МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**
Кафедра математической кибернетики и компьютерных наук

АНАЛИЗ РАЗВИТИЯ АВАРИЙНЫХ КОМБИНАЦИЙ СОБЫТИЙ В СИСТЕМЕ «ЧЕЛОВЕК-МАШИНА-СРЕДА»

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 411 группы
направления 02.03.02 — Фундаментальная информатика и информационные технологии
факультета КНиИТ
Копытова Михаила Александровича

Научный руководитель
профессор, д. т. н., доцент _____ А. С. Богомолов

Заведующий кафедрой
к. ф.-м. н., доцент _____ С. В. Миронов

Саратов 2022

ВВЕДЕНИЕ

Актуальность темы

Безопасность — многоплановая проблема, которая должна быть разрешена известными способами еще до того, как отсутствие правильного решения приведет к неблагоприятному инциденту.

Первый шаг к ликвидации опасностей состоит в их выявлении, т.е. идентификации. Необходимо определить потенциальные источники опасности, которые могли и не вызвать аварий до сих пор; выявить опасности, которые маловероятны, но которые могут привести к серьезным последствиям; устранить из рассмотрения опасности, которые практически неосуществимы.

Оценка каждой опасности включает изучение вероятности ее появления, а также серьезности травм персонала, повреждений систем, зданий и пр. компонентов производства, а также экологического ущерба, к которым может привести авария. Опасности должны быть сравнимы, это необходимо для их ранжирования. Для успешного анализа опасностей необходимо провести изучение контрмер по отношению к каждой из опасностей, что добавляет еще одно направление при проведении анализа, так как в последующем принимаемые решения будут связаны с компромиссами среди альтернативных решений.

Функционирование человекомашинных систем сопровождается сложным взаимодействием разнородных процессов. Для предотвращения аварий и катастроф в таких системах требуется анализировать эти процессы, что предполагает использование причинно-следственных схем событий, которые их характеризуют и программного обеспечения для их анализа

В современных программных комплексах по расчету надежности динамика в определенном смысле учитывается, например, в RELEX (США) реализована возможность задания динамических операторов дерева отказов, учитываются временные соотношения. Находят широкое применение и другие программные комплексы: A.L.D.Group (Израиль), ISOGRAPH (Великобритания), Risk Spectrum (Швеция). Эти продукты реализуют достаточно широкий спектр функций, однако обладают такими недостатками, как высокая стоимость, технологическая зависимость, необходимость специального обучения персонала. Из отечественных разработок для структурно-логического моделирования надежности и безопасности имеются Арбитр, ПК АСМ, ПК Универсал, отличающиеся меньшим спектром предоставляемых инструментов, но в большей степени реа-

лизующие отдельные оригинальные функции и результаты.

Перечисленные программные комплексы имеют высокую стоимость и предъявляют высокие требования к компьютерам, кроме того, достаточно сложны и для работы с ними требуется обучение. Поэтому достаточно часто для исследований в области логико-вероятностного анализа безопасности требуется компактные и мобильные утилиты для анализа причинно-следственных структур и их базовых объектов.

Цель бакалаврской работы — разработка и использование компактного мобильного ПО для анализа путей развития и предупреждения аварийных комбинаций событий путем исследования минимальных сечений и путей успешного функционирования деревьев отказов (событий) в системе "человек-машина-среда".

Поставленная цель определила следующие задачи:

1. исследование теоретического материала;
2. постановка проблемы аварийных комбинаций событий;
3. предложить критерий для определения рациональных путей предупреждения аварий на среднесрочных периодах и решить задачу с этим критерием;
4. обзор и выбор инструментальных средств решения задачи разработки программных средств;
5. разработка и программная реализация средства анализа деревьев отказов путем фильтрации и анализа минимальных сечений и путей успешного функционирования;
6. тестирование и отладка программного средства;
7. использование приложения в научном исследовании вопроса определения рациональных путей предупреждения аварий на среднесрочных периодах.

Методологичесские основы анализа развития аварийных комбинаций событий в системе «человек-машина-среда» представлены в работах Богомолова А. С., Косицына А. А., Мельникова А. Ю., Ларичева О. И., Сихомбинга Ф., Рябинина И. А.

Теоретическая и практическая значимость бакалаврской работы

В ходе бакалаврской работы рассматривается проблема развития аварийных комбинаций событий и определяется критерий для нахождения рациональных путей предупреждения аварий на среднесрочных периодах. Далее с помощью представленного теоретического материала реализовывается программа и

с её помощью решается задача, используя определенный ранее критерий. Таким образом, получаем полностью работоспособное компактное переносное приложение, имеющее все основные функции для анализа минимальных сечений и путей успешного функционирования деревьев отказов. Причем по сравнению с аналогичными программами, построенное приложение является интуитивно понятным, абсолютно бесплатным и не требует получения каких-либо лицензий на его использование.

Структура и объём работы

Бакалаврская работа состоит из введения, 4 разделов, заключения, списка использованных источников и 3 приложений. Общий объем работы – 61 страниц, из них 44 страниц – основное содержание, включая 19 рисунков и 6 формул, список использованных источников информации – 21 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Первый раздел «Проблема аварийных комбинаций событий» посвящен проблеме предупреждения аварий в системе «человек-машина-среда». В разделе описывается формальная постановка задачи предупреждения аварий и представлен процесс решения задачи развития аварийных комбинаций событий.

Аварийной комбинацией событий называется совокупность дефектов техники, программного обеспечения и человеческих ошибок, относительно неопасных по отдельности, но приводящих к аварии при возникновении в определенном порядке на определенном отрезке времени.

Полагаем, что аварии являются следствиями развития критических комбинаций небольших событий. Первым этапом решения задачи будет определение состава и структуры аварийных комбинаций. Для изображения связи между авариями и этими событиями будем использовать логико-вероятностный анализ безопасности и рассматривать деревья отказов с их минимальными сечениями. Для первого этапа решения задачи — определения аварийных комбинаций событий — нам потребуется разработать совокупность деревьев отказов, характеризующих развитие аварий из различных событий в системе.

В качестве корневой вершины дерева отказов будем рассматривать событие — неудачу в выполнении задания, аварию. Каждое минимальное сечение дерева отказов соответствует одному или нескольким сценариям развития этой аварии. В качестве концевых событий (листьев) дерева отказов целесообразно рассматривать события, на которые при управлении системой могут быть оказаны предупреждающие или парирующие воздействия.

Второй раздел «Анализ деревьев отказов» посвящен вопросам, касающимся определения и анализа деревьев отказов.

Дерево отказов представляет собой иерархическую структуру, отражающую причинно-следственные связи событий при развитии ситуации, отражаемой корневой вершиной.

Анализ деревьев отказов обычно применяется в качестве основного метода при анализе надежности больших систем. Дерево отказов представляет собой логическую блок-схему, состоящую из вершинного события (представляемого корнем), промежуточных событий и нижних событий (представляемых листьями). Оно используется для описания внутренней функциональной логической взаимосвязи между событиями. Логические взаимосвязи между компонентами

системы и их событиями получаются на основе принципов работы и отказов механизмов системы. Вероятность отказа системы верхнего уровня может быть получена с помощью логической взаимосвязи между уровнями событий и с помощью данных о вероятности отказов базовых компонентов системы. Затем может быть выполнена оценка надежности на системном уровне. Метод анализа деревьев отказов, основанный на вероятностной модели, нашел широкое применение в нескольких областях системной инженерии, таких как авиация, аэрокосмическая промышленность и ядерная энергетика.

Анализ деревьев отказов полезен в машиностроении, особенно в отраслях, где отказ может иметь серьезные последствия, таких как ядерная энергетика или авиация. Однако, анализ дерева отказов также может быть использован при разработке программного обеспечения для отладки сложных систем. Такой метод также используется в проектировании и диагностике, т.к. имеет возможность без значительных дорогих по ресурсам изменений выявлять потенциальные отказы и исправлять события верхнего уровня. [**?**]

При анализе деревьев отказов используются логические символы чтобы связать неисправности на более низких уровнях системы путем проверки основных событий для выявления причин сбоев на системном уровне. Дерево отказов отображает состояние системы путем проверки состояния элементарных событий в этой системе, используя логические символы и символы событий, т.е. с помощью методов булевой алгебры.

Анализ деревьев отказов можно представить в виде алгоритма, состоящего из 5 основных шагов:

1. Определение нежелательной ситуации, анализ основной неисправности;
2. Сделать вывод о непосредственных причинах события;
3. Продолжать анализ нежелательного события до тех пор, пока не будут выявлены самые базовые причины;
4. На основе полученных данных о причинах нежелательного события начинаем построение дерева отказов;
5. Оцениваем выполненный анализ дерева отказов.

В третьем разделе «Реализация программы для поиска минимальных сечений дерева отказов» описывается пошаговый процесс создания приложения и его тестирование на примере.

Для написания программы выбран язык JavaScript из-за удобства пользовательского интерфейса, мощной экосистемы и производительности. Получаем, что на языке JavaScript написана программная часть, т.е. все функции. На HTML и CSS описан интерфейс программы.

Сборка программы в полноценное приложение происходит с помощью фреймворка Electron. Electron — это фреймворк для разработки настольных приложений с использованием HTML, CSS и JavaScript. Такие приложения могут работать на различных платформах. Помимо этого, с помощью Electron можем производить как установщик нашего приложения, так и переносную версию, которую достаточно лишь запустить.

Интерфейс программы представлен на рисунке 1.

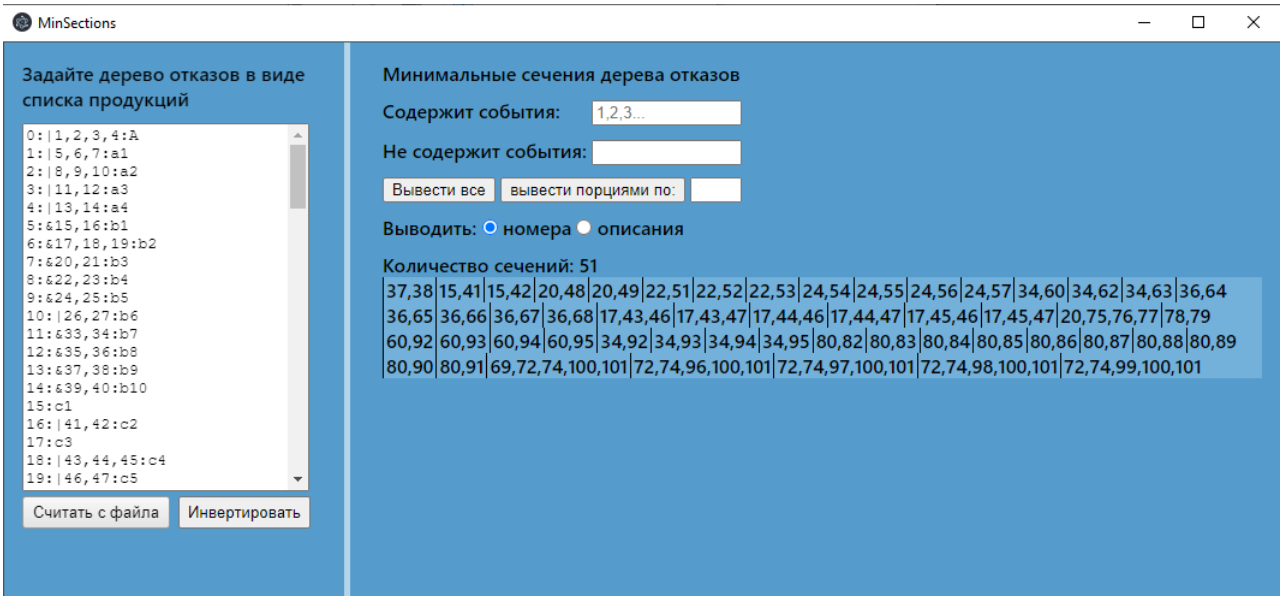

Рисунок 1 – Интерфейс программы

Тело нашей программы можем разделить на 2 части. Первая часть содержит текстовую область ввода совокупности продукций, кнопки чтения списка продукций из файла и инвертирования логических отношений между событиями нашего дерева отказа. Вторая часть — результат выполнения программы. В данной части предусмотрена возможность для отбора или отбрасывания определенных событий (или связанных с ними) из совокупности событий всех минимальных сечений. Так же реализована возможность вывода как сразу всех минимальных сечений, соответствующим нашим условиям выбора, так и по

некоторым порциям, размер которых можно задать вручную. И наконец сам вывод может быть представлен в двух видах: вывод только номеров событий или вывод преимущественно описаний событий (если таковых не имеется, выводится номер). При выполнении вывода мы получаем значение с количеством отобранных минимальных сечений и сам список полученных сечений.

Рассмотрим корректность работы реализованной программы на примере дерева отказов в процессе функционирования беспилотной системы. (Рисунок 2)

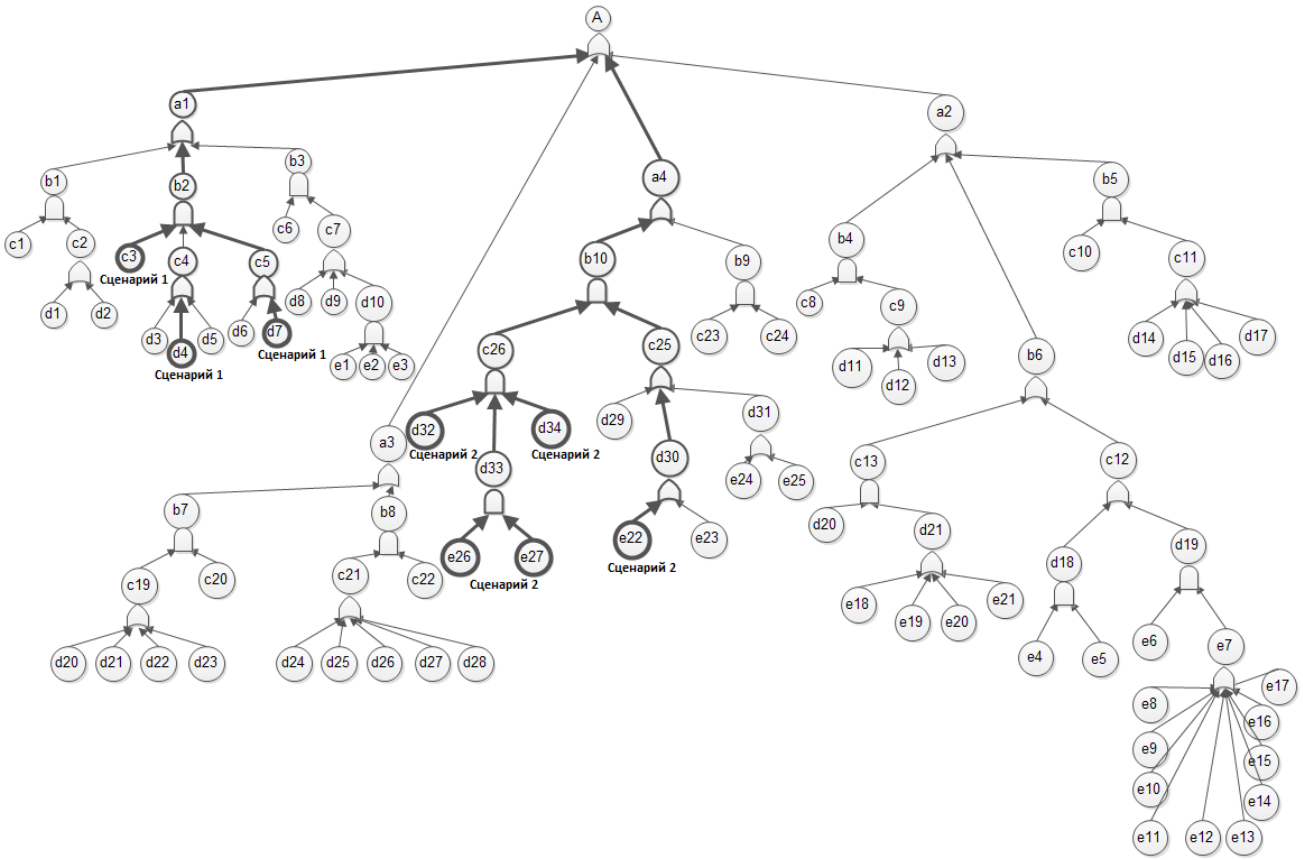

Рисунок 2 – Фрагмент дерева отказов в процессе функционирования беспилотной системы

Известно, что множество минимальных путей успешного функционирования дерева отказов совпадает с множеством минимальных сечений этого инвертированного дерева. Найдем первые 30 таких путей. Для этого нам необходимо инвертировать наше дерево. После инвертирования можем искать пути успешного функционирования. Результат работы программы отображен на рисунке 3.

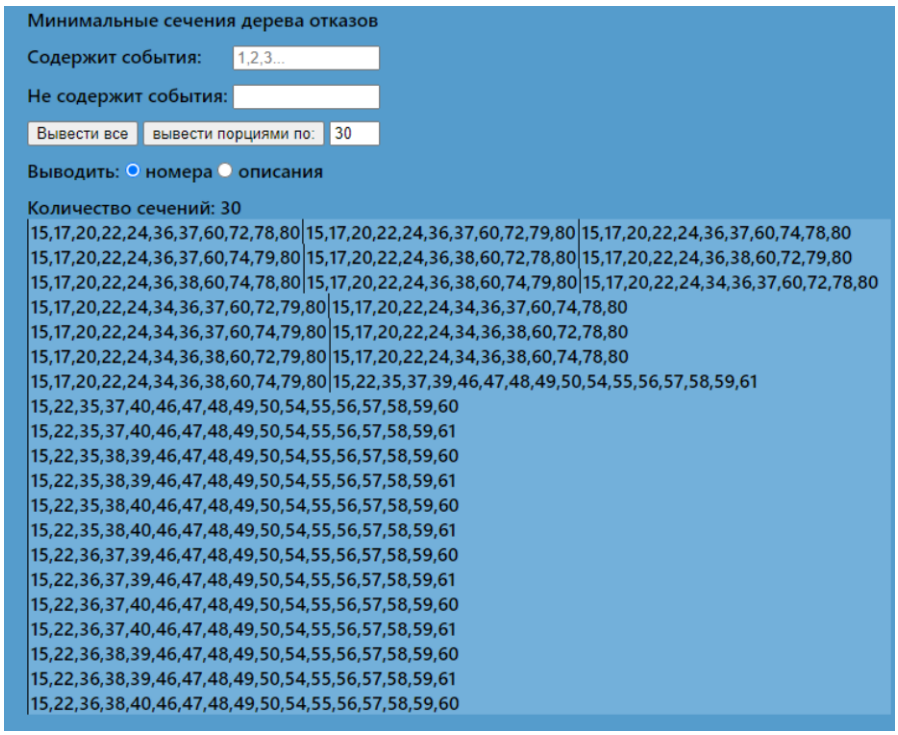

Рисунок 3 – Построение путей успешного функционирования

В конечном итоге определим общее количество минимальных сечений и путей успешного функционирования в нашем дереве отказов. Для этого заново инвертируем список продукций, которым представлено дерево, в исходный вид. Очищаем поля фильтрации, нажимаем кнопку вывода и получаем, что дерево отказов имеет 51 минимальное сечение. Далее необходимо найти пути успешного функционирования дерева. Снова инвертируем дерево отказов и теперь можем вывести все возможные пути. По результатам программы получаем, что дерево содержит 3440 путей успешного функционирования. По полученным результатам делаем вывод, что приложение функционирует абсолютно корректно.

Четвертый раздел «Исследование рациональных путей предупреждения аварий на среднесрочных периодах» посвящен вопросам предупреждения аварийных комбинаций событий на среднесрочных периодах, в частности определение подхода к задаче и способ её решения.

Задача предупреждения аварий на среднесрочных периодах состоит в выборе путей успешного функционирования, которые имеют наименьший вес или затраты с точки зрения заданной весовой функции. Для событий вес назначаются экспертами путем проведения системного анализа.

Пусть для решения задачи предотвращения аварийных комбинаций событий на среднесрочном интервале требуется сделать минимальные пути успешного функционирования практически нереализуемыми. Для этого достаточ-

но исключить (сделать практически невозможными) на исследуемом интервале времени все события любого из минимальных ПУФ.

Допустим, что в результате исследования дерева отказов мы получили несколько путей успешного функционирования. Далее необходимо рассчитать затраты на их реализацию, суммируя веса событий. В результате подсчета получим стоимости ПУФ. Отсюда следует, что решением задачи будет исключение событий, входящих в пути успешного функционирования с минимальной стоимостью, с последующими мероприятиями по их исключению.

Для решения задачи определения наименее затратного по заданному критерию пути предупреждения всех аварий в дереве, нам необходимо реализовать ПО, с помощью которого мы сможем работать с весами событий: по списку всех сечений необходимо определять минимальный и максимальный вес среди сечений, количество сечений с данными весами, а также выводить их на экран.

Реализуем такое ПО путем усовершенствования нашего приложения путем добавления некоторых функций и изменения интерфейса. Для ввода добавляем текстовую область и кнопки, отвечающие за работу с весами, в первый блок, где уже содержится ввод дерева отказов в виде списка продукций. Блок вывода помещаем во второй основной блок, где уже содержится вывод минимальных сечений, но только в правую, свободную часть этой области.

В результате расширенная версия нашей программы принимает следующий вид. (рисунок 4)

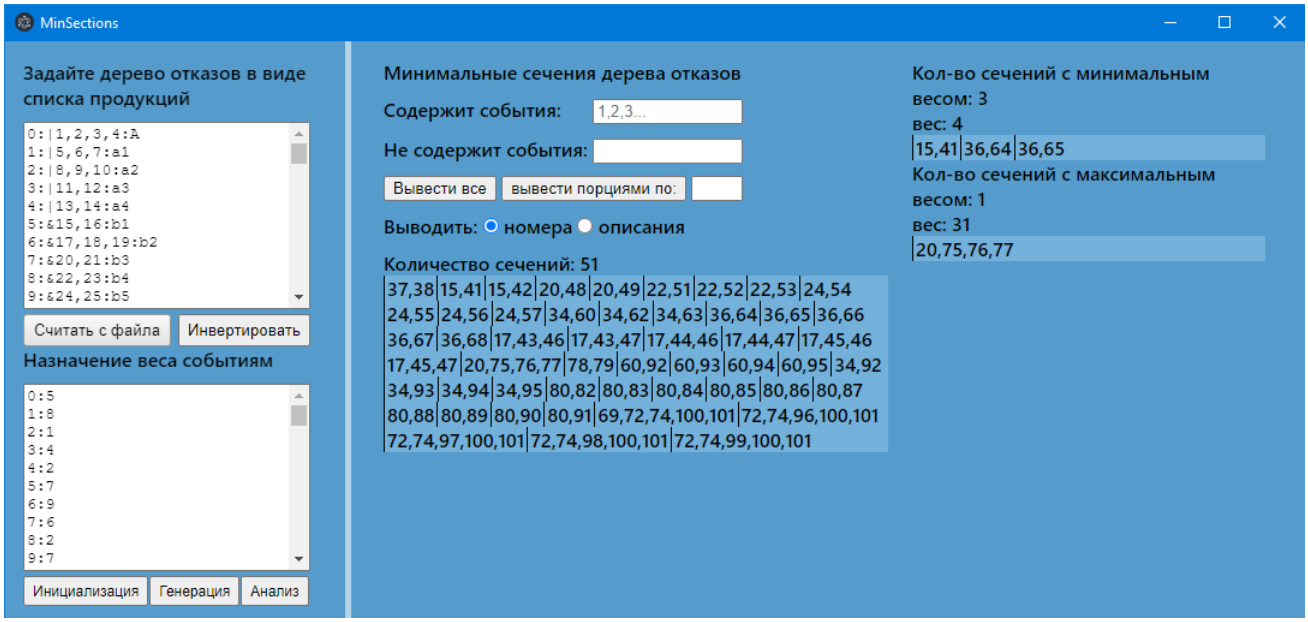

Рисунок 4 – Расширенная версия приложения

ЗАКЛЮЧЕНИЕ

В дипломной работе описывается проблема предупреждения аварий: дали определение аварийной комбинации событий, разобрана постановка проблемы и основной подход к решению данной задачи. Данный подход позволяет выделять минимальные множества неблагоприятных событий, парирование которых дает возможность снизить вероятность аварийных комбинаций до безопасного уровня.

В ходе работы изучены деревья отказов, а именно общие положения и определения, структура деревьев, их особенности использования. Ознакомились с разновидностью логических знаков и символов событий, рассмотрен общий алгоритм для проведения анализа деревьев отказов. Также изучены понятие и свойства минимальных сечений и путей успешного функционирования деревьев отказов.

На основе изученного материала построено приложение, которое может быть использовано для анализа развития аварийных комбинаций событий в системе «человек-машина-среда». Приложение позволяет вводить и редактировать информацию о дереве отказов, определять множество минимальных сечений и его проекцию как множество сечений с заданным событием. Кроме этого, имеется возможность вывода желаемых и нежелаемых событий. Сечения можно выводить как полным списком, так и заданными пользователем порциями, причем имеется возможность вывода событий не только по их номерам, но и по их описаниям. Реализованный алгоритм - один из ключевых алгоритмов логического анализа безопасности. Он также позволяет определять пути успешного функционирования системы, используемые для определения воздействий по предупреждению развития аварий, путем встроенной в приложение возможности инвертирования дерева отказов. Программа отличается мобильностью и компактностью, что дает возможность использовать ее в исследованиях по анализу безопасности без необходимости установки, оплаты и дополнительного обучения сотрудников, а также в рамках импортозамещения зарубежных комплексов для анализа безопасности. Помимо этого, приложение может распространяться как в виде установочного файла, так и в уже предустановленном переносном виде, требующим только запуска.

При написании работы произведено исследование вопроса предупреждения аварий на среднесрочных периодах с использованием рациональных путей

успешного функционирования и варианта нахождения таких рациональных путей. Для этого экспертам необходимо взвесить каждое событие, после чего искать пути, наименее затратные по ресурсам, с последующими исключением событий, входящих в такие рациональные пути, и проведением мероприятий по их исключению.

Основные источники информации:

1. *Богомолов, А. С.* Анализ путей возникновения и предотвращения критических сочетаний событий в человеко-машинных системах / А. С. Богомолов // *Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика.* — 2017. — Т. 17, № 2. — С. 219–230.
2. *Косицын, А. А.* Мониторинг аварийных комбинаций событий при обследовании промышленных объектов беспилотными летательными аппаратами / А. А. Косицын, А. С. Богомолов, В. А. Кушников, В. А. Иващенко, Д. В. Сердечный // *Системы управления и информационные технологии.* — 2022. — № 2(88). — С. 65–70.
3. *Мельников, А. Ю.* Использование метода дерева отказов для расчета показателей надежности персонального компьютера / А. Ю. Мельников, Ю. А. Соломко. — 2016.
4. *Ларичев, О. И.* Теория и методы принятия решений / О. И. Ларичев. — Москва: Логос, 2000.
5. *Рябинин, И. А.* Надежность и безопасность структурно-сложных систем / И. А. Рябинин. — СПб: Политехника, 2000.
6. *Богомолов, А. С.* Предотвращение аварийных комбинаций событий при управлении человеко-машинными системами / А. С. Богомолов // *Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика.* — 2019. — Т. 19, № 2. — С. 197–202.
7. *Sihombing, F.* Parallel fault tree analysis for accurate reliability of complex systems / F. Sihombing, M. Torbol // *Structural Safety.* — 2018. — Vol. 72. — Pp. 41–53.