выбора, могут быть представлены его функции, категории обязанностей, безопасность и номинальная шкала, ее значимость - характеристики и общие характеристики категории, описания, рефлексивных наборов - категорий, свойств; число представляет собой непрерывное или дискретное украшение, представляющее собой набор точек порядка, а также заданный интервал или относительный диапазон, но это объективная мера и количественное требование; качество - (- не хорошо - плохо) очки классифицируются по категориям или категориям - более или менее персонализированные свойства, отобранные и в основном субъективные и оцененные экспертом.

Программные функции реализованы в определенной аппаратной, операционной и пользовательской среде, что существенно влияет на функциональность. Для выполнения необходимых функций программного комплекса соответствующие объекты внешней среды должны быть снабжены соответствующей информацией, содержание которой должно быть полностью реализовано. Полнота дизайна номенклатуры является одним из наиболее важных компонентов при определении функциональной пригодности ПС в соответствующей внешней среде, чтобы гарантировать, что структура и качество входной информации используются для выполнения требуемых функций.

Цель и функции ПС реализуются тогда, когда выходная информация достигает потребителей объектов или операторов-пользователей с требуемым содержанием и качеством, достаточным для обеспечения её эффективного применения. Содержание этой информации определяется конкретными задачами системы, их основными техническими, экономическими и социальными показателями эффективности и отражается в существующих критериях. Степень, в которой предоставляется вся исходящая информация: цель, задачи и функции ПС для пользователей должны рассматриваться как основная мера функциональной пригодности. Начиная с информации о простоях, отслеживая и оценивая соответствие и полноту определения ПС, независимо от объема системы, необходимо заполнить выбор основных характеристик замещения функционального качества пригодности.

Список использованных источников

1.ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. [Текст]. – Введ. 2012-03-01 -М.: Стандартинформ, 2011

2.ISO/IEC 25001:2014 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Planning and management. – (https://www.iso.org/standard/64787.html)

3.Исмаил Е.Е. Характеристики качества программных средств космического назначения: монография. – Saarbrücken: Изд-во LAP LAMBERT Academic Publishing, 2015. - 213 с. ISBN: 978-3-659-79520-6,

4.ECSS-Q-ST-80C Rev.1: 2017 Space product assurance. Software product assurance. - (http://ecss.nl/standard/ecss-q-st-80c-rev-1-software-product-assurance-15-february-2017/)

5.ECSS-Q-HB-80-03A: 2012 Space product assurance. Software dependability and safety. – (http://ecss.nl/hbstms/ecss-q-hb-80-03a-software-dependability-and-safety/)

6.СТ РК ECSS-Q-ST-80C-2012 Гарантия космической продукции. Гарантия качества программного обеспечения [текст]. – Введ. 2013–07–01. – Астана, 2012. – 98 с.: ил.

7.ГОСТ Р ИСО/МЭК 25040-2014 Требования и оценка качества систем и программного обеспечения (SQuaRE). Процесс оценки. определения [Текст]. – Введ. 2015-06-01. – М.: Стандартинформ, 2014

8.ISO/IEC 25030:2007 Software engineering - Software product Quality Requirements and Evaluation (SQuaRE)- Quality requirements. – (https://www.iso.org/obp/ui/#iso:std:iso-iec:25030:ed-1:v1:en

9.Характеристики качества программного обеспечения и методы их оценки Лозинин А.И., Шубинский И.Б. 2009

10.Липаев В.В. Экономика производства программных продуктов. Издание второе. – М.: СИНТЕГ. 2011

11.Липаев В.В. Экономика производства сложных программных продуктов. – М.: 2008.

12.Липаев В.В., Надежность и функциональная безопасность комплексов программ реального времени. –М.: Изд. Светлица. 2013

13.Липаев В.В., Программная инженерия сложных заказных программных продуктов. Изд. Макс - пресс. 2014

14.Липаев В.В. Функциональная безопасность программных средств. – М.: 2004.

15.Липаев В.В. Обеспечение качества программных средств. Методы и стандарты. – М.: 2001.

16.Липаев В.В. Выбор и оценивание характеристик качества программных средств. Методы и стандарты. – М.: 2001.