Fundamentals of smart grid safety analysis and assurance
Practicum
E. Brezhnev
Edited by V.S. Kharchenko

Methods and software tools for smart grid reliability and safety assessment

Fuzzy methods and tools of smart grid degradation assessment

Methods and software tools for smart grid safety assurance

Fundamentals of smart grid safety analysis and assurance. Practicum

PRACTICUM

FUNDAMENTALS OF SMART GRID

SAFETY ANALYSIS AND ASSURANCE

2017

Co-funded by the Tempus Programme of the European Union

Министерство образования и науки Украины
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»

Е.В. Брежнев

Основы анализа и обеспечения безопасности смарт грид

Fundamentals of smart grid safety analysis and assurance

Практикум

Под редакцией В.С. Харченко

Проект
Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains
(543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR)

2017

УДК 004.9+004.052:621.38
Р13

Викладені матеріали практичної частини начального курсу “Основи аналізу та забезпечення безпеки смарт грид” (“Fundamentals of smart grid safety analysis and assurance”), підготовленого в рамках проекту Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

Курс присвячений методології та практиці оцінювання ризиків, безпеки, надійності смарт грид. Приводиться навчальна програма курсу, опис семінарів, практикумів, методичні рекомендації щодо самостійного вивчення курсу.

Книга призначена для аспірантів університетів, що навчаються за напрямками комп’ютерних наук, комп’ютерної та програмної інженерії, при вивченні методів та засобів оцінювання ризиків, безпеки смарт грид, а також може бути корисна викладачам, що проводять заняття з відповідних курсів.

Рецензенты:

– Опанасенко Владимир Николаевич, профессор, доктор технических наук, начальник отдела Института кибернетики им. В.М. Глушкова Национальной Академии наук Украины;

– Сидоренко Николай Федорович, доцент, кандидат технических наук, главный инженер НТ СКБ «Полисвит» (Харьков, Украина), заслуженный изобретатель Украины.

Основы анализа и обеспечения безопасности смарт грид. Практикум / Под ред. Харченко В.С. – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2017. – 134 с.

В пособии изложены материалы практической части учебного курса «Основы анализа и обеспечения безопасности смарт грид» (Fundamentals of smart grid safety analysis and assurance), подготовленного для аспирантов в рамках проекта Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR). Курс посвящен методологии и практике оценивания рисков, надежности и безопасности смарт грид.

Приводится учебная программа курса, дается описание семинаров, практикумов и тренингов, методические рекомендации по самостоятельному изучению материала курса.

Книга предназначена для аспирантов университетов, обучающихся по направлениям компьютерных наук, компьютерной и программной инженерии, при изучении методов и средств оценивания рисков и безопасности смарт грид, а также может быть полезна для преподавателей, ведущих занятия по соответствующим курсам.

Библ. – 29 наименований, рисунков – 75, таблиц – 13.

Рекомендовано к изданию ученым советом Национального аэрокосмического университета имени Н.Е. Жуковского «Харьковский авиационный институт» (протокол № 1 от 16 апреля 2017 г.).

УДК 004.9+004.052:621.38

СПИСОК СОКРАЩЕНИЙ

АСУ	Автоматизированная система управления
АЧР	Автоматическая частотная разгрузка
ИУС	Информационно-управляющая система
ИТ	Информационные технологии
ИУФ	Информационно-управляющая функция
ИС	Инструментальное средство
ЛЛМ	Логико-лингвистическая модель
ПЛК	Программируемый логический контроллер
СБ	Система безопасности
СНЭ	Система нормальной эксплуатации
ЦПС	Цифровая подстанция
CAFTA	Computer Aided Fault Tree Analysis
FMECA	Failure Mode and Effect Analysis
HAZOP	Hazard and Operability Study
NPP	Nuclear Power Plan
RPN	Risk Priority Number
RTU	Remote Terminal Unit
SMART	Self Monitoring Analysis and Reporting Technology
SCADA	Supervisory Control and Data Acquisition Systems
SC	Soft-computing

ВВЕДЕНИЕ

В пособии изложены материалы практической части учебного курса «Основы анализа и обеспечения безопасности смарт грид» (Fundamentals of smart grid safety analysis and assurance), подготовленного для аспирантов в рамках Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains[1] (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

Курс посвящен методологии и практике оценивания, обеспечения рисков, надежности и безопасности смарт грид, нового поколения энергоэффективных систем.

В пособии приводятся описание семинаров, практикумов, в приложениях изложены учебная программа курса и методические рекомендации по самостоятельному изучению материалов курса.

В первом разделе приведены материалы семинара по обзору и применению методов анализа надежности и безопасности смарт грид и их информационно-управляющих систем (ИУС). Теоретический материал содержит краткое описание смарт грид, основные показатели надежности, а также обзор функциональности программных инструментальных средств (ИС), применяемых на этапах проектного анализ надежности и безопасности.

Раздел содержит также описание семинара и практикума, направленного на изучение ИС анализа надежности.

В разделе также приведены лабораторные работы, ориентированные на более глубокое изучение ИС, основанных на реализации методов анализа деревьев отказов.

Разнообразие входных данных, используемых при анализе безопасности, предусматривает возможность интеграции методов

[1]*Этот проект финансируется при поддержке Европейской комиссии. Эта публикация (сообщение) отражает мнения только авторов, и Комиссия не может нести ответственность за любое использование содержащейся в нем информации.*

This project has been funded with support from the European Commission. This publication (communication) reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

оценивания надежности и безопасности в рамках одного подхода. Для ознакомления с возможными способами интеграции в разделе приведена лабораторная работа, направленная на изучение и практическое усвоение способов интеграции ИС.

Во втором разделе представлены практикумы по анализу деградации смарт грид систем (ИУС) с использованием логико-лингвистических моделей. Первый практикум направлен на ознакомление с методами и подходами оценивания многоуровневой деградации. Второй практикум основан на применении Fuzzy Logic Toolbox, позволяющего провести нечеткую оценку деградации с использованием экспертных данных. Изложена методика применения нечеткой логики при решении задачи оценивания многоуровневой деградации.

Третий раздел содержит практикум по обеспечению безопасности смарт грид систем и их ИУС. Приведен обзор основных нормативных документов, используемых для обеспечения безопасности систем критического применения. Приведены этапы метода выбора диверсных систем, основанного на оценивании степени сходства основной и диверсной системы, и учете стоимости реализации диверсного решения. Приведено описание ИС, поддерживающего реализацию данного метода.

Рисунки, таблицы и формулы для удобства нумеруются в пределах каждого раздела.

Книга предназначена для аспирантов университетов, обучающихся по направлениям компьютерных наук, компьютерной и программной инженерии, при изучении методов оценивания и обеспечения надежности, безопасности смарт грид (ИУС), а также может быть полезна для преподавателей, ведущих занятия по соответствующим курсам.

Пособие подготовлено доцентом кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ» к.т.н., с.н.с. Брежневым Е.В. Общее редактирование проведено проф. д.т.н. Харченко В.С.

Автор выражает благодарность рецензентам, а также студенту кафедры компьютерных сетей и систем Мягкому М.В. за помощь в подготовке материалов практической части данного курса.

1 МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ОЦЕНИВАНИЯ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ СМАРТ ГРИД

1.1 Семинар. Обзор и применение методов анализа надежности и безопасности смарт грид

Цель и задачи семинара.

Целью является обзор и применение методов риск-анализа безопасности смарт грид.

Учебные задачи:

– изучение основных положений анализа надежности смарт грид;

– изучение возможностей и ограничений методов анализа безопасности смарт грид;

– изучение подходов к проведению анализа надежности смарт грид.

Практические задачи:

– проведение аналитического обзора методов риск анализа;

– выполнение учебного проекта по оценке методов анализа надежности и безопасности смарт грид;

– приобретение навыков командной работы при выполнении учебного проекта.

Подготовка к семинару

При подготовке к семинару необходимо:

– уяснить цели и задачи;

–изучить теоретический материал, приведенный в описании, а также в [1-12].

Теоретический материал

Smart Grid (далее, смарт грид) представляет собой систему, оптимизирующую энергозатраты, позволяющую перераспределять электроэнергию. "Интеллектуальные" сети – комплекс технических средств, позволяющий оперативно менять характеристики электрической сети. На технологическом уровне

происходит объединение электрических сетей, потребителей и производителей электричества в единую автоматизированную систему, которая в реальном времени позволяет отслеживать и контролировать режимы работы всех участников процесса.

Надежность смарт грид определяется надежностью ее физических активов (генерирующих агрегатов, трансформаторов, линий электропередачи, коммутационных аппаратов, устройств защиты и автоматики и др.), надежностью схемы (степенью резервирования), надежностью режима (запасами статической и динамической устойчивости), а также живучестью системы, т.е. способностью выдерживать системные аварии цепочечного характера без катастрофических последствий, или, без перерывов электроснабжения потребителей, не подключенных к системе автоматической частотной разгрузки (АЧР).

Под надежностью смарт грид понимается комплексное свойство, определяющее способность осуществлять электроснабжение потребителей путем выполнения функций по производству, передаче и распределению электрической энергии нормированного (требуемого) качества при едином технологическом взаимодействии генерирующих установок, электрических сетей и электроустановок потребителей, удовлетворять в любой момент времени спрос на мощность и электроэнергию (адекватность, балансовая составляющая системной надежности), противостоять возмущениям, вызванным отказами отдельных элементов энергосистемы (безопасность, оперативная составляющая системной надежности).

К *частным показателям надежности* относятся: параметр потока отказов - отношение числа отказавших в единицу времени элементов к общему числу испытываемых однотипных элементов при условии, что отказавшие элементы заменяются новыми; наработка на отказ - среднее значение времени между последовательными отказами; время восстановления - отношение суммарного времени восстановления технического устройства за выбранный календарный срок к количеству его отказов за тот же календарный срок; коэффициент готовности - отношение времени безотказной работы технического устройства к суммарному времени его безотказной работы и вынужденных простоев из-за отказов.

К основным интегральным показателям надежности относятся:

- средний индекс длительности прерываний (SAIDI) в работе КЭИ. Этот индекс используется для измерения суммарной длительности прерывания для усредненного потребителя энергии за данный период времени. В качестве временного интервала используется месячный или годовой период. Этот показатель определяется по соотношению вида

$$SAIDI = \frac{\sum r_i N_i}{N_T},$$

где r_i - время восстановления системы после сбоя, мин

N_i - общее число потребителей, которые потеряли энергоснабжение

N_T – общее число потребителей

- средняя величина эксплуатационной готовности (ASAI) определяется как отношение фактического времени наличия энергоснабжения к общему времени. Эта величина определяется как:

$$ASAI = [1 - (\sum (r_i \cdot N_i) / (N_T \cdot T))] \cdot 100,$$

где T – общий период времени, ч;

r_i – время восстановления, ч;

N_i - число потребителей без энергоснабжения;

N_T – общее число потребителей.

Электрическая подстанция является одной из важных систем, обеспечивающей прием, преобразование и распределение электрической энергии. Цифровая подстанция как основной элемент смарт грид, обеспечивает интерфейс между АЭС и электросетью.

К частным показателям надежности подстанции относят вероятность отказа оборудования, среднее время наработки на отказ, интенсивность отказа, время восстановления, коэффициент готовности, пр.

Рассмотренные методы оценивания надежности позволяют учесть влияние надежности на безопасность смарт грид и их ИУС. Вместе с тем, учет только лишь одной надежности не позволяет получить достоверные оценки безопасности в виду ее

многофакторности. Существенным недостатком является отсутствие статистики (редкие события), не позволяющей использовать вероятностные показатели надежности в задачах оценивания безопасности КЭИ. Кроме того, необходимо комплексно учитывать влияние других факторов безопасности (рассмотренных ранее) и учитывать неопределенности, свойственные данной проблеме.

Обзор инструментальных средств оценки надежности смарт грид

Для анализа надежности смарт грид систем применяются следующие инструментальные средства (ИС):

ReliaSoft's Xfmea

Программный инструмент Xfmea ReliaSoft облегчает управление данными и отчетности для всех типов режимов и последствий отказов анализ - FMEA - и режимы отказа, эффекты и критичности анализа - FMECA. Программное обеспечение предоставляет предварительно определенные настройки, чтобы соответствовать основным отраслевым стандартам (например, MIL-STD-1629A), а также предоставляет широкие возможности настройки в соответствии с требованиями конкретного анализа и отчетности.

Xfmea обеспечивает централизованное хранение данных, чтобы сделать его легким для нескольких пользователей сотрудничать по FMEA проектов. Программное обеспечение предлагает гибкий и мощный набор инструментов для:

– Записи и управления данными для текущего режима и последствий отказов анализа (FMEAs);

– Поиска и использования соответствующей информации из существующих FMEAs;

– Оценки риска с помощью RPN или критичности;

– Отслеживания завершения рекомендуемых действий;

– Представления данных FMEA с помощью отчетов, запросов и диаграмм, пр.

Общий вид графического интерфейса ИС приведен на рисунке 1.1.

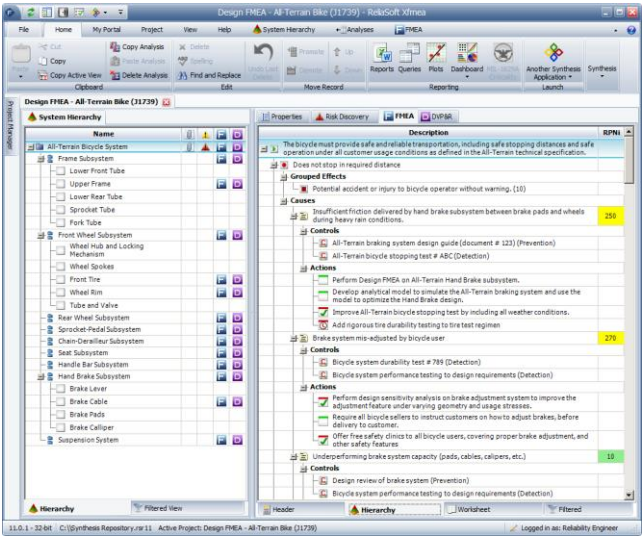


Рис. 1.1. Общий вид графического интерфейса инструментального средства ReliaSoft’s Xfmea

Reliability Block Diagram Analysis Software

BlockSim поддерживает широкий спектр надежности блок - схем конфигураций и анализа дерева неисправностей (FTA) ворот и событий, в том числе расширенные возможности для моделирования сложных конфигураций, распределение нагрузки, в режиме ожидания резервирования, фаз и циклов. С помощью точных вычислений и/или дискретного моделирования событий, BlockSim облегчает широкий спектр анализов для обоих восстанавливаемых и невосстанавливаемых систем, а именно:

– системный анализ надежности;

– определение критических компонентов;

– оптимальное распределение надежности для систем ремонтопригодности, анализа (определения оптимальных

интервалов профилактического обслуживания запасных частей провизия и т.п.);

– оценки стоимости жизненного цикла.

Общий вид графического интерфейса ИС приведен на рис. 1.2.

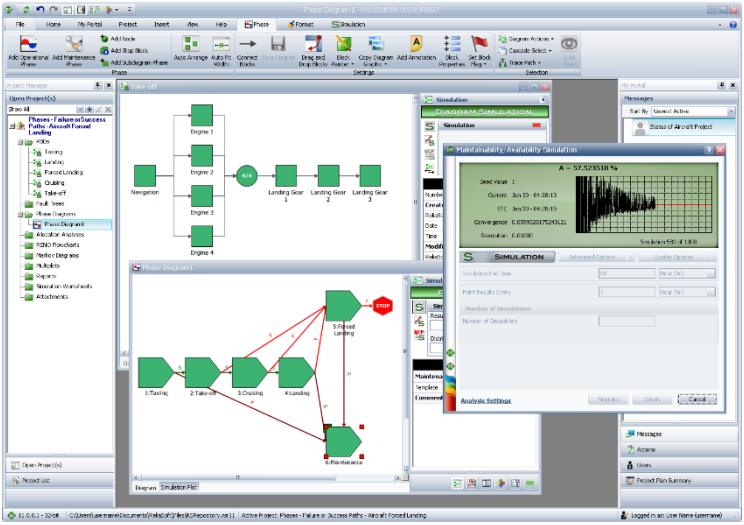


Рис. 1.2. Общий вид графического интерфейса инструментального средства BlockSim Soft.

HAZOP Manager

HAZOP Manager представляет собой программу персонального компьютера для исследования опасности и работоспособности (HAZOPs) и других обзоров, связанных с безопасностью.

ИС включает в себя функции:

– подачи в качестве основы для проведения обзоров безопасности систем;

– облегчения задач записи протокола заседания групп обзора безопасности, а также помощи поддержки фокуса команды при исследованиях;

– поддержка базой данных по причинам аварий (отказов);
– возможности проведения анализа SIL, пр.

Общий вид графического интерфейса инструментального средства, поддерживающего использование данной методологии, приведен на рисунке 1.3.

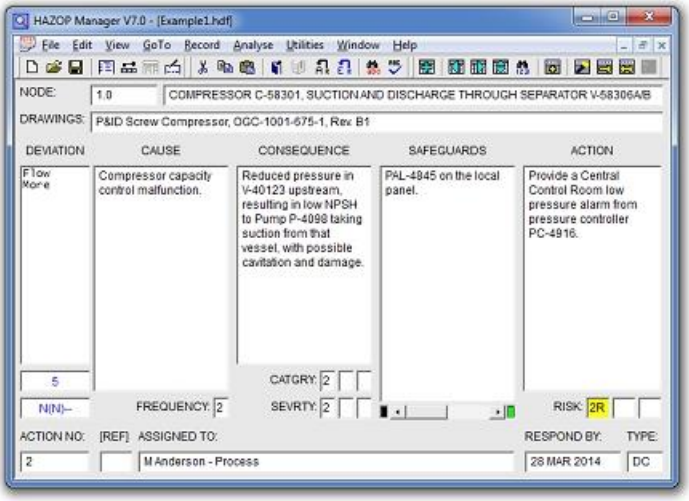


Рис 1.3. Общий вид графического интерфейса инструментального средства HAZOR Manager V7.0.

CAFTA (Computer Aided Fault Tree Analysis (FTA))

CAFTA - это программное приложение, используемое для анализа дерева событий и дерева дефектов сложных систем. Это гибкий, интуитивно понятный инструмент, который может использовать один аналитик риска или целая команда проекта.

FTA обеспечивает дисциплинированный способ разложить сложную систему на составляющие ее части и исследовать места, где общая первопричина влияет на несколько уровней.

CAFTA позволяет:

– визуализировать и упростить понимание взаимодействия между отдельными отказами компонентов и сбоями всей системы;
– провести количественную оценку надежности, пр.

RAMS (надежность, доступность, ремонтопригодность и безопасность)

Программное обеспечение RAM Commander представляет собой комплексное программное средство для анализа надежности, ремонтопригодности и прогнозирования, оптимизации запасных частей, FMEA / FMECA, анализа тестируемости, анализ дерева событий и оценки безопасности. Модули надежности и безопасности покрывают все широко известные стандарты надежности и подходы анализа отказов. RAM Commander является незаменимым инструментом для анализа надежности сложных систем.

Общий вид графического интерфейса ИС приведен на рис.1.4.

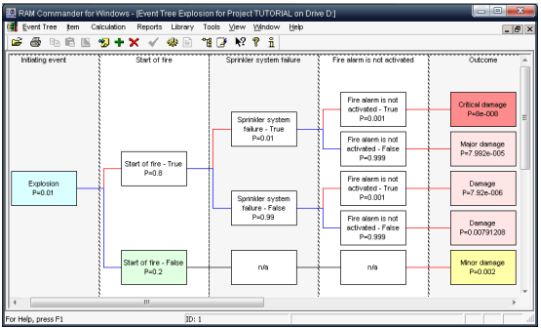


Рис 1.4. Общий вид графического интерфейса инструментального средства RAM Commander

Netica

Netica – это приложение разработанное компанией Norsys Software Corp., которое можно использовать для поиска закономерностей в данных, диагностику системы и т.д. Netica представляет собой комплексный инструмент для работы с байесовской сетью доверия и диаграмм влияния. ИС используется для построения, изучения, модификации БСД.

Общий вид графического интерфейса ИС приведен на рис.1.5.

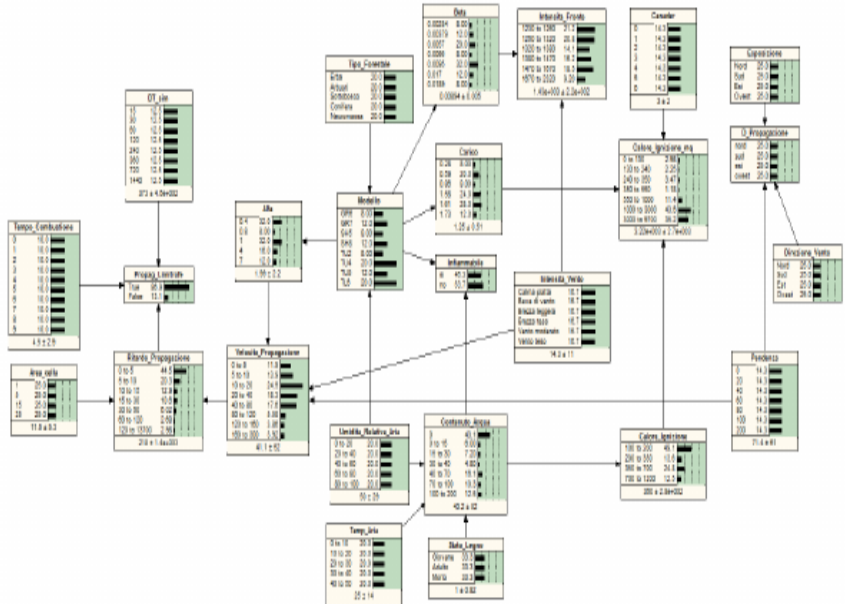


Рис.1.5. Общий вид графического интерфейса ИС Netica

Программа разработок и исследований

Работа выполняется коллективно. Коллективное выполнение работы состоит в следующем. Студенты распределяются на команды. Каждая команда получает задачу, связанную с подготовкой учебного проекта по сравнительной оценке двух ИС анализа надежности.

Этапы создания учебного проекта:

1. Формирование команд. Распределение ролей в команде.
2. Выбор группы методов.
3. Постановка целей.
4. Постановка задач.
5. Внутрикомандная работа (дискуссия).
6. Презентация результатов.

Сравнительная оценка ИС включает:

- составление и заполнение чек-листа для описания ИС.

Секции чек-листа для описания ИС представлены в табл. 1.1

Таблица 1.1. Секции чек-листа для описания ИС

№	Секции для описания
1.	Идентификация ИС (функция, имя, производитель и номер версии)
2.	Описание функционала ИС
3.	Наличие руководства пользователя (со ссылкой)
4.	Сфера (области) применения ИС (список типичных применений)
5.	Оценка практик управления тестированием и изменениями для инструмента на сайте производителя
6.	Документы известных неисправностей и возможности обходить эти неисправности (дать ссылку)
7.	Доказательство того, что инструмент выполняет в соответствии со своей спецификацией (указать возможные подходы к тестированию, чтобы доказать правильность инструмента)
8.	Анализ механизмов отказа и способов смягчения по мере необходимости

Оценка должна быть основана на разработке и обосновании критериев сравнения. Примерами критериев могут быть простота применения, обоснованность этапов, распространенность в практике оценки безопасности, инструментальная оценка.

По результатам выполнения двух заданий команда готовит презентацию и заполненный чек-лист по анализируемым ИС.

Варианты заданий приведены в таблице 1.2.

Таблица 1.2 - Варианты заданий для подготовки презентаций по ИС оценки надежности систем смарт грид

Вариант	Наименование метода риск анализа безопасности
Индивидуальные задания	
1	ReliaSoft’s Xfmea
2	Reliability Block Diagram Analysis Software
3	HAZOP Manager
4	RAMS
5	CAFTA
6	Netica
7	Cafta+Netica
Работа в команде	
1	Комбинации 1,2
2	Комбинации 1,3
3	Комбинации 1,4
4	Комбинации 1,5
5	Комбинации 1,6
6	Комбинации 1,8
7	Комбинации 1,9
8	Комбинации 2,7
9	Комбинации 3,7
10	Комбинации 4,7

Требования к содержанию аналитического отчета

Отчет должен содержать:

- титульный лист;
- цели и программу проведения исследований;
- описание этапов метода оценки надежности смарт грид;
- преимущества и недостатки метода;
- ограничения по применению ИС;
- обзор ИС, использующих данный метод для оценки надежности (заполненный чек лист);
- результаты анализа и выводы.

Контрольные вопросы

1. Что понимается под смарт грид?
2. Что понимается под термином «безопасность» смарт грид?
3. Что понимается под надежностью систем в смарт грид?
4. Назовите основные показатели надежности цифровых подстанций?
5. Перечислите основные ИС оценки надежности и безопасности систем в смарт грид?
6. Назовите основные преимущества и недостатки указанных ИС?
7. Приведите примеры технологий SMART grid.
8. Каковы основные практические требования к выбору методов анализа надежности смарт грид?

1.2 Практикум. Ознакомление с инструментальными средствами оценивания надежности смарт грид на примере ИС Cafta

Цель и задачи практикума:

Изучение особенностей применения ИС анализа надежности систем в смарт грид на примере Cafta.

Учебные задачи:

– изучение основных теоретических сведений метода анализа надежности систем, основанном на построении деревьев отказов;

– изучение инструментальных средств оценивания надежности.

– изучение возможностей и ограничений существующих ИС анализа надежности.

Практические задачи:

– получение навыков практического применения ИС Cafta при выполнении иллюстративного примера.

Подготовка к практикуму

При подготовке к практикуму необходимо:

– уяснить цели и задачи;

– изучить теоретический материал, приведенный в описании.

Теоретический материал

ИС Cafta поддерживает практическую реализацию метода анализа «дерева отказов» («Fault Tree Analysis» - FTA). Данный метод позволяет определить множество условий и факторов, способных привести к определенному нежелательному событию (так называемому головному событию).

«Дерево отказов» - логически организованная графическая конструкция, в которой демонстрируется взаимодействие элементов системы, отказ которых по отдельности или в сочетании

может способствовать появлению нежелательного события - отказа системы в целом.

Анализ дерева отказов эффективно используется в аэрокосмической отрасли, атомной энергетике, химической и перерабатывающих отраслях, в фармацевтической, нефтехимической и других, связанных с высокой степенью риска.

Структура «дерева отказа» включает одно головное событие (аварию, инцидент), которое соединяется с набором соответствующих нижестоящих событий (ошибок, отказов, неблагоприятных внешних воздействий), образующих причинные цепи (сценарии аварий).

Для связи между событиями в узлах «деревьев» используются знаки «И» и «ИЛИ». Логический знак «И» означает, что вышестоящее событие возникает при одновременном наступлении нижестоящих событий.

Знак «ИЛИ» означает, что вышестоящее событие может произойти вследствие возникновения одного из нижестоящих событий.

Символы событий приведены на рис.1.6.

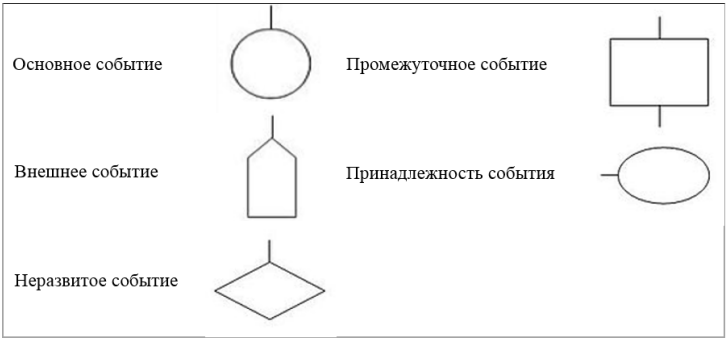


Рис. 1.6. Символы событий FTA

Символы элементов, используемых при построении деревьев отказов, приведены на рис. 1.7.

Символы элементов описывают отношения между входными и выходными событиями.

Символы событий следуют классической булевой логике:

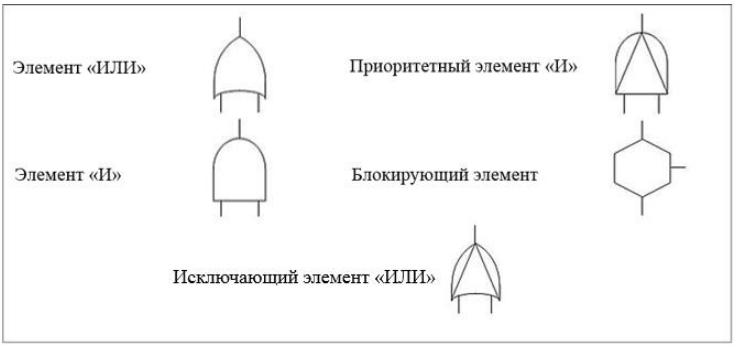


Рис. 1.7. Символы элементов

Символы элементов включают:

– элемент «ИЛИ» - выходное событие происходит, если есть любое входное событие;

– элемент «И» - выходное событие происходит только тогда, когда происходят все входные (входы независимы) события;

– исключающий элемент «ИЛИ» - выходное событие происходит, если происходит только одно входное событие;

– приоритетный элемент «И» - выход происходит, если входы происходят в определённой последовательности указанного события;

– блокирующий элемент – выход происходит, если вход происходит при благоприятных условиях для указанного события.

Элементы передачи приведены на рис. 1.8.

Элементы передачи используются для соединения входов и выходов, соответствующих деревьев отказов, таких как дерево отказов подсистемы в своей системе.

Рис. 1.8. Элементы передачи

Рассмотрим иллюстрированный пример построения дерева отказов (рис 1.9).

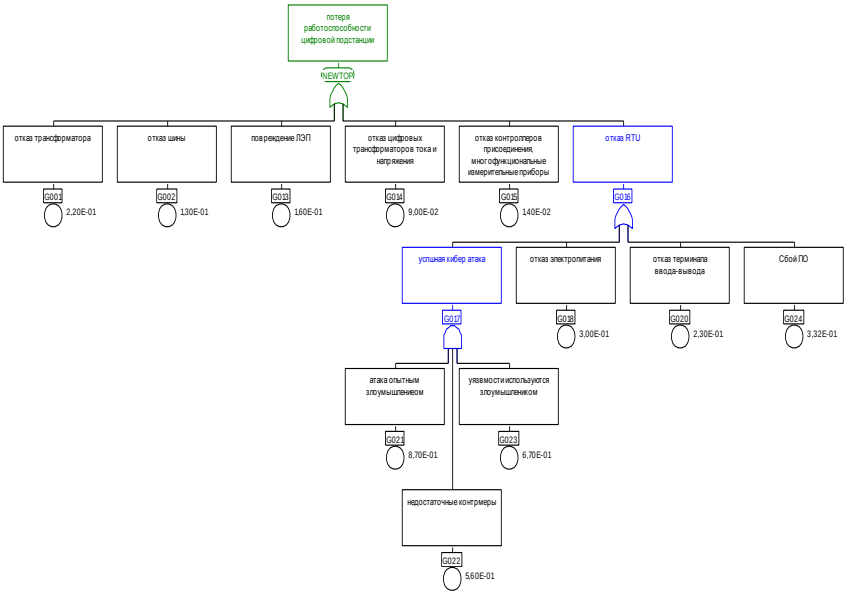


Рис. 1.9. Пример «дерева отказов»

Для построения и анализа дерева используем программное обеспечение CAFTA (Computer Aided Fault Tree Analysis) (рис.1.10).

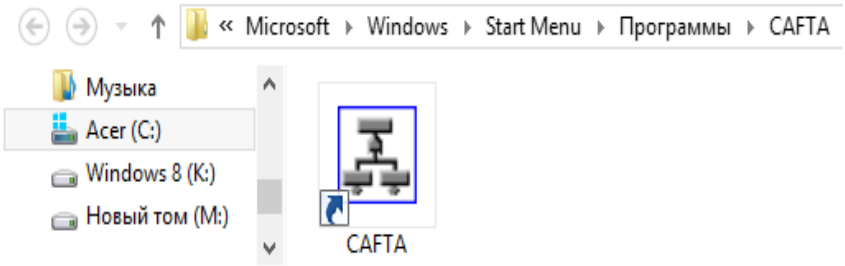


Рис. 1.10. Ярлык ПО CAFTA

При первом запуске программы, видим окно (рис.1.11):

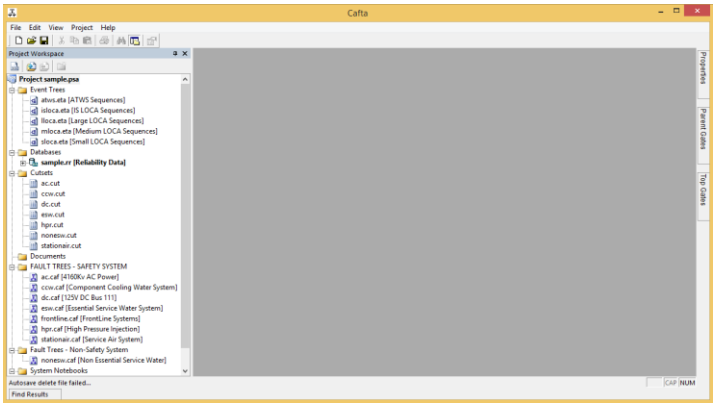


Рис. 1.11. Первый запуск программы

После нажатии комбинации CTRL+N необходимо выбрать стандартное дерево отказов (Standart Fault Tree) (рис.1.12):

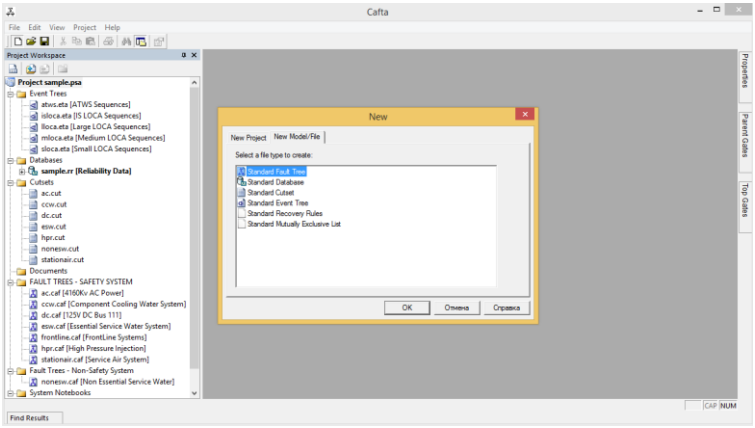


Рис. 1.12. Выбор типа файла проекта

Выбираем пункт «Создать новую базу данных (create New Database) (рис.1.13):

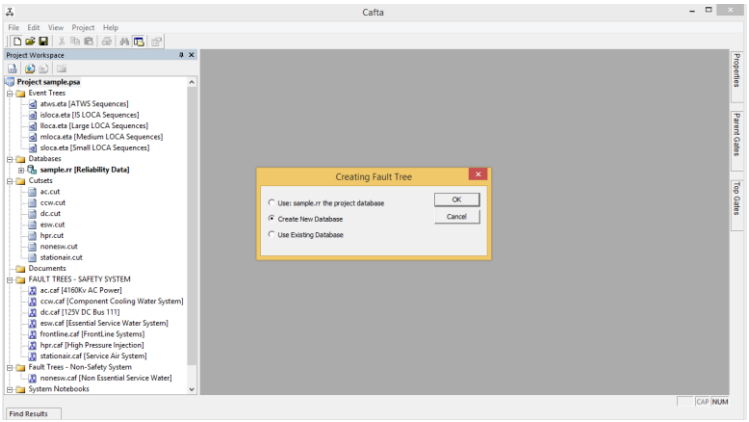


Рис. 1.13. Выбор «базы данных»

Выбираем «Стандартный шаблон» (Standard Database) (рис.1.14):

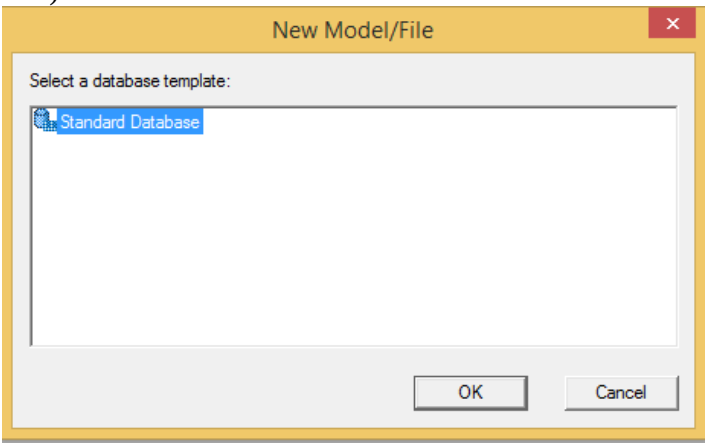


Рис. 1.14. Выбор шаблона

По умолчанию, программное обеспечение предложит сохранить «новый проект». Сохраняем будущее «дерево отказов» (рис.1.15):

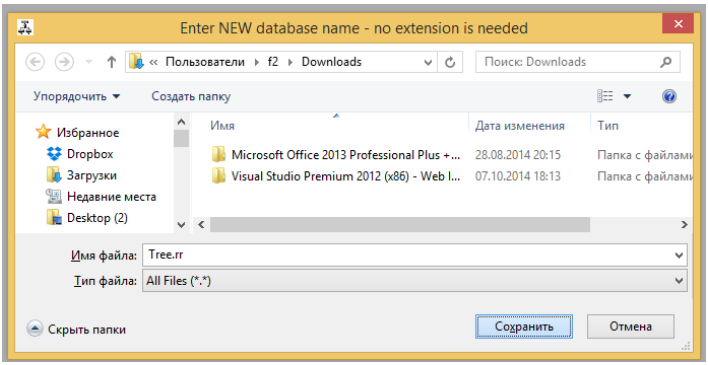


Рис. 1.15. Сохранение проекта

После сохранения, экран «нового» проекта выглядит таким образом (рис.1.16):

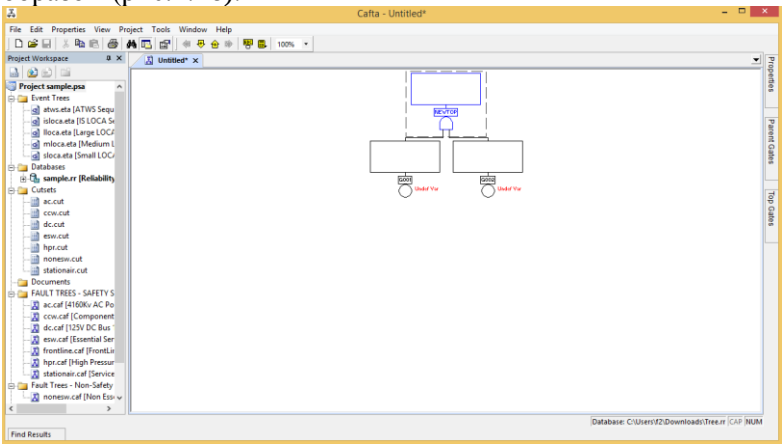


Рис. 1.16. Создание нового проекта

В верхней части находится панель управления. С помощью выделенных клавиш мы можем добавлять модули в «дерево отказов» (рис.1.17):

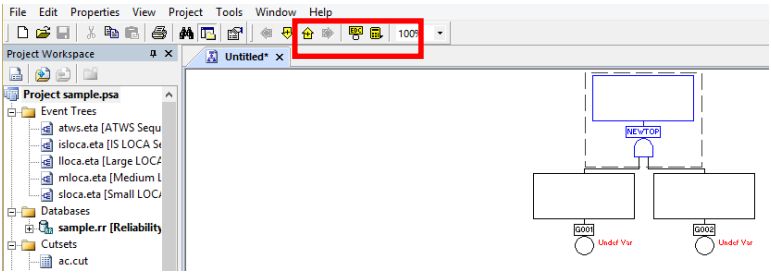


Рис. 1.17. Панель управления модулями

При нажатии и удержании на месте пересечения модулей ПКМ, может быть выбран символ элементов отношения между модулями (рис.1.18).

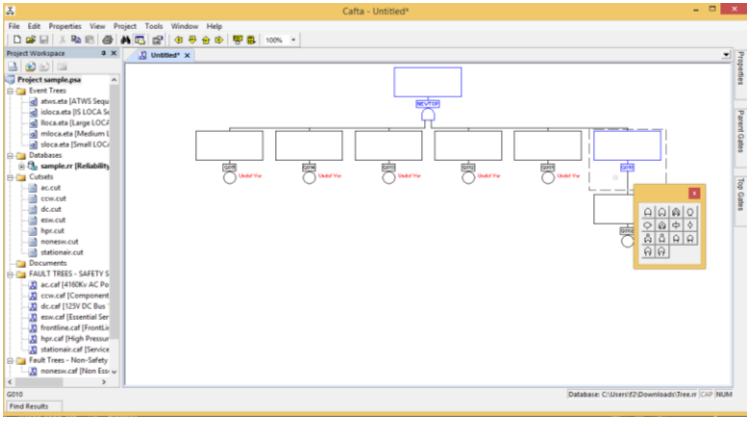


Рис. 1.18. Выбор символа элементов отношения модулей

Достраиваем «дерево отказов» согласно примеру (используем панель управления модулями) (рис.1.19):

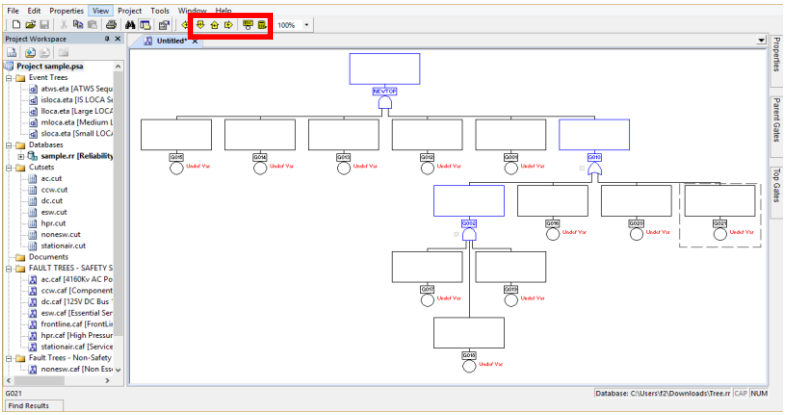


Рис. 1.19. Использование панели управления модулями при построении дерева отказов

При нажатой ПКМ, выбираем «свойство(Properties)» модуля (рис.1.20):

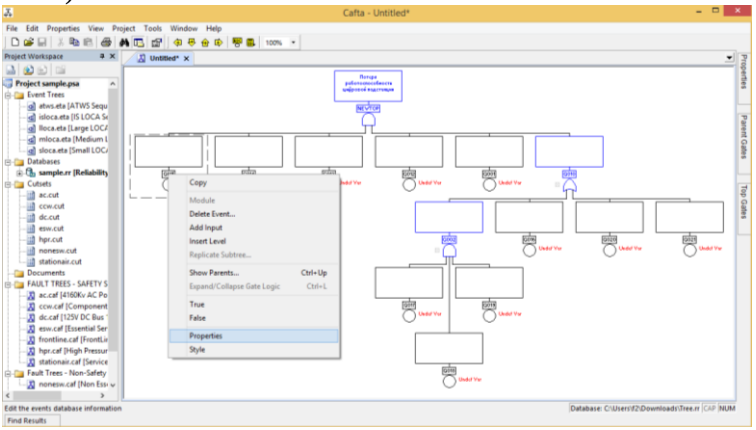


Рис. 1.20. Свойства модуля (Properties)

Для каждого модуля добавляем описание, согласно примеру, в поле «описание(Description) (рис.1.21):

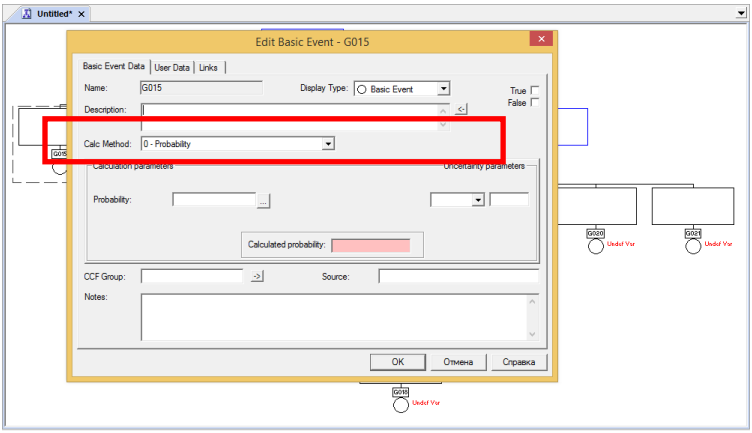


Рис. 1.21. Добавление описания модуля

Конечное «дерево» с описанием выглядит следующим образом (рис.1.22):

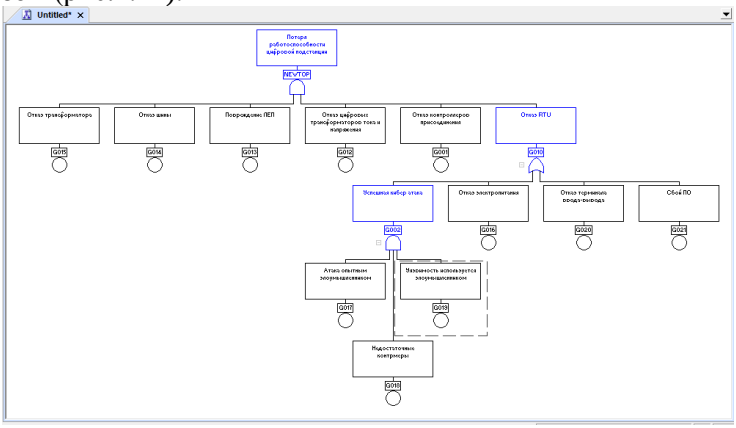


Рис. 1.22. Конечное «дерево» отказов

При нажатой ПКМ, выбираем «свойства (Properties) (рис.1.23):

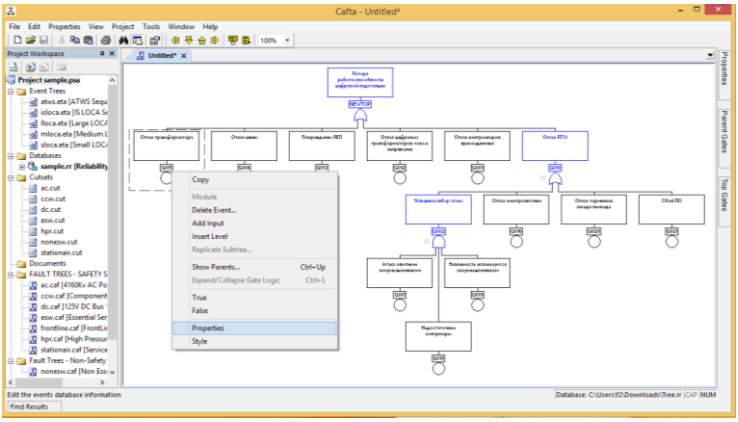


Рис. 1.23. Ввод значений вероятности появления отказов

В поле «Calculation parameters» вводим значение вероятности появления данного отказа (согласно примеру) (рис.1.24):

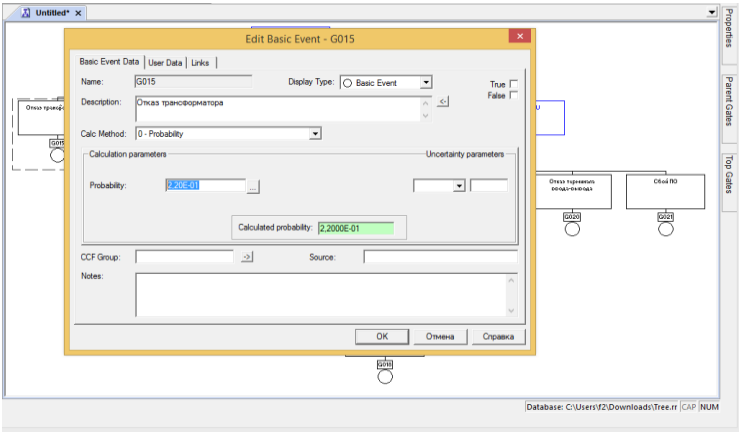


Рис. 1.24. Ввод значений вероятности появления отказов

Итоговое «Дерево отказов» выглядит следующим образом (рис.1.25):

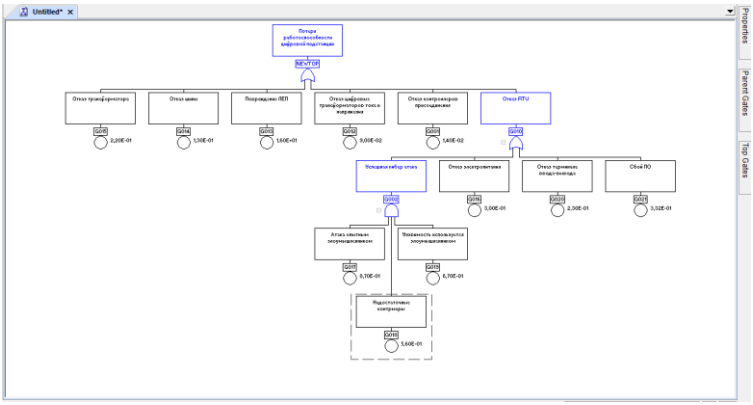


Рис. 1.25. Итоговое «дерево отказов»

В правой части окна находятся дополнительные вкладки. При нажатии ЛКМ на любой из модулей, и нажатии на вкладку «Свойства(Properties) можно увидеть информацию о данном модуле (с указанными изменениями и вероятностями появления) (рис.1.26).

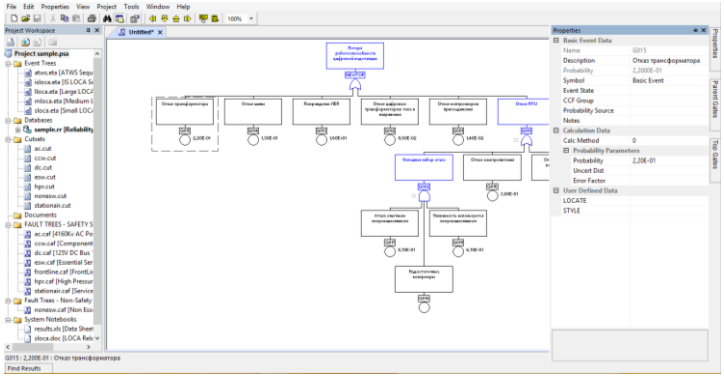


Рис. 1.26. Модуль Properties

На рис. 1.27 показаны отказы и их вероятности появления, используемые в рамках рассматриваемого примера:

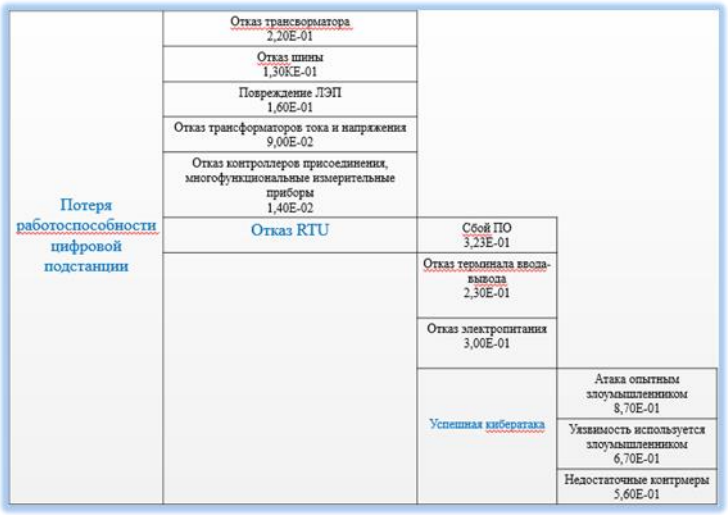


Рис. 1.27. Отказы и вероятности появления отказов

Проведем анализ и подсчет вероятности «головного» процесса. Для расчета «головного процесса необходимо нажать на знак калькулятора в верхней части панели управления (рис.1.28).

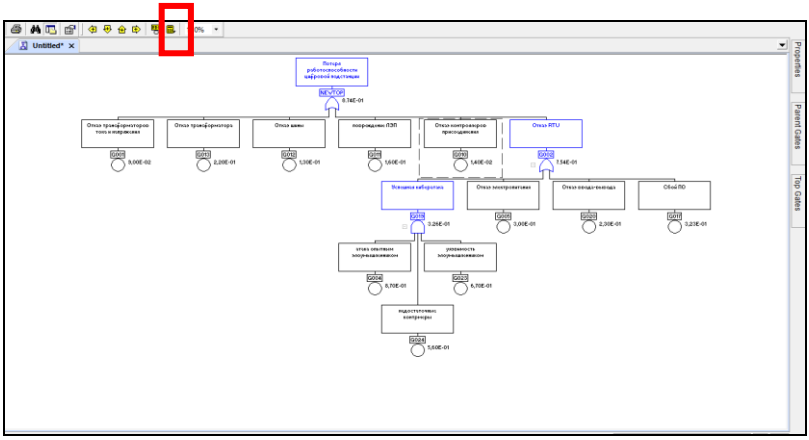


Рис. 1.28. Расчет вероятности «головного» процесса

После нажатия на клавишу калькулятора, мы видим данное окно (рис.1.29).

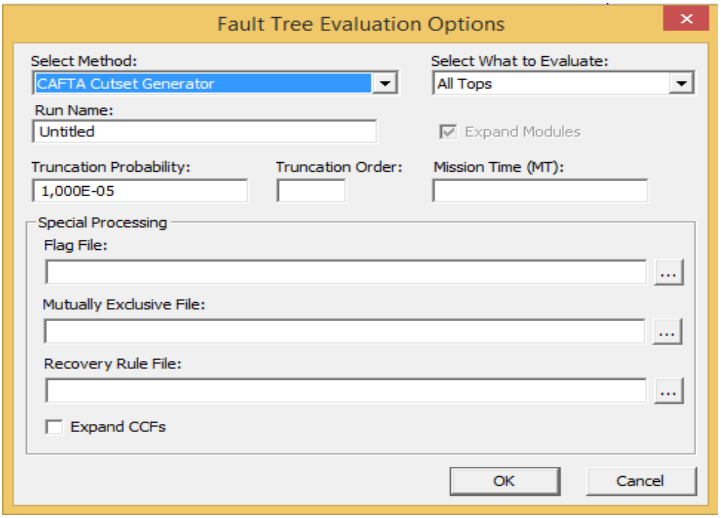


Рис. 1.29. Окно «калькулятор»

Далее, нажимаем “OK”. После чего, наблюдается следующее (Рис.1.30).

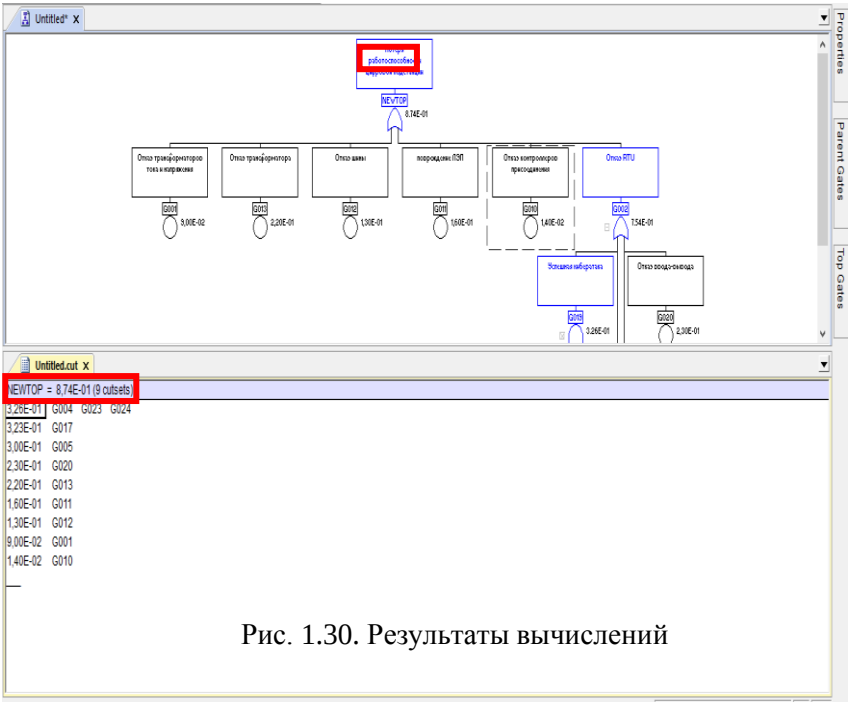


Рис. 1.30. Результаты вычислений

Итоговая вероятность «головного» процесса автоматически добавляется в модуль после подсчета.

Программа разработок

Практикум выполняется индивидуально.

Результатом работы является подготовка аналитического отчета (презентация по данному ПО + отчет).

Презентация должна включать:

1. Титульный лист.
2. Содержание презентации.
3. Краткое описание ИС.
4. Перечень ограничений при использовании ИС.
5. Область применения ИС.
6. Выводы.

Практикум завершается подтверждением практического освоения ИС каждым студентом (подготовка и защита презентации).

1.3 Описание лабораторных работ с использованием ИС Cafta

1.3.1 Лабораторная работа №1. Анализ надежности систем в смарт грид с использованием ИС Cafta

Цель работы: оценить основные параметры надежности систем в смарт грид с использованием современных ИС оценки надежности.

Учебные задачи:

– изучение возможностей ИС;
– построение дерева отказов согласно варианту;
– подсчет вероятности отказа системы.

Практические задачи:

– получение навыков практического анализа параметров систем смарт грид с использованием ИС Cafta.

Исследовательские задачи:

- исследование и подсчет вероятностей отказов систем;
- анализ параметров дерева отказов.

Задание

Оценка надежности систем в соответствии с вариантом (см. **ниже).**

Программа разработок

Практикум выполняется индивидуально. Результатом работы является подготовка аналитического отчета.

Отчет должен содержать:

1. Титульный лист.
2. Содержание презентации.
3. Краткое описание ИС Cafta.
4. Перечень ограничений при использовании ИС.

5. Область применения ИС.

6. Результаты расчета надежности согласно варианта.

Практикум завершается подтверждением практического освоения ИС каждым студентом.

Варианты заданий.

Вариант 1: Построить дерево отказов с заданными вероятностями для ситуации: перелив воды в дамбе через гребень плотины.

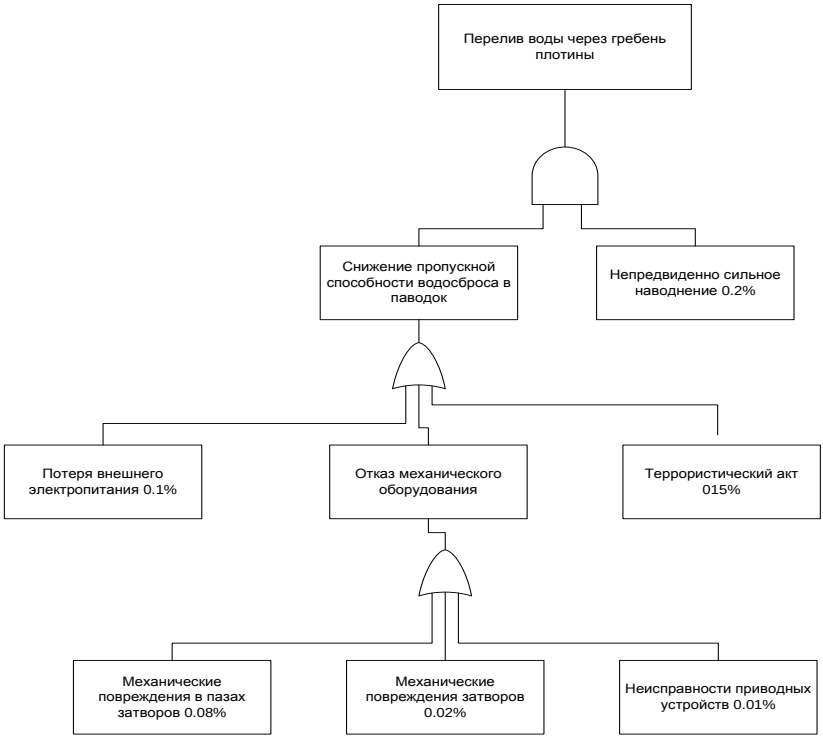


Рис. 1.31. Графическая иллюстрация варианта задания 1

Вариант 2: Построить дерево отказов с заданными вероятностями для ситуации: взрыв на заводе газа в баллоне.

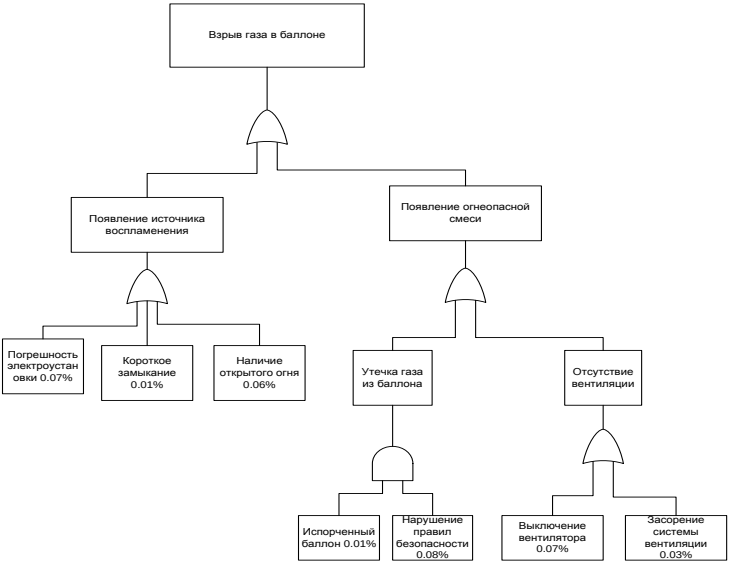


Рис. 1.32. Графическая иллюстрация варианта задания 2

Вариант 3: Построить дерево отказов с заданными вероятностями для ситуации: пожар в квартире.

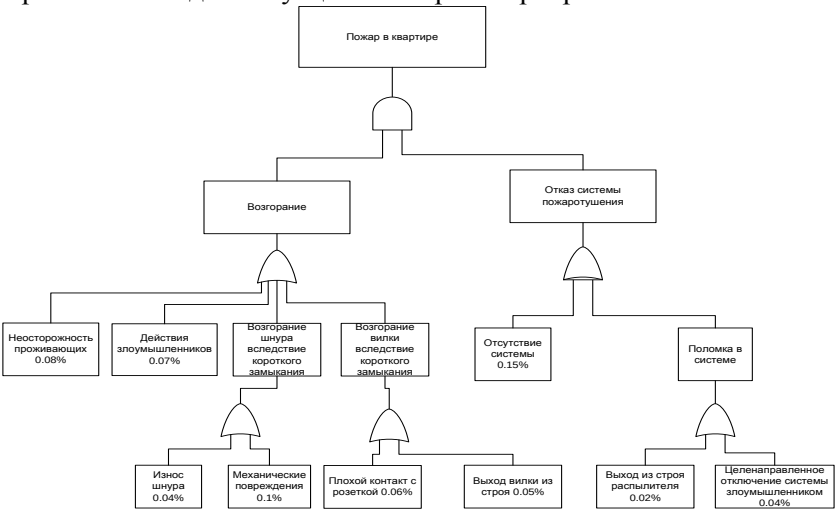


Рис. 1.33. Графическая иллюстрация варианта задания 3

Вариант 4: Построить дерево отказов с заданными вероятностями для ситуации: разрушение плотины.

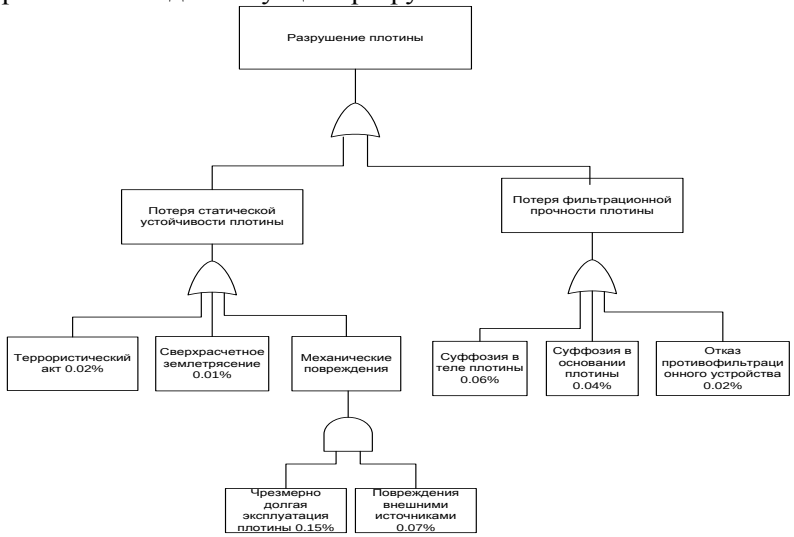


Рис. 1.34. Графическая иллюстрация варианта задания 4

Вариант 5: Построить дерево отказов с заданными вероятностями для ситуации: отказ работы подъемного крана.

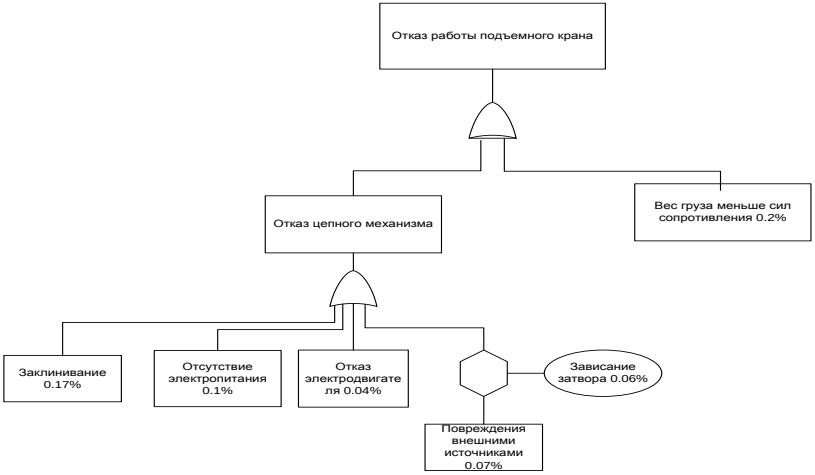


Рис. 1.35. Графическая иллюстрация варианта задания 5

Вариант 6: Построить дерево отказов с заданными вероятностями для ситуации: разгерметизация газопровода.

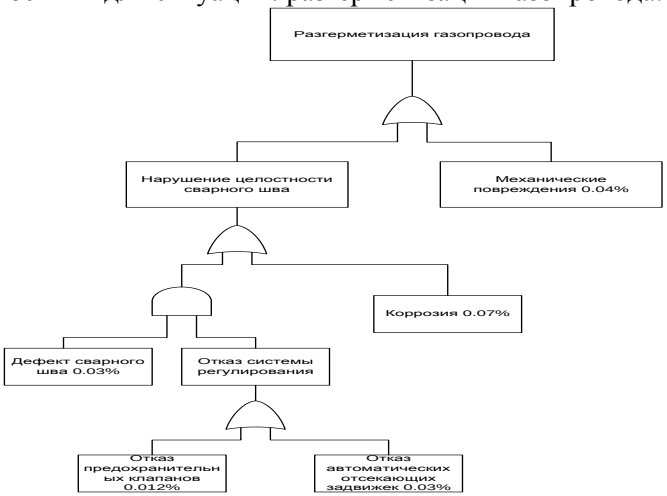


Рис. 1.36. Графическая иллюстрация варианта задания 6

Вариант 7: Построить дерево отказов с заданными вероятностями для ситуации: взрыв резервуара

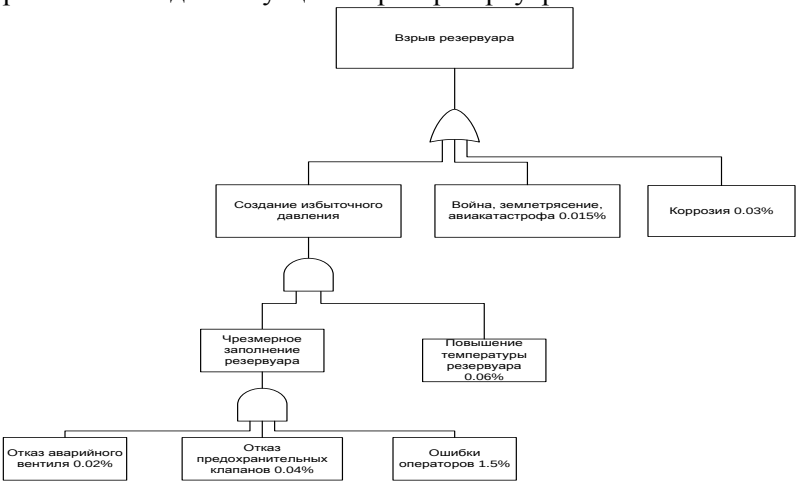


Рис. 1.37. Графическая иллюстрация варианта задания 7

Вариант 8: Построить дерево отказов с заданными вероятностями для ситуации: отказ работы двигателя самолета.

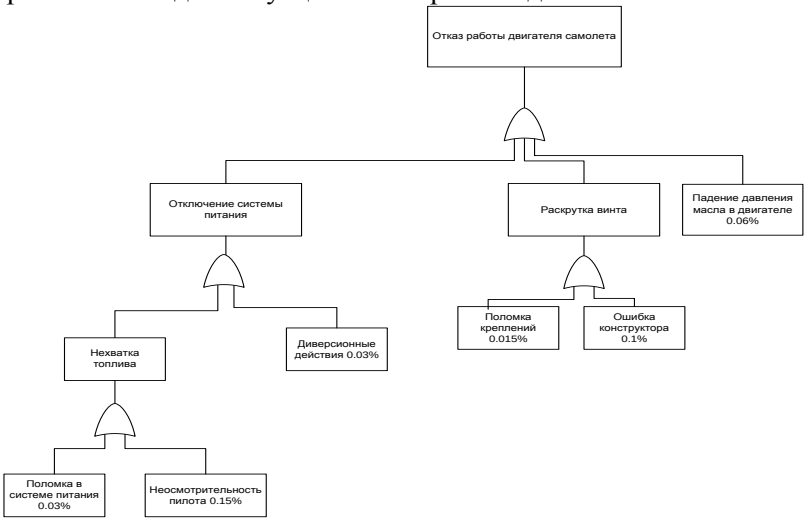


Рис. 1.38. Графическая иллюстрация варианта задания 8

Вариант 9: Построить дерево отказов с заданными вероятностями для ситуации: отказ работы кардиостимулятора.

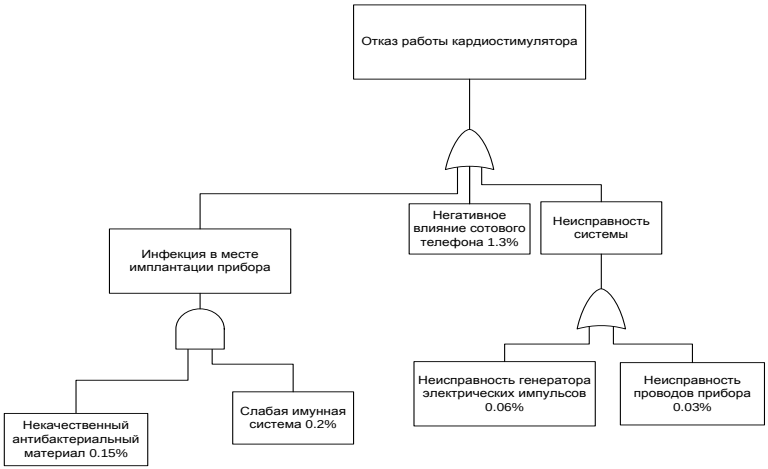


Рис. 1.39. Графическая иллюстрация варианта задания 9

Вариант 10: Построить дерево отказов с заданными вероятностями для ситуации: отказ работы двигателя автомобиля

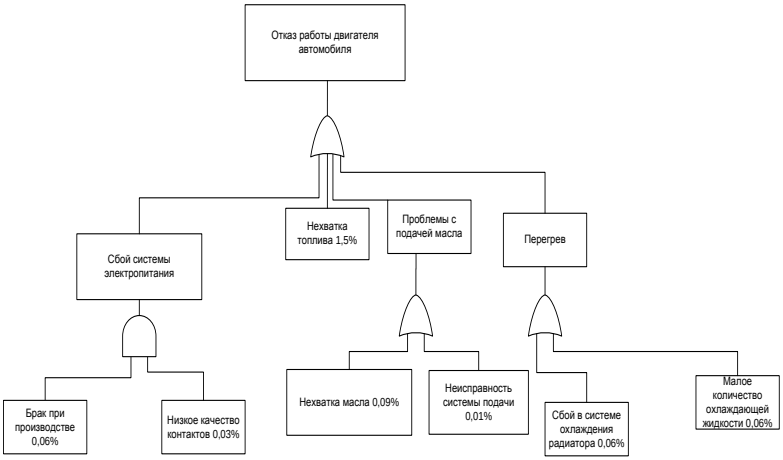


Рис. 1.40. Графическая иллюстрация варианта задания 10

1.3.2 Лабораторная работа №2. Интеграция методов оценивания надежности и безопасности (Cafta & Netica)

Цель работы: исследовать особенности интеграции метод оценивания надежности и безопасности смарт грид для решения задач оценивания безопасности с учетом параметров надежности систем в смарт грид

Учебные задачи:

– изучение основных теоретических сведений об цифровых подстанциях смарт грид;

– изучение возможностей рабочего пакет Netica и Cafta с учетом их интеграции при оценивании безопасности смарт грид с учетом надежности цифровой подстанции.

Практические задачи:

– получение навыков практического анализа параметров сетей с использованием средств имитационного моделирования.

Исследовательские задачи:

- исследование возможностей интеграции методов оценивания надежности и безопасности систем в смарт грид.

Задание

Необходимо исследовать возможность проведения интеграции методов оценивания надежности и безопасности на примере интеграции ИС Netica и Cafta.

Варианты заданий приведены в таблице 1.3.

Требования к оформлению отчета приведены на стр. 53.

Краткие теоретические сведения

Безопасная эксплуатация систем в смарт грид (например, объектов генерации электричества) выдвигает большие требования к качеству параметров электрической сети. Так, например, для нормальной работы всех систем безопасности реактора АЭС частота тока должна быть в пределах +3% и – 5%; напряжение в пределах +/ – 5%. Любые отклонения от этих параметров могут привести к остановке реактора АЭС. Так, например, в сентябре 2011 г., в Сан Диего, США, в результате отказа оборудования подстанции произошла аварийная остановка реактора АЭС в Сан Клименте, Калифорния.

Несмотря на повышение безотказности компонентой базы смарт грид, проблемы обеспечения ее надежности остаются актуальными.

Это обусловлено прежде всего: 1) растущими требованиями энергетического рынка, обуславливающими функционирование электросети на грани ее предельных возможностей по току, напряжению, частоте, пр.; 2) возрастающими потребностями в электричестве, стремлению стейкхолдеров энергокомпаний к получению максимальной прибыли; это приводит к принятию технически необоснованных решений, например, по передаче электричества на большие расстояния, что ведет к росту нагрузки на оборудование этих сетей, и как следствие, к его износу; 3) использованием современных ИТ для повышения возможностей контроля за состоянием сети; однако, с одной стороны, ИТ повышают возможности по контролю за состоянием и самоадаптации, а с другой, – увеличивают требования к надежности оборудования; 4) высокой динамикой системы, что приводит к необходимости принятия качественных решений в режиме реального времени; 5) высокой географической распределенностью активов энергосистемы; 6) интеграцией альтернативных источников в энергосистему, что вносит дополнительные риски в возможность поддержания ее стабильной работы и качества параметров сети, пр.

В настоящее время одной из проблем обеспечения инфраструктурной безопасности является адекватное моделирование инфраструктур, учет влияния надежности систем и

компонентов современной электрической сети на безопасность инфраструктуры. Для оценки безопасности смарт грид используются Марковские сети, сети Петри, Байесовские сети доверия (БСД).

Показатели надежности смарт грид и подстанции.

Под надежностью смарт грид понимается комплексное свойство, определяющее ее способность осуществлять электроснабжение потребителей путем выполнения функций по производству, передаче и распределению электрической энергии нормированного (требуемого) качества при едином технологическом взаимодействии генерирующих установок, электрических сетей и электроустановок потребителей, удовлетворять в любой момент времени спрос на мощность и электроэнергию (адекватность, балансовая составляющая системной надежности), противостоять возмущениям, вызванным отказами отдельных элементов энергосистемы (безопасность, оперативная составляющая системной надежности).

КЭИ состоит из генерирующих станций и электросистемы (см. рис. 1.41). Основной функцией электросистемы является передачи и распределение электроэнергии от генерирующих станций к потребителю.

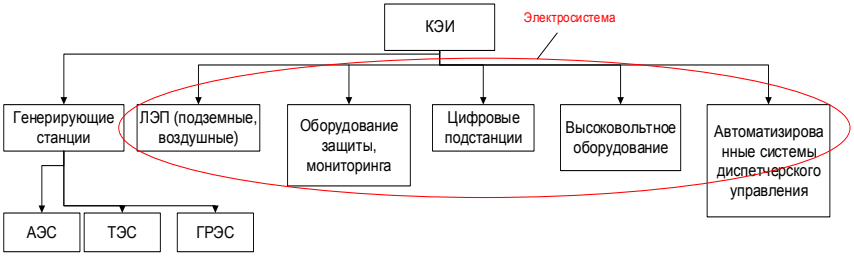


Рис. 1.41. Общая схема смарт грид

Основными компонентами электросистемы, надежность которых определяет безопасность АЭС, являются подвесные и подземные ЛЭП; цифровые подстанции; высоковольтное

оборудование; автоматы защиты, системы мониторинга; системы связи и управления, пр.

Все показатели надежности смарт грид можно представить в виде групп частных и интегральных показателей.

Существуют такие интегральные показатели как: суммарное время простоя оборудования, отключения энергопринимающих установок потребителей, недоотпуски электроэнергии, пр.

Цифровая подстанция является одним из важных активов электросистемы, обеспечивающим прием, преобразование и распределение электрической энергии. Фактически, она является интерфейсом между АЭС и электросистемой, расположенной в непосредственной близости к станции.

Цифровая подстанция содержит комплекс цифровых устройств (терминалов) для решения задач релейной защиты и автоматики и АСУ ТП - регистрации аварийных событий, учёта и контроля качества электроэнергии, телемеханики. Все оборудование станции общается между собой и центральным сервером объекта по последовательным каналам связи на единых протоколах.

Частные показатели используются для оценки надежности цифровой подстанции. Для подстанции выделяют следующие частные показатели надежности: вероятность отказа оборудования подстанции, среднее время наработки на отказ, интенсивность отказа, время восстановления, коэффициент оперативной готовности, пр.

В рамках данного подхода в качестве показателя надежности цифровой подстанции предлагается использовать коэффициент оперативной готовности. Под коэффициентом оперативной готовности понимается вероятность того, что цифровая подстанция окажется работоспособной (обеспечит электроснабжение для АЭС) в произвольный момент времени и с этого момента будет работать безотказно в течение заданного промежутка времени. Предполагается, что рассматривается установившийся процесс эксплуатации, математической моделью которого является стационарный случайный процесс

Оценка безопасности смарт грид систем с учетом параметров надежности подстанции.

Для оценки влияния показателей надежности цифровой подстанции на безопасность смарт грид предлагается использовать метод, основанный на комбинированном использовании БСД и метода анализа деревьев отказов (МАДО).

При построении БСД очень важно правильно задать априорные вероятности состояний узлов родителей. Для этого предлагается использовать метод анализа дерева отказов.

Метод анализа деревьев отказов интенсивно используется в различных отраслях, например, машиностроении, с целью выявления способов уменьшения рисков или определения частоты системного отказа.

Предлагаемый метод учета надежности цифровой подстанции при оценке безопасности смарт грид с использованием комбинации БСД и МАДО включает следующие этапы: определение и структуризация всех активов подстанции; риск анализ активов подстанции, с учетом тяжести отказов для подстанции смарт грид; ранжирование активов подстанции по рискам с учетом влияния на работоспособность цифровой подстанции. На этом этапе выявляются наиболее критичные активы, отказы которых приводят к потере готовности цифровой подстанции; построение БСД, включающей узел (узлы), учитывающий надежность цифровой подстанции в виде коэффициента готовности, а именно, вероятности нахождения подстанции в работоспособном состоянии;

- вероятности нахождения активов подстанции в работоспособном состоянии определяются с помощью МАДО.

Этапы метода приведены на рис. 1.42.

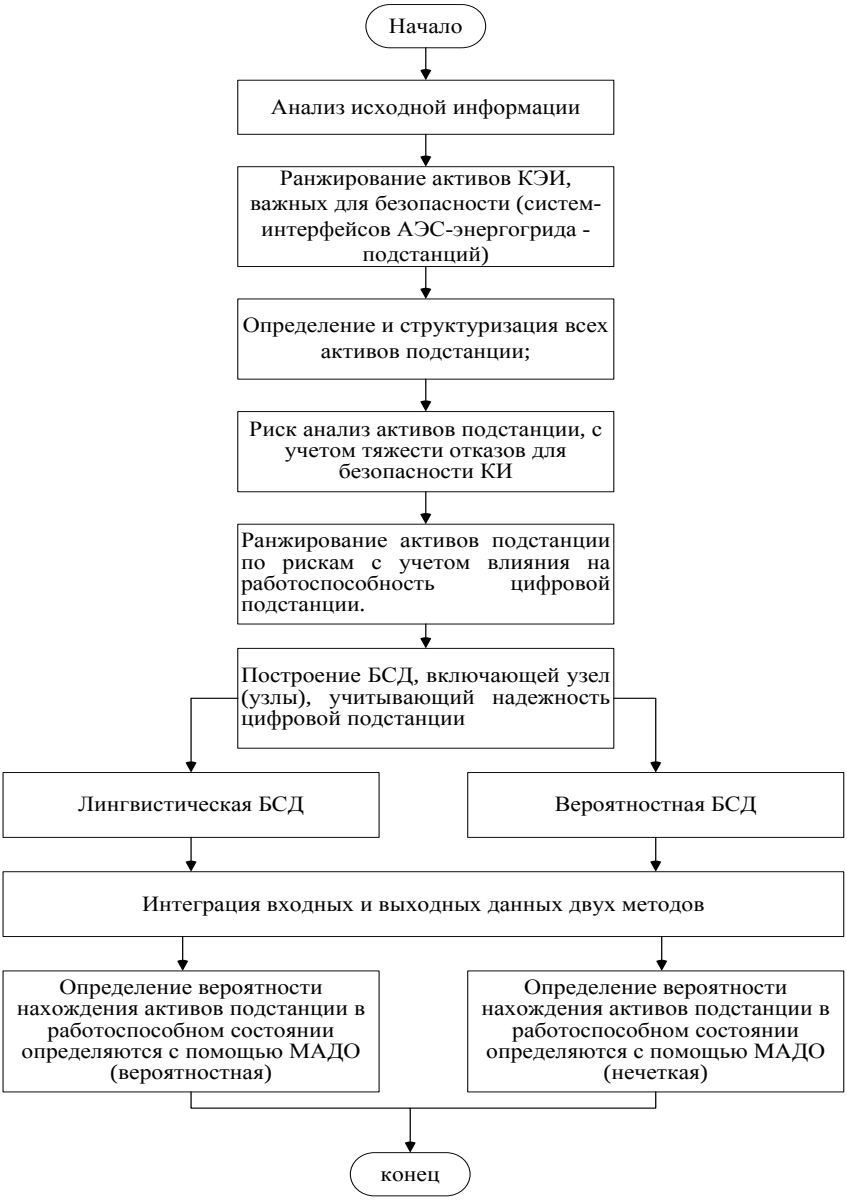


Рис. 1.42. Этапы метода оценивания безопасности смарт грид (ИУС) с учетом надежности ее подсистем (подсистем).

Пример оценки безопасности смарт грид системы с учетом параметров надежности.

В качестве примера применения метода рассмотрен фрагмент БСД для оценки безопасности реактора АЭС с учетом состояния источников внешнего и внутреннего энергоснабжения (рис. 1.43).

В качестве основных узлов рассматриваются: узел состояния реактора (reactor state unit), узлы учета состояния двух систем безопасности (RCIC, RPS), узлы учета состояния внешнего и внутреннего энергоснабжения (Off_site_power_state, On_site_power_state), узлы состояний трех цифровых подстанции (smart_substation_(1-3)), узлы для дизель-генератора (DG) и аккумуляторной батареи (DC_batteries). Данная БСД была построена с использованием инструментального средства Netica 512.

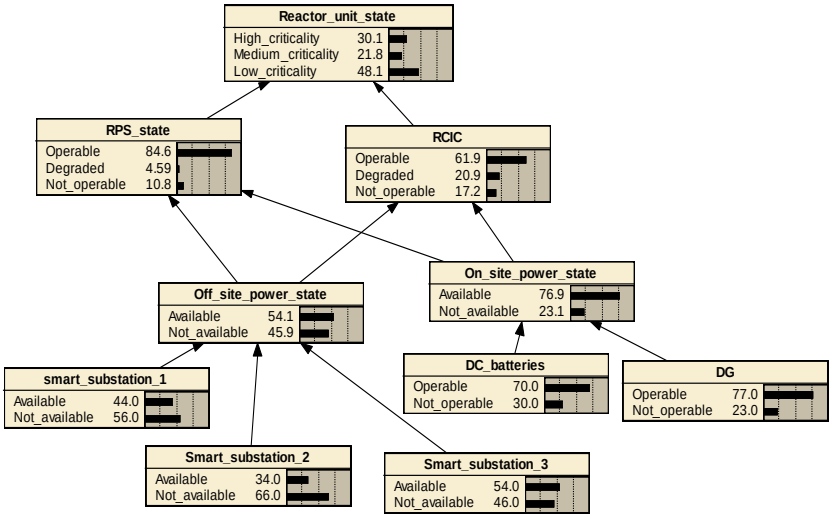


Рис. 1.43. Фрагмент БСД для оценки безопасности АЭС с учетом работоспособности цифровых подстанций и внутреннего энергоснабжения

К основным причинам потери нагрузки (работоспособности) цифровой подстанции можно отнести:

- отказы полевого оборудования, датчиков сбора дискретной информации и передачи команд управления на удаленные коммутационные устройства (remote terminal unit, RTU);

- отказы датчиков для сбора аналоговой информации (цифровые трансформаторы тока и напряжения).

- отказы устройств управления и мониторинга (контроллеры присоединения, многофункциональные измерительные приборы, счетчики, системы мониторинга трансформаторного оборудования и т.д.).

- выход из строя серверов верхнего уровня (сервер базы данных, сервер, сервер телемеханики, сервер сбора и передачи технологической информации и т.д., концентратор данных), пр.

В рамках примера, после ранжирования наиболее критичным активом определен RTU. RTU представляет собой удаленное оконечное устройство, которое выполняет важные функции в обеспечении работоспособности цифровой подстанции. Устройство подключено к окончанию канала связи с центральным устройством системы.

Его отказы могут приводить к потере нагрузки (работоспособности) цифровой подстанции. В свою очередь, это событие приводит к потере одной из линий, обеспечивающей снабжение всех систем безопасности АЭС.

В качестве основных причин потери работоспособности RTU, могут быть: отказы терминалов ввода/вывода, отказы ПО, электропитания.

Отказы RTU могут быть классифицированы первичные, вторичные. Причиной первичного отказа RTU являются непосредственно его компоненты и элементы, т.е. он сам. Вторичные отказы RTU обусловлены различного рода входными воздействиями (сигналами), лежащими вне диапазона, предусмотренного технической спецификацией на RTU. Эти внешние воздействия вызываются соседними элементами и окружающей средой, а также ошибочными действиями персонала подстанции. Вторичные отказы могут возникать вследствие успешных кибератак, проведенных опытным злоумышленником на уязвимости RTU.

Дерево отказов для события – потеря эксплуатационной готовности подстанции, построенное в рамках иллюстративного примера, приведено на рис. 1.33.

Коэффициент оперативной готовности подстанции определен на основе метода анализа деревьев отказов. Расчеты показателей надежности подстанции были проведены с использованием средства Cafta 6.0 a.

Построение БСД и ее интеграция с методом анализа деревьев отказов (см. раздел МАДО) на рис. 1.44

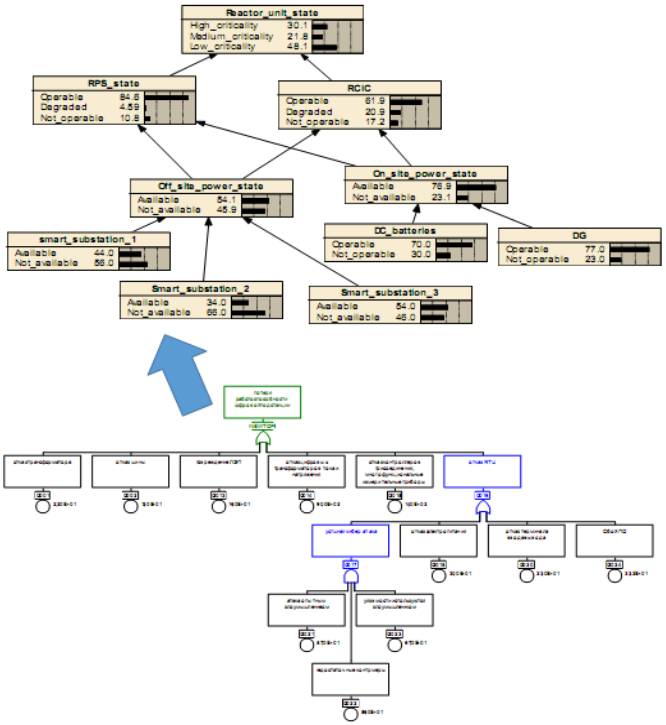


Рис. 1.44. Интеграция методов анализа деревьев отказов и БСД

Следует также отметить, что при совместном использовании БСД и МАДО могут возникнуть два случая:

- для оценки безопасности смарт грид используется комбинация лингвистической БСД и классического

(вероятностного) метода анализа дерева отказов. В лингвистической БСД все параметры сети, включая условные вероятности, представлены в виде лингвистических переменных;

- для оценки безопасности смарт грид используется комбинация классической (вероятностной) БСД и метода анализа дерева отказов, в которой вероятности базовых событий могут частично или полностью быть представлены в виде лингвистических переменных. Нечеткое расширение метода анализа деревьев отказов применяется в случае наличия недостаточной статистики отказов, позволяющей определить параметры надежности сложной системы.

Для обоих случаев возникает вопрос интеграции входных и выходных данных двух методов. В качестве решения могут быть предложены существующие методы фазификации и дефазификации. Причем, оба метода могут быть использованы в обоих случаях. Так, например, фазификация позволяет провести интеграцию вероятности в лингвистическую БСД. Теоретически возможно провести и дефазификацию лингвистической БСД. Однако эта задача может потребовать затрат ресурсов. Для второго случая можно использовать фазификацию классической БСД, что также является затратным процессом. Наиболее удобным подходом в этом случае является дефазификация выходных величин, полученных с использованием нечеткого метода анализа деревьев отказов.

Появление смарт грид приводит к появлению новых рисков для безопасности смарт грид и АЭС, в частности, рисков информационной безопасности и сложных отказов ее компонент. Подход к учету влияния надежности цифровых подстанций на безопасность КЭИ может быть основан на комбинированном применении БСД и МАДО. МАДО используется для получения показателей надежности подстанции с учетом вероятностей отказов наиболее критичных активов. Возможны два случая интеграции методов, для которых предложены варианты реализации.

Интеграция методов позволит получить обоснованные оценки вероятностей состояний цифровых подстанций, которые в дальнейшем интегрируются в БСД для получения оценок

безопасности реактора АЭС. Варианты заданий приведены в таблице 1.3.

Таблица 1.3. Варианты заданий

№	Авария	Примечание
1.	Чернобыльская АЭС	Построить БСД оценки безопасности реактора с учетом надежности систем безопасности
2.	Three Mile Island accident	Построить БСД оценки безопасности реактора с учетом надежности человека-оператора
3.	Фукусима-1 АЭС	Построить БСД оценки безопасности реактора с учетом надежности человека-оператора
4.	"Фобос-Грунт"	Построить БСД оценки безопасности КА с учетом надежности ПО
5.	шаттл Колумбия	Построить БСД оценки безопасности КА с учетом надёжности наружного теплозащитного слоя
6.	Авария Аполлона-13	Построить БСД оценки безопасности КА с учетом надёжности систем связи
8.	"Союз-11"	Построить БСД оценки безопасности КА с учетом надёжности систем герметизации
9.	авария airbus 320	Построить БСД оценки безопасности самолета с учетом надежности автопилота
10.	СШ ГЭС	Построить БСД оценки безопасности ГРЭС с учетом надежности гидроагрегатов

Требования к отчету при выполнении лабораторных работ

Отчёт формируется в следующем порядке:

1. Титульный лист.

2. Цель работы. Цель работы показывает, для чего выполняется работа, например, для получения или закрепления каких навыков, изучения каких явлений, законов и т.п.

4. Краткое содержание работы. Краткое содержание работы включает теоретическое описание тематики лабораторной работы, описание моделей, методов и алгоритмов, необходимых для обработки полученных данных, описание ПО, используемое, используемого в работе.

5. Обработка результатов. Обработка результатов включает описание хода выполнения работы, перечень полученных результатов, сопровождающихся необходимыми комментариями, расчетами и промежуточными выводами, графики.

6. Выводы по результатам выполнения работы. Выводы по работе делаются на основании обобщения полученных результатов. В выводах также отмечаются все недоработки, по какой-либо причине имеющие место, предложения и рекомендации по дальнейшему исследованию поставленной в работе задачи.

7. Приложения. В приложения выносятся библиографический список, содержащий ссылки на книги, периодические издания, интернет ресурсы, использованные при выполнении работы и оформлении отчёта. В приложение выносятся также справочная и прочая информация, не включённая в основные разделы отчёта.

2 НЕЧЕТКИЕ МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА АНАЛИЗА ДЕГРАДАЦИИ В СИСТЕМАХ СМАРТ ГРИД

2.1 Практикум 1. Анализ методов оценивания деградации систем в смарт грид

Форма занятия: практикум

Цель и задачи практикума является анализ показателей деградации систем в смарт с использованием нечеткой логики.

Учебные задачи:

– изучение основных положений анализа деградации ИУС с использованием нечеткой логики;

– изучение пакета Fuzzy Logic Toolbox.

Практические задачи:

– получение навыков применения пакета нечеткой логики Fuzzy Ligic Toolbox при решении задачи оценивания деградации ИУС в смарт грид.

Исследовательские задачи:

- провести оценку деградации ИУС в смарт грид.

Подготовка к практикуму

При подготовке к практикуму необходимо:

– уяснить цели и задачи;

– изучить теоретический материал, приведенный в описании, а также в [13-19].

Теоретический материал

Деградации ИУС в смарт грид приводит к изменению параметров функционирования и параметров качества выполнения функций. Эмерджентные риски для АЭС Фукушимы, связанные с потерей внешнего электроснабжения (негативное географическое

влияние природной системы), были частично компенсированы дизель генераторами станции (системы смарт грид - АЭС). Далее, они были переданы на уровень подсистем ИУС, где были компенсированы работой батареи. После разряда батарей – началась деградации информационно-управляющих функций (ИУФ) ИУС, т.е. ИУС деградирует при реализации эмерджентных рисков в смарт грид.

ИУС характеризуется критичностью решаемых задач, информационной распределенностью, сложностью аппаратной и архитектурной реализации, временными ограничениями цикла управления и т.д. Технические средства также могут иметь внутреннюю структуру, состоящую из нескольких элементов, отказы которых влияют на ее работоспособность.

Математическим методам оценки систем с деградацией или деградирующих систем (ДС) посвящено большое число работ. В англоязычной литературе эти системы получили название "multi-state systems" (MSS). Использование этого термина не является вполне корректным, поскольку существует множество приложений, не относящихся к проблеме надежности и живучести, где он может применяться.

Развитие теории ДС (MSS) базируется на применении специальных структурных функций, Марковских моделей и комбинированных методов. Ряд результатов в этой области получено применительно к деградирующим многоярусным мажоритарным резервированным системам, а также для систем с многоступенчатой деградацией и восстановлением, в которых использовался аппарат Марковских процессов совместно с диаграммами многоступенчатой деградации (QD-диаграммами). Системы, исследуемые в указанных публикациях, имеют одно общее ограничение: деградация рассматривается, как правило, только на системном уровне. Другими словами, в них работает (одноуровневая) схема: отказ элемента (участка резервирования) – деградация системы. Современные критические ИУС являются сложными иерархическими системами, поведение которой не может быть описано подходами одноуровневой деградации. Для сложных динамических эргатических систем целесообразно, на наш взгляд, говорить о многоуровневой деградации.

Процесс формализации и разработки моделей многоуровневой деградации является сложной задачей. Основная проблема в исходных данных, которые, особенно на ранних стадиях проектирования подобных систем, характеризуются неточностью, неясностью и размытостью. Эти неточные данные не могут быть использованы для традиционных моделей.

Понятие деградации и уровней деградации ИУС является сложным и слабо формализуемым. Границы перехода из одного состояния в другое являются размытыми и нечеткими. Изменение состояния компонентов и ИУС в целом происходит скорее плавно, чем скачкообразно. Высокая неопределенность при решении задач оценки уровней деградации критической ИУС обуславливает необходимость использования большого спектра разнородной информации. В результате, оценка уровней деградации с учетом какого-то одного параметра, характеризующего процесс функционирования, становится сложной. Разнородность физической природы параметров не позволяет в полной мере использовать аналитические соотношения.

Сложной и неопределенной является формализация зависимости между изменением уровня деградации компонентов, элементов и систем ИУС в целом.

Кроме того, большая часть информации, которая могла быть использована для анализа состояний ИУС является качественной, доступной только в виде знаний экспертов.

Поэтому возникает целесообразность разработки новых методов оценки уровней деградации критической ИУС с использованием аппарата теории нечетких множеств, который позволяет использовать качественную информацию для анализа многоуровневой деградации ИУС как результата реализации эмерджентных рисков в смарт грид.

Деградирующая ИУС, представленная множеством $E=\{E_j\}$, $j=\overline{1,m}$, это система, в которой отказ одного или нескольких компонент (или элементов) E_j, приводит к ухудшению качества (и/или количества) информационно-управляющих функций, характеризуемых скалярным или векторным показателем $П$. Каждый компонент, элемент и система критической ИУС может выполнять несколько функций. Каждая функция оценивается

своим индивидуальным показателем. В общем случае этот показатель является комплексным и в ряде практических задач не всегда может быть преобразован в скалярную форму.

Снижение показателя $П$ от некоторой исходной $П_0$ до минимально допустимого $П_{\min}$ означает переход ИУС в новое состояние. Определение границ перехода является условным и субъективным. Поскольку переход из одного состояния в другое является условным и в большей степени является требованием математической модели, используемой при анализе, целесообразно говорить о размытом состоянии и размытых границах перехода. Это предположение является более гибким при анализе подобных систем.

Можно говорить о множестве нечетких состояний всех уровней иерархии критической ИУС. Изменение показателей функционирования компонентов ИУС приводит к изменению состояния ее элементов, которые в свою очередь приводит к изменению состояния ИУС в целом.

Формально любая критическая ИУС может быть представлена в виде взаимосвязанного множества узлов (node). Узлы каждого уровня иерархии взаимосвязаны между собой множеством связей. Каждый узел в свою очередь является сложной системой, включающей множество узлов следующего уровня и связей между ними.

Формально компонент критической ИУС может быть представлен как:

$$S = [\{m\}, \{n\}, \{r\}],$$

где m – элемент компонента критической ИУС; n – свойства элемента, описывающие его состояние; r – взаимовлияние между элементами.

Каждый компонент ИУС может находиться в одном из множеств состояний критичности, обусловленных отказами его элементов. Такие состояния могут быть представлены в виде выражений естественного языка, например, *High, Medium, Low* уровнями критичности. *High* уровень критичности характеризуется низким качеством выполнения функций

безопасности, и, соответственно, *Low*, высоким качеством или отсутствием деградации.

Траекторией деградации t_{rd} называют кортеж, объединяющий кортежи *СТ* и *СП* $t_{rd} = CT \cup CП = \langle (t_0, П_0), (t_1, П_1), ..., (t_{d-1}, П_{d-1}), (t_d, 0) \rangle$, где $CT = \langle t_0, t_1, \ldots, t_d \rangle$ - кортеж времен и соответствующих им кортеж значений $CП = \langle П_0, П_1, \ldots, П_{d-1}, 0 \rangle$.

При одном и том же значении d возможны разные траектории деградации пары кортежей *СТ* и *СП*. В общем случае траектории деградации одной системы могут отличаться и мощностью кортежей *СТ* и *СП*. Это зависит от очередности отказов элементов и влияния этих отказов на степень снижения показателя *П*. Таким образом, система с многоступенчатой деградацией характеризуется множеством траекторий деградации $Mt_{rd} = \{t_{rdi}\}$, $i = \overline{1,n}$.

На начальных этапах разработки системы значения показателя значения показателя, характеризующее выполнения функций критической ИУС, не может быть определено в виде точечной оценки. Для каждого показателя может быть введена верхняя и нижняя оценка. Таким образом, каждому моменту времени может быть поставлена в соответствие интервальная оценка показателя, характеризующая выполнение некоторой функции.

Изменения в показателях функционирования одного уровня иерархии ИУС обуславливают изменения состояния элементов, которые в свою очередь приводят к изменению состояния всей системы.

Формализация зависимости между изменением состояния компонента и его влиянием на состояние компонента более высокого уровня является сложной задачей. Она может проведена с использованием базы правил или на основе графических моделей, например, байесовских сетей доверия.

Пример траектории деградации ИУС показан на рис. 2.1. В каждый момент времени *t*, ИУС описывается различными нечеткими уровнями деградации (degradation Level, DL), характеризуемые качеством выполнения функций безопасности (SFP) ИУС (I&C).

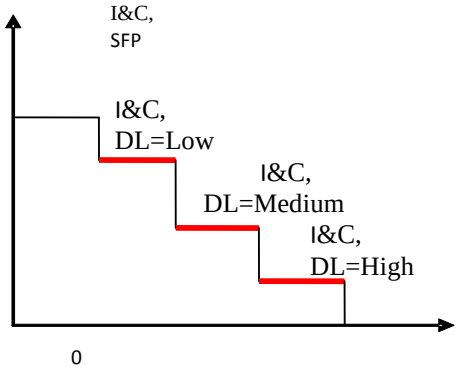


Рис. 2.1. Пример траектории деградации ИУС

В свою очередь то или иное состояние деградации системы соответствует определенной критичности ее состояния. Изменение критичности состояния с учетом изменения параметров, описывающих качество выполнения ИУФ рассматривается как деградация. Изменение показателей функционирования может быть связано с приближением системы к пределам безопасности. Пример соответствия уровней деградации и критичности системы приведен на рисунке 2.2.

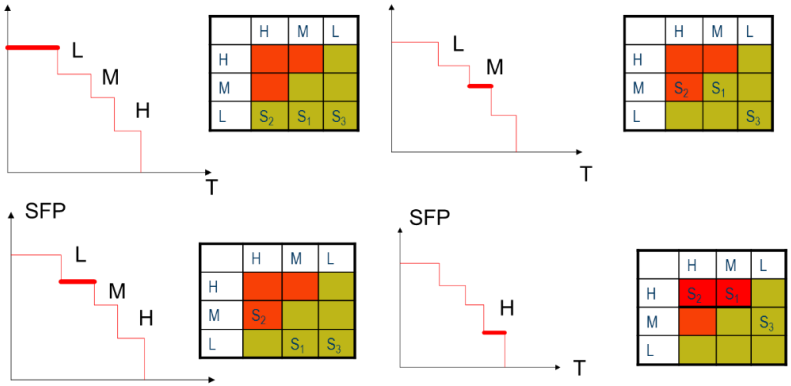


Рис. 2.2. Пример соответствия уровней деградации и критичности системы

Взаимовлияние между элементами, компонентами и подсистемами ИУС обуславливает соответствующую зависимость между их траекториями деградации. Иерархическое представление траекторий деградации систем (ИУС) в смарт грид приведено на рис. 2.3.

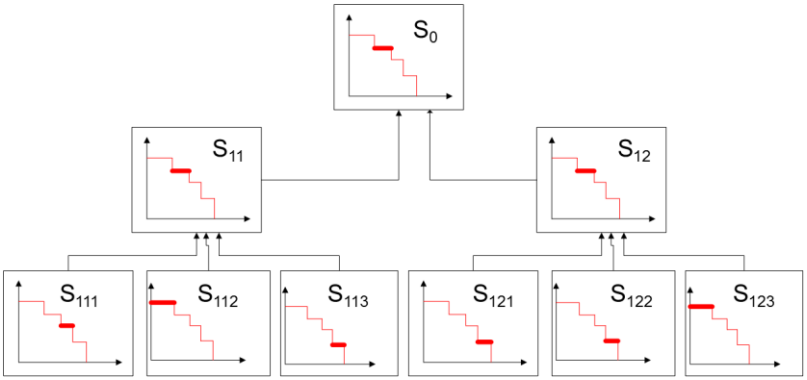


Рис. 2.3. Иерархическое представление траекторий деградации систем (ИУС) в смарт грид

Программа разработок и исследований

Работа выполняется индивидуально. Индивидуальная работа предусматривает подготовку каждым студентом презентации по определенному методу оценивания деградации, в соответствии с вариантом. Результатом работы является подготовка аналитического отчета.

Аналитический отчет представляется в виде презентации, которая должна содержать:

1. Титульный слайд
2. Описание этапов метода.
3. Основные недостатки и преимущества метода.
4. Описание области применения.
5. Анализ ИС, поддерживающих практическое использование метода.
6. Выводы.

Представление презентации проводится публично.

Таблица 2.1 - Варианты заданий для аналитического отчета

Вариант	Наименование метода оценивания деградации
1	Диаграммы деградации
2	HAZOP
3	FTA
4	ETA
5	Марковские цепи
6	FMECA
7	БСД
8	Нечеткие продукционные системы
9	сети Петри
10	Логико-вероятностные методы Рябинина

2.2 Практикум 2. Анализ деградации систем смарт грид с использованием нечетких методов

Форма занятия: практикум

Цель и задачи практикума является анализ безопасности систем смарт грид систем с использованием нечеткой логики.

Учебные задачи:

– изучение основных положений анализа деградации с использованием нечеткой логики;

– изучение пакета Fuzzy Logic Toolbox.

Практические задачи:

– получение навыков применения пакета нечеткой логики Fuzzy Ligic Toolbox для оценки деградации систем смарт грид.

Исследовательские задачи:

- провести анализ зависимости параметров выполнения ИУФ ИУС и уровней деградации систем смарт грид.

Подготовка к практикуму

При подготовке к практикуму необходимо:

–уяснить цели и задачи;

– изучить теоретический материал, приведенный в описании (см. ниже).

Краткие теоретические сведения

Задача определения оценки многоуровневой деградации смарт грид (ИУС) может быть представлена в виде задачи поиска отображения вида:

$$X^* = (Crt(S_1), QF_{S_1}; Crt(S_2), QF_{S_2}; Crt(S_3), QF_{S_3} ...., Crt(S_n), QF_{S_n}) \rightarrow$$
$$d_j \in D = (d_1, d_2, ..., d_m),$$

где $Crt(S_n)$ - критичность состояния системы S_N, $n = \overline{1,N}$, представленная в виде ЛП с термами (Высокий, Средний, Низкий); D – множество d_j, $j = \overline{1,m}$, уровней деградации, соответствующих критичности состояния; QF_{S_n} - уровень выполнения ИУФ.

Основными этапами (см. рис.2.4) метода оценивания многоуровневой деградации смарт грид (ИУС) являются:

1. Анализ спецификации системы.
2. Анализ основных параметров систем важных для безопасности. Выделение параметров состояния подсистем и параметров, описывающих качество выполнения ИУФ (информационно-управляющих функций).
3. Анализ основных видов взаимовлияния между подсистемами (показаны на схеме красным цветом).
4. Построение ЛЛМ безопасности для каждой подсистемы.
5. Построение ЛЛМ оценки качества выполнения функций Оценка качества проводится с учетом параметров, характеризующих выполнение ИУФ. К ним относят параметры, характеризующие получение, обработку и передачу информации между подсистемами.
6. Оценка критичности каждой подсистемы с учетом взаимовлияний между системами и качеством функций.
7. Построение ЛЛМ оценки деградации системы с учетом критичностей состояния подсистем. Оценка уровня деградации системы. Визуализация уровней деградации подсистем.
8. Определение мер повышения качества функционирования подсистем.
9. Реализация мер повышения качества подсистем.
10. Оценка текущего значения уровня деградации с требуемым. Выполнение дополнительных мер в случае несоответствия.

Рис. 2.4. Основные этапы метода оценивания многоуровневой деградации смарт грид систем (ИУС)

Описание метода оценивания многоуровневой деградации ИУС.

Первым этапом оценивания деградации ИУС является построение нечеткой модели состояний ее подсистем. Эта оценка определяется показателями, характеризующими близость подсистем к предельному состоянию. Сложность задачи определяется нелинейностью связей между входными параметрами (показателями), $x_1 \div x_n$, которые описывают функционирование подсистемы (включая качество информационно-управляющих функций, ИУФ) и выходными параметрами, описывающими уровни критичности ее состояния.

Особенностями решения данной задачи является:

- представление параметров функционирования подсистем (параметров качества ИУФ) и оценок уровней критичности в виде лингвистических переменных;
- представление в виде совокупности нечетких логических правил типа ЕСЛИ ...ТО…ИНАЧЕ причинно-следственных связей между критичностью всех подсистем и уровнем деградации ИУС.

Таблица 2.2. Нечеткая база правил многоуровневой деградации ИУС (фрагмент)

D (S_{11})	D (S_{12})	……	D (S_{1n})	Уровень деградации ИУС (S_1)
High (H)	High (H)	Medium (M)	Medium (M)	High (H)
High (H)	Medium (M)	Low (L)	Low (L)	High (H)
….	…….	……	……	…….
Low (H)	High (H)	Low (L)	Low (L)	Medium (M)

Входными данными для построения базы знаний являются:

- экспертные знания;
- исторические данные;

- общие инженерные знания.

Приведенные логические уравнения позволяют вычислить значения функций принадлежности оценок деградации при фиксированных значениях частных показателей, характеризующих критичность состояния подсистем и качества выполнения ИУФ.

Пусть $\mu^{a_{ij}^{jp}}(x_i)$ - функция принадлежности параметра $x_i \in [\underline{x_i}, \overline{x_i}]$ лингвистическому терму a_i^{jp}, $i = \overline{1,n}$, $j = \overline{1,m}$, $p = \overline{1,k_j}$; $\mu^{d_j}(x_1, x_2, ..., x_n)$ - функция принадлежности вектора входных переменных $X = (x_1, x_2, ..., x_n)$, который зависит от n переменных, значению выходной переменной y=dj.

Нечеткие логические уравнения вместе с функциями принадлежности нечетких термов позволяют оценивать уровни деградации компонент ИУС по следующему алгоритму:

- определяются значения параметров (включая качество ИУФ), описывающие критичность состояния подсистем ИУС $X^* = (x_1^*, x_2^*, x_3^*, ..., x_n^*)$;

- определяются значения функции принадлежности $\mu^{a_i^{jp}}(x_i^*)$ при фиксированных значениях параметров $X^* = (x_1^*, x_2^*, x_3^*, ..., x_n^*)$;

- используя логические уравнения, определяются значения функций принадлежности $\mu^{d_j}(x_1^*, x_2^*, ..., x_n^*)$ для всех возможных оценок уровней критичности каждого компонента ИУС;

- далее по значениям ЛП критичность состояния определяются уровни деградации ИУС в целом.

- на основании значений о текущем уровне деградации принимается решение о выработке мероприятий по повышению безопасности ИУС.

В оценки уровня деградации выбирается d_j^*, для которого:

$$\mu^{d_j^*}(Cr_{S_1}^*, Cr_{S_2}^*, Cr_{S_3}^*, ..., Cr_{S_n}^*, ...Cr_{S_N}^*) = \max \mu^{d_j^*}(Cr_{S_1}^*, Cr_{S_2}^*, Cr_{S_3}^*, ..., Cr_{S_n}^*, ...Cr_{S_N}^*),$$
$$j = \overline{1,m}.$$

На рис. 2.5 приведен фрагмент оценки и снижения уровня деградации для всей системы (АЭС).

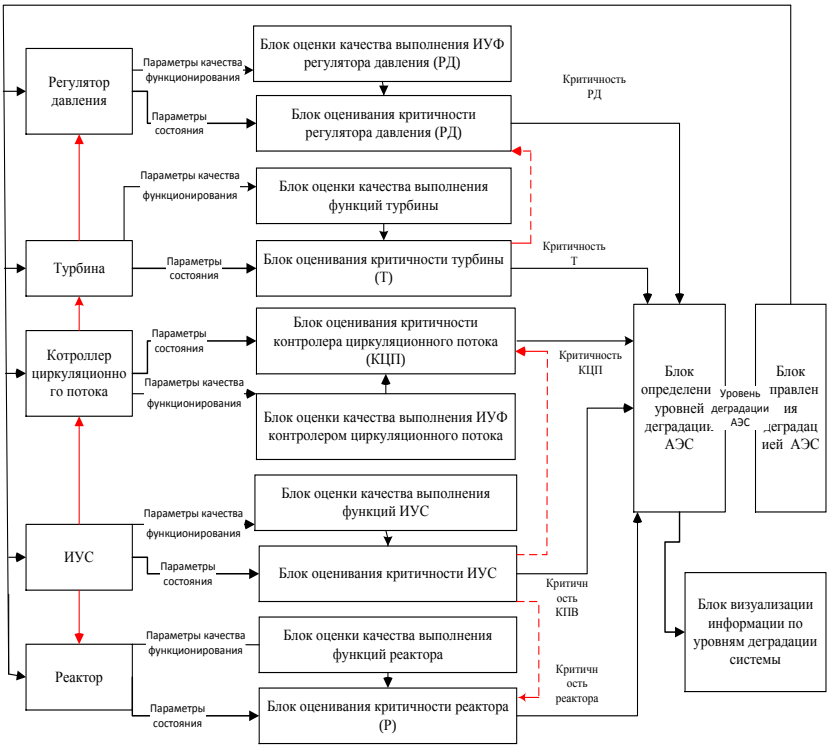


Рис. 2.5. Фрагмент оценки и снижения уровня
деградации системы (АЭС)

Таким образом, с использованием ЛЛМ могут быть получены прогнозные оценки уровней деградации ИУС. Нечеткий вывод, используемый для определения оценок критичности систем и деградации смарт грид в целом, позволяет учесть большее количество показателей, описывающих их функционирование и понизить размерность вычислений без ограничений по квалиметрической природе показателей. Нечеткую продукционную модель целесообразно использовать для уровня, который может быть адекватно описан с использованием базы правил, имеет расширенную систему мониторинга параметров, характеризующих качество выполнения функций безопасности.

Fuzzy Logic Toolbox – это пакет расширения MATLAB, содержащий инструменты для проектирования систем нечеткой логики.

Пакет позволят создавать экспертные системы на основе нечеткой логики, проводить кластеризацию нечеткими алгоритмами, а также проектировать нечеткие нейросети.

Пакет включает графический интерфейс для интерактивного пошагового проектирования нечетких систем, функции командной строки для разработки программ, а также специальные блоки для построения систем нечеткой логики в Simulink.

Все функции пакета написаны на открытом языке MATLAB, что позволяет контролировать исполнение алгоритмов, изменять исходный код, а также создавать свои собственные функции и процедуры.

Ввод исходных данных

1. Подсистема сбора и размножения информации от первичных датчиков – отвечает за сбор информации с датчиков и их передачу на дальнейшую обработку. На её работу влияют следующие параметры:

1.1. Точность измерений аналоговых сигналов первичными датчиками – неточные данные не позволят системе сделать правильные выводы о состоянии каких-либо объектов и предпринять необходимые меры.

1.2. Состояние линий связи – влияет на скорость и точность передачи данных, полученных с помощью датчика.

1.3. Напряжение в линиях связи – при низких значениях сигнал может не доходить до приемника, при высоких – нагрев линий связи, что ведет к их повреждению.

2. *Подсистема сбора и обработки входной информации* – отвечает за сбор дополнительной информации и обработку информации, полученной от первичных датчиков.

2.1. Состояние блоков логики – в случае выхода из строя большей части блоков логики обработка сигналов значительно замедлится или же станет невозможной.

2.2. Скорость обработки входных сигналов – низкая скорость обработки значительно замедлит работу систему.

2.3. Вероятность ошибки квантования АЦП – ошибка квантования может исказить сигнал, тем самым повлиять на решение, принимаемое блоками управления.

3. *Подсистема алгоритмов* – отвечает за вторичную обработку сигналов, их преобразование для передачи в блоки управления.

3.1. Состояние демпфера – в неисправном состоянии не способен погасить колебания сигнала.

3.2. Вероятность ошибки при контроле скорости изменения параметра – при ошибке система не сможет правильно и своевременно отреагировать на изменение какого-либо параметра.

3.3. Точность медианного фильтра – низкая точность может привести к неправильному преобразованию сигнала.

4. *Подсистема избирательного управления* – отвечает за ПТК (программно-технические комплексы) и работу с информационными потоками.

4.1. Состояние линий связи - влияет на скорость и точность передачи данных.

4.2. Вероятность ошибки передачи данных в ПТК – передача сигнала в неправильный ПТК может привести к непредсказуемым последствиям.

4.3. Состояние ПТК – в случае неисправности возможен полный отказ системы.

5. *Подсистема формирования сигналов управления* – отвечает за формирование сигналов и их передачу в БУИМ (блок управления исполнительным механизмом) и от ИМ (исполнительный механизм).

5.1. Количество исправных ламп мнемосхемы – при недостаточном количестве ламп корректное формирование управляющих сигналов будет невозможно.

5.2. Состояние линий между БУИМ и ИМ – в случае неисправности линий работа ИМ будет невозможна.

5.3. Скорость работы БУИМ – при низкой скорости работы конкретного БУИМ возможна асинхронная работа внутри подсистемы, что значительно замедлит работу подсистемы.

6. *Подсистема электропитания первичных датчиков* – отвечает за питание первичных датчиков.

6.1. Точность вычисления выходного напряжения – ошибка при

задании выходного напряжения может привести к отказу работы первичных датчиков.

6.2. Состояние датчиков в рабочей зоне – в случае выхода датчиков из строя корректная работа системы невозможна.

6.3. Количество рабочих выходов – при низком значении этого параметра обеспечить все датчики необходимым уровнем питания невозможно.

7. *Подсистема диагностики, архивирования и представления информации* – отвечает за диагностику, хранение и вывод информации, полученной в результате работы АСУ ТП.

7.1. Исправность диагностических систем – в случае неисправности обнаружить поломку в другой системе становится затруднительно.

7.2. Исправность линий связи – при неисправности скорость и точность передачи информации значительно падает

7.3. Пропускная способность линии связи – при низком значении параметра время получения информации значительно возрастет.

Рассмотрим иллюстративный пример определения уровня деградации подсистемы электропитания первичных датчиков с использованием логико-лингвистического моделирования первого рода. Будем использовать три параметра, описывающие уровень деградации подсистемы: точность вычисления выходного напряжения, состояние датчиков в рабочей зоне, количество рабочих выходов.

В соответствии с предлагаемым методом, вводятся лингвистические переменные, которые определяют уровень деградации подсистемы.

Лингвистические переменные, определяющие уровень деградации подсистемы, представлены в таблице 2.3.

Таблица 2.3. Лингвистические переменные, определяющие уровень деградации подсистемы

№	Лингвистические переменные	Универсальное множество	Оценочные термы
1	Точность вычисления выходного напряжения, x_1	VoltageAccuracy	High (H), Middle (M), Low(L)
2	Состояние датчиков в рабочей зоне, x_2	SensorState	
3	Количество рабочих выходов, x_3	CountOfOutput	

Пример экспертных данных, определяющих критичность состояния гидроэлектростанции, представлены в таблице 2.4.

Таблица 2.4. Пример экспертных данных, определяющих критичность состояния лингвистических переменных

№	Лингвистические переменные	Универсальное множество	High (H)	Middle (M)	Low (L)
1	Количество рабочих выходов, x3	CountOfOutput	0%-30%	10%-90%	66%-100%

Приступим к работе с программой. Стартовый экран Matlab показан на рис. 2.6.

Первое, что нужно сделать – это открыть fuzzy logic toolbox. Открытие происходит при нажатии на кнопку Apps => Show more и выборе Fuzzy Logic Designer (рис. 2.7):

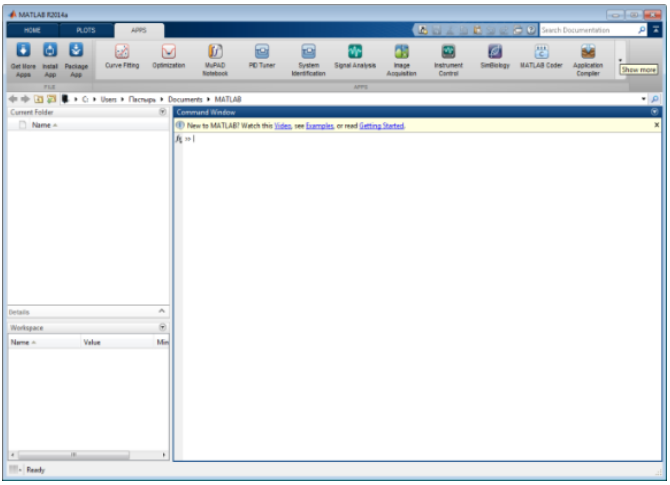


Рис. 2.6. Открытие Fuzzy Logic box (1)

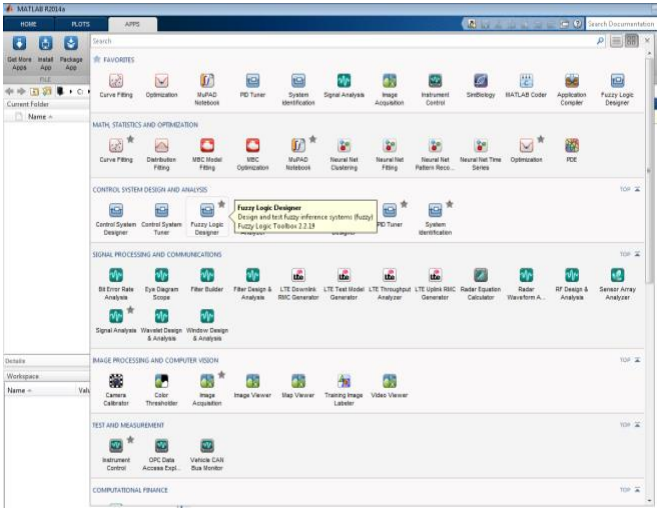


Рис. 2.7. Открытие Fuzzy Logic box (2)

Стартовая страница Fuzzy Logic box выглядит таким образом (рис. 2.8):

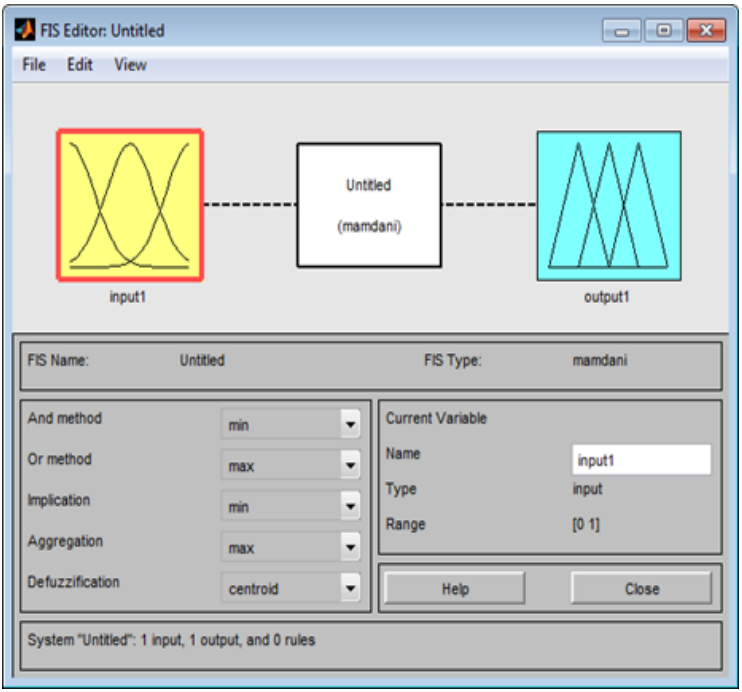


Рис. 2.8. Стартовая страница

где: **Input1** – входная переменная; **Output1** – выходная переменная; **Untilied** – это правила

Входные переменные

Для удобства работы переименуем входную переменную. Для этого выделим переменную, которая нам нужна и в графе **name** укажем имя (рис. 2.9):

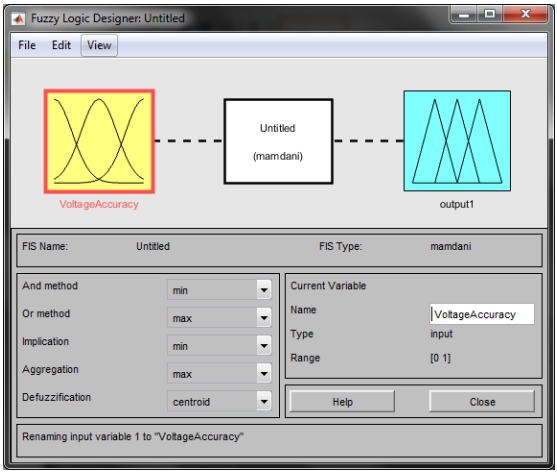


Рис. 2.9. Переименование переменных

Остальные параметры оставляем по умолчанию.

Откроем входную переменную и присвоим ее значения, определенные в таблице 2.10:

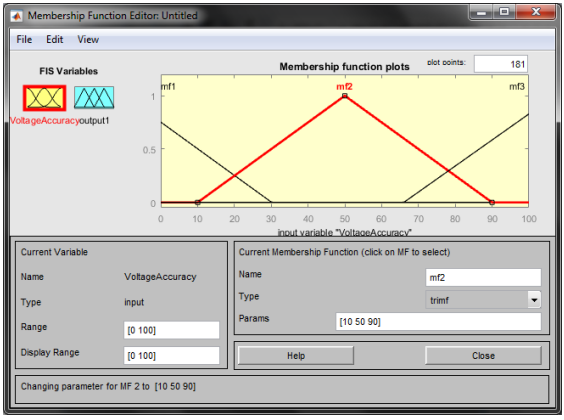


Рис. 2.10. Membership Function Editor

Приведем краткие пояснения к окнам, приведенным на рис.2.10:

- Current Variable Текущая переменная

– Name – Имя переменной;
– Type – Тип переменной (In/Out);
– Range – Интервал допустимых значений;
– Display Range – Размерность показываемых на графике значений.

- Current Membership Function

– Name – Имя текущего оценочного терма;
– Type – Тип графика (см. Fuzzy logic);
– Params – Интервал значений оценочного терма.

Рекомендуется выполнять изменения в таком порядке:

1) Изменения Интервала значений у переменной. Выполняются эти изменения во вкладке Range. В конкретной переменной это не нужно, потому что максимальное значение – 1 мм, а минимальное – 0 мм.

2) Изменения имен оценочных термов. Mf1, Mf2, Mf3 – это оценочные термы. В конкретном примере они носят имена High, Middle и Low, поэтому переименуем их.

Делается это во вкладке Name (рис. 2.11):

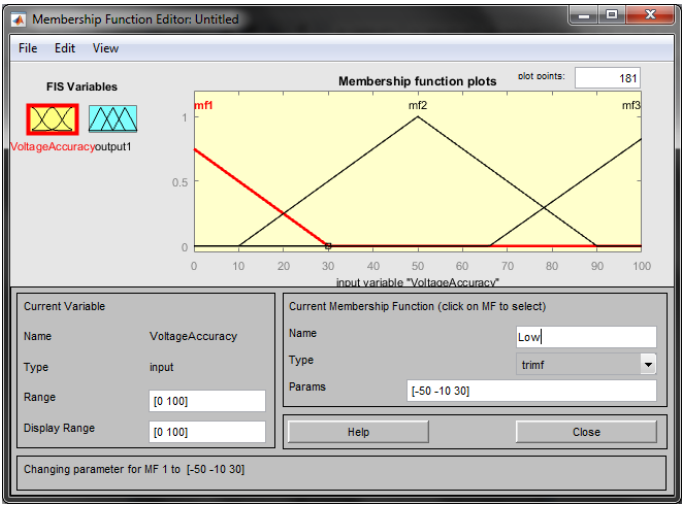


Рис. 2.11. Переименование оценочных Термов

3) Изменения типа графика. Во вкладке type можно изменить тип графика. Так как нам нужна треугольный график – оставим trimf (рисунок 2.12).

Могут быть использованы следующие функции принадлежности:

– trimf - треугольная функция принадлежности;
– trapmf - трапециевидная функция принадлежности;
– gbellmf - обобщенная колокообразная функция принадлежности;
– gaussmf - гауссовская функция принадлежности;
– gauss2mf - двухсторонняя гауссовская функция принадлежности;
– sigmf - сигмоидная функция принадлежности;
– dsigmf - функция принадлежности в виде разности между двумя сигмоидными функциями.

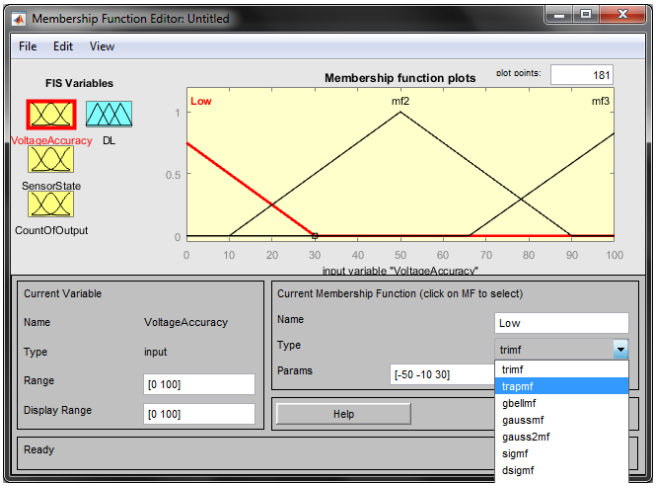


Рис. 2.12. Функции принадлежности

4) Изменения допустимых значений. Изменения выполняются во вкладке Params (рис. 2.13):

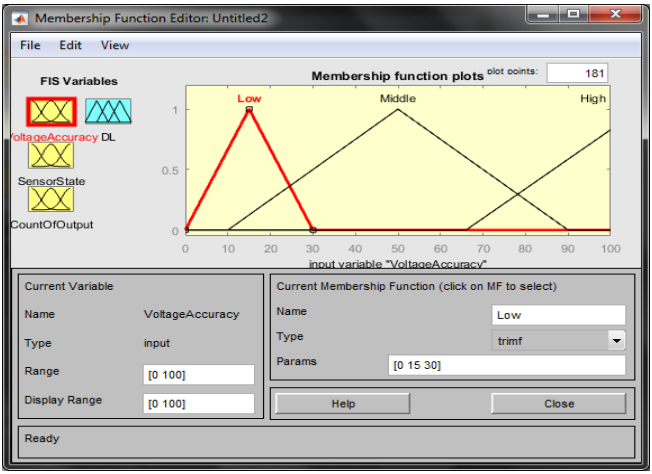


Рис. 2.13. Изменения интервала оценочных термов

В результате изменения получается готовая переменная RVK (рис. 2.14).

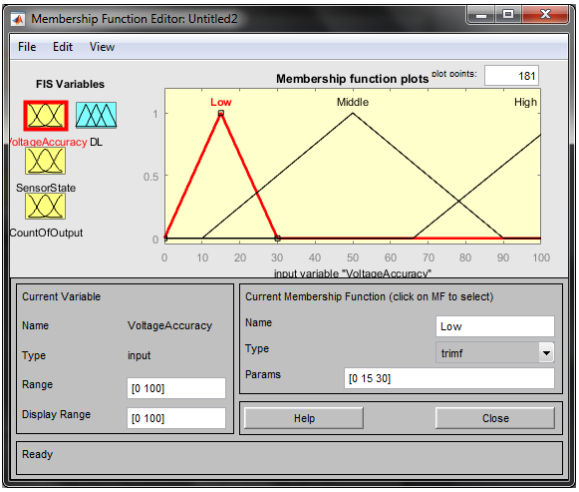


Рис. 2.14. Готовая переменная RVK

Далее нам нужно создать еще 2 входные переменные (по условию примера – три переменных) (рис. 2.15):

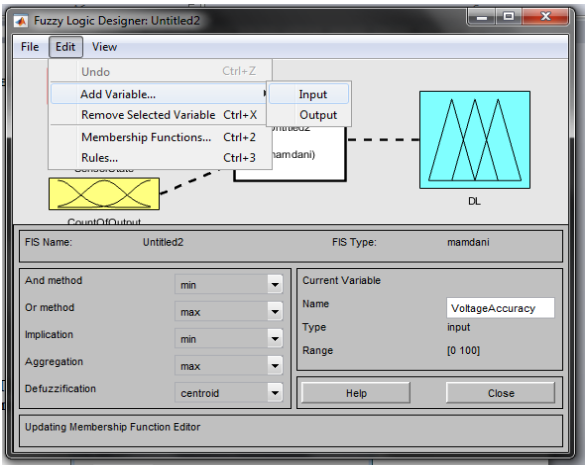


Рис. 2.15. Добавление переменных

При воспроизведении предыдущих шагов входные переменные примера должны выглядеть следующим образом (рис. 2.16):

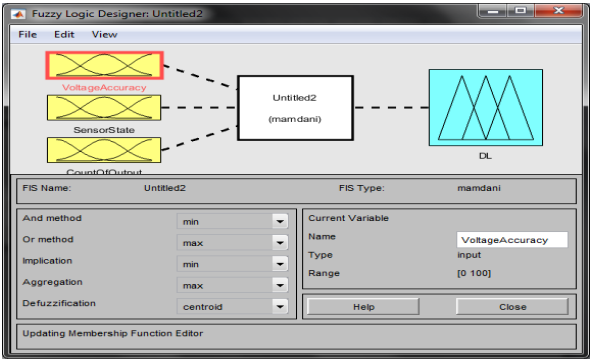


Рис. 2.16. Входные переменные

Выходные переменные

Производим изменение выходной переменной по такому же алгоритму, что и входных (рис. 2.17):

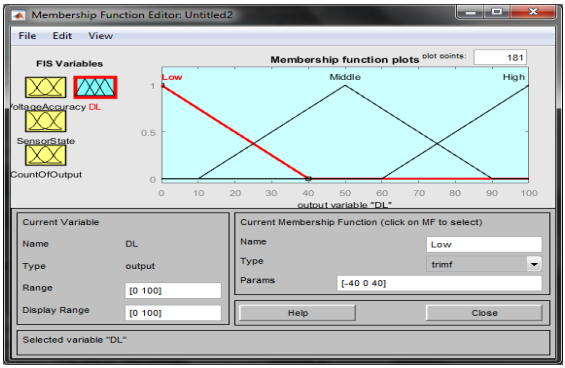


Рис. 2.17. Выходные переменные

Описание правил

Структура модели для определения уровня деградации представлена в виде:

$$Crt = f_d(x_1, x_2, x_3).$$

Логико-лингвистическое описание связи между параметрами состояния и уровнем деградации позволяет представить полученные знания в виде матрицы, представленной в таблице 2.5.

Таблица 2.5. Матрица знаний для оценивания уровня деградации

DL	Voltage Accuracy	SensorState	CountOfOutput
High (H)	L	L	L
H	M	L	L
H	L	M	L
H	M	L	M
Middle(M)	M	M	M
M	L	M	M
M	L	M	H
Low(L)	M	H	H
L	H	M	M
L	H	H	H

Далее, используя таблицы и операции ∧ (И – min) и ∨ (ИЛИ – max) записывается система логических уравнений (см. рисунок 2.18, для открытия в Fuzzy Logic Designer выбрать Edit-Rules), которая связывает функции принадлежности решений о величине оценки уровня деградации с переменными, которые влияют на нее (таблица 2.5):

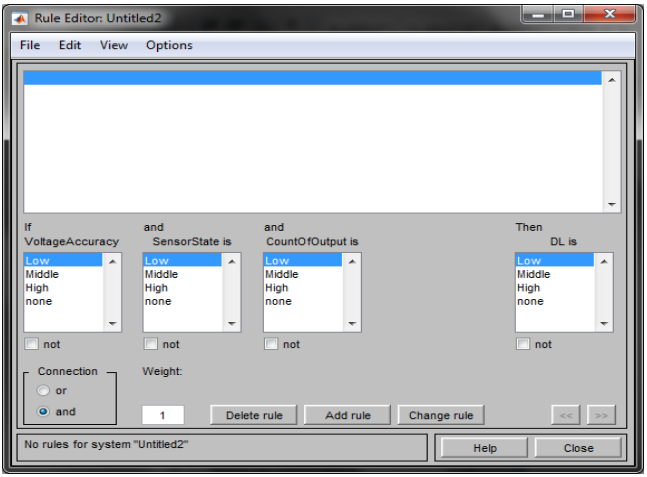


Рис. 2.18. Интерфейс для изменения fuzzy правил

В результате все правила выглядят таким образом (рис. 2.19):

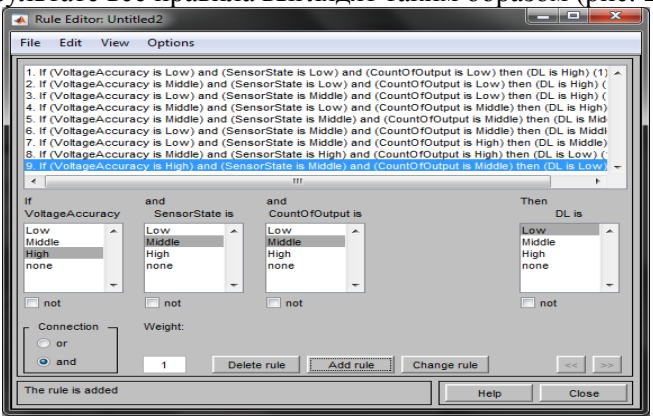


Рис. 2.19. Итоговая таблица правил

Результат:

Когда все правила будут заполнены, можно будет посмотреть результат анализа во вкладке **View** (рис.2.20):

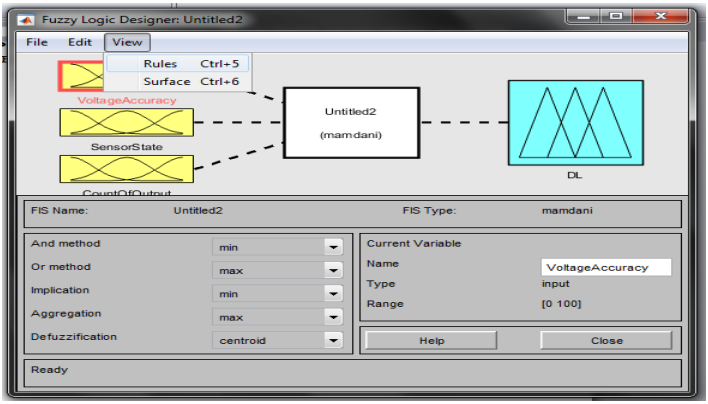


Рис. 2.20. Выбор вывода результата

При нажатии на **Rules** откроется Rule Viewer (рис. 2.21):

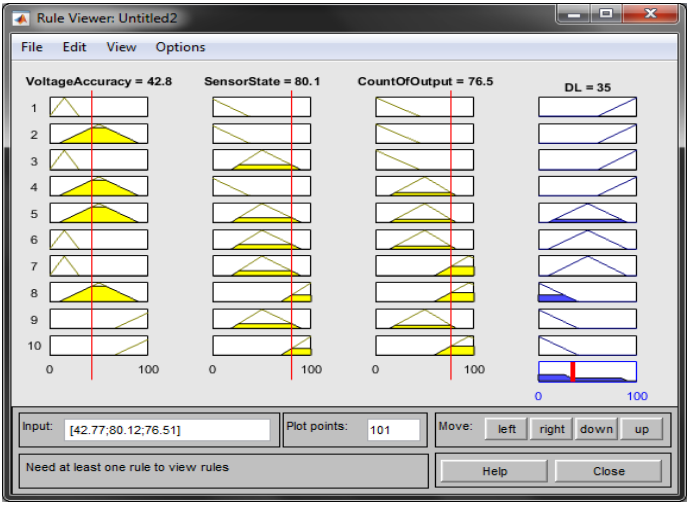


Рис. 2.21. Rule Viewer

В этой вкладке, изменяя входные данные значения происходит изменения выходной переменной, в данном случае оценка уровня деградации системы. Все изменения проходят согласно правил, описанных в таблице 2.8.

Так, например, для исходных данных:

- точность напряжения (VoltageAccuracy) 42,77%,
- состояние первичных датчиков датчиков (SensorState) 80,12%,
- кол-во рабочих выходов (CountOfOutput) 76,51%.

Уровень деградации системы составляет 35%.

Красная линия показывает в каком состоянии сейчас находиться система на термах выходной переменной.

При нажатии на вкладку **Surface** откроется (рис. 2.22):

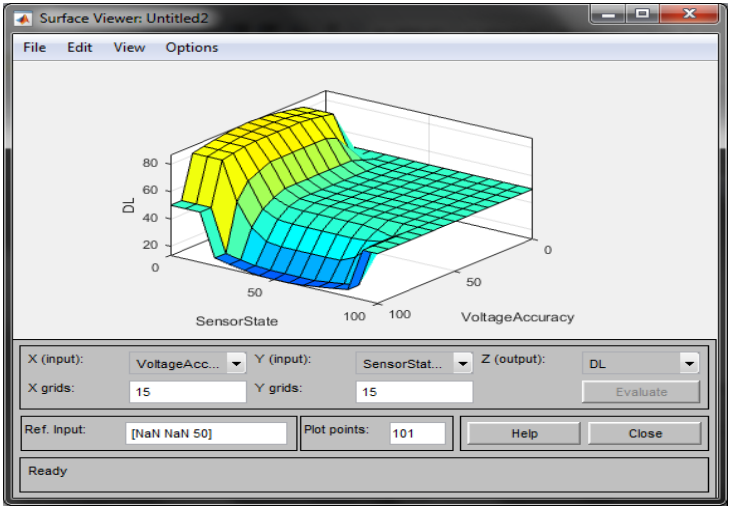


Рис. 2.22. График зависимости входных параметров и уровня деградации системы

Это 3D график зависимостей входных переменных и выходной переменной. Сохранение результатов проводится в следующем порядке (рис. 2.23):

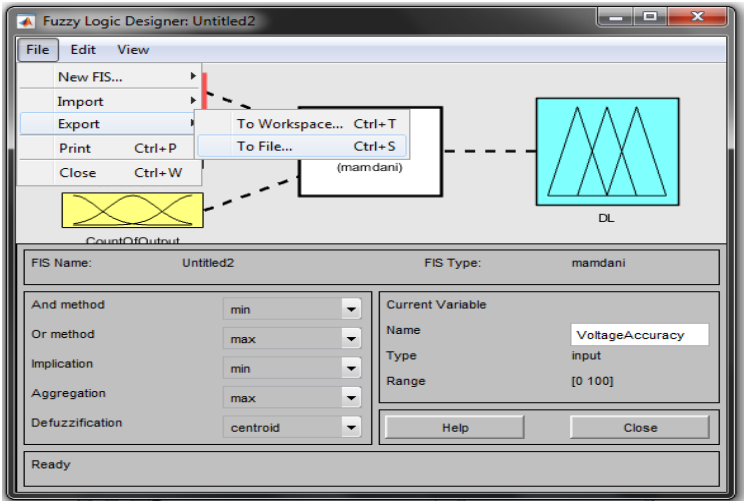


Рис. 2.23. Сохранение результатов

При выборе **To File** появляется такое диалоговое окно (рис.2.24):

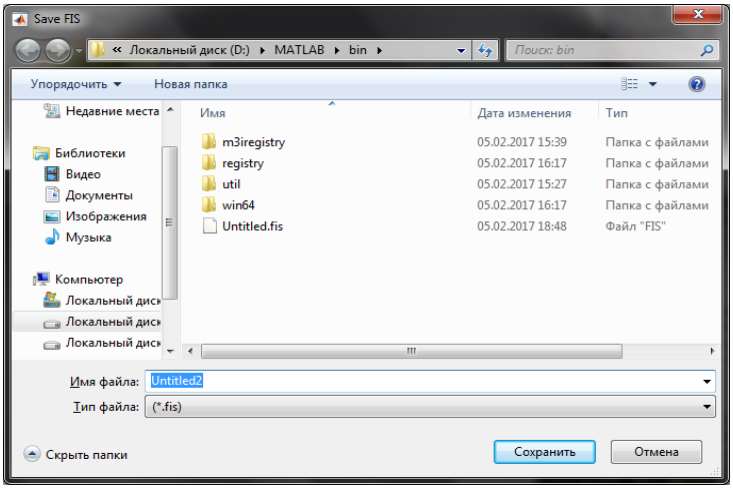


Рис. 2.24. Выбор файла для сохранения

Требования к содержанию аналитического отчета

Отчет должен содержать:
- цели и задачи проведения исследований;
- краткие теоретические сведения о подсистеме;
- результаты анализа с использованием Fuzzy logic Toolbox;
- результаты анализа и выводы, рекомендации.

Таблица 2.6. Варианты индивидуальных заданий для аналитического отчета

Вариант	Вид функции принадлежности	Стандартные системы нечеткого вывода	Подистема
1.	trimf	Сугено	Сбора и размножения информации от датчиков
2.	trapmf	Мамдани	Сбора и обработки входной информации
3.	gbellmf	Сугено	Подсистема алгоритмов
4.	gaussmf	Мамдани	Подсистема избирательного управления
5.	gauss2mf	Сугено	Формирования сигналов управления
6.	sigmf	Мамдани	Диагностики и архивирования информации
7.	dsigmf	Сугено	Подсистема технического обеспечения
8.	gauss2mf	Мамдани	Подсистема технологической сигнализации
9.	dsigmf	Сугено	Дистанционного управления
10.	gbellmf	Мамдани	Подсистема защит

Контрольные вопросы

1. Назовите основные особенности применения нечеткой логики при оценивании уровня деградации различных подсистем?
2. В чем особенности нечеткого управления сложными технологическими процессами?
3. Что такое нечеткие продукционные системы?
4. В чем основные отличия методов нечеткой логики от вероятностных методов анализа безопасности смарт грид?
5. В чем идея использования Fuzzy Logic Toolbox для оценки уровня деградации?
6. Как связаны между собой параметры подсистем и системы в целом? Как это учитывается в нечеткой логике?
7. Какие бывают виды функций принадлежности?
8. Какие виды отображения результата есть в Fuzzy Logic Toolbox? Кратко опишите их.
9. Как задаются правила в Fuzzy Logic Toolbox? Какие логические операции при этом используются? Приведите пример.
10. Для каких еще целей можно применять нечеткую логику? Приведите примеры.

3 МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕСДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СМАРТ ГРИД

3.1 Практикум №1. Изучение нормативной базы по диверсности систем в смарт грид (ИУС)

Форма занятия: практикум

Цель и задачи практикума

Целью является изучение нормативной базы по использованию диверсности систем смарт грид (ИУС).

Учебные задачи:

– изучение содержания основных документов нормативной базы использования диверсности ИУС для обеспечения безопасности;

– изучение существующих подходов и практик к использованию принципа диверсности при проектировании диверсных ИУС.

Практические задачи:

– получение навыков логического анализа нормативной базы по обеспечению безопасности смарт грид и ИУС, важных для ее безопасности.

Исследовательские задачи:

Провести сравнительный анализ нормативной базы по обеспечению безопасности смарт грид (ИУС).

Подготовка к практикуму

При подготовке к работе необходимо:

– уяснить цели и задачи;

– изучить теоретический материал, приведенный в описании, а также в [20-29].

Краткие теоретические сведения.

Основные характеристики нормативной базы, используемой для реализации принципа диверсности в ИУС критического применения

Стандарт IAEA Safety Glossary

В данном документе даны определения понятий "отказ по общей причине" и "диверсность". *Отказ по общей причине* (*common cause failure*) – отказ двух или более конструкций, систем и элементов вследствие единичного конкретного события или причины. *Диверсность (diversity)* – наличие двух или более резервных систем или элементов для выполнения одной определенной функции, при котором разные системы или элементы наделяются различными признаками таким образом, чтобы уменьшалась возможность ООП, включая общий отказ.

Стандарт IEC 60880–2:2006

В стандарте приведены требования по защите от дефектов программного обеспечения (ПО) и кодирования, способных привести к ООП функций, классифицированных по категории А в соответствии со стандартом IEC 61226. ООП относятся к отказам системы, возникающим в результате дефектов в функциональных требованиях, проектах системы или ПО.

В данном документе указывается, что: средством улучшения надежности ИУС и снижения вероятности определенных ООП является разнообразие. Поэтому возможность возникновения ООП из-за ПО должна рассматриваться при проектировании. Для защиты от ООП из-за ПО могут потребоваться изменения проекта и элементы защиты, включая разнообразие ПО;

- при реализации диверсности следует использовать следующее виды разнообразия:

1) независимые системы с функциональным разнообразием;

2) системное разнообразие,

3) разнообразие элементов ПО;

4) разнообразие подходов к проектированию.

Виды разнообразия 2–4 следует использовать, если функциональное разнообразие неуместно, недостаточно или невозможно.

Стандарт IEC 62340:2007

В документе отмечено, что применение диверсности формирует единственную возможность обеспечить защиту от постулируемого скрытого функционального дефекта в

спецификации требований. Диверсность позволяет реализовать следующее:

– при проектировании предотвращать дефекты в спецификации требований;

– во время эксплуатации осуществлять функции контроля и управления в случае отказа одной независимой системы контроля и управления путем реализации защиты в глубину и применения принципа диверсности.

В стандарте предложены методы предотвращения ООП ИУС. При реализации ИУС предлагается использовать следующие принципы: принцип независимости; применение функционального разнообразия; предотвращение распространения отказа через каналы связи, пр.

Стандарт IAEA.NS-G-1.1:2000

В стандарте указывается, что надежность ИУС может быть улучшена путем использования диверсности, чтобы уменьшить риски отказов по общей причине. Использование диверсных функций и системных компонент на различных уровнях проекта должно быть рассмотрено. Диверсность методов, языков, инструментальных средств и персонала также должна быть принята во внимание.

Показано, что для уменьшения рисков ООП диверсность следует инкорпорировать в архитектуру компьютерной системы. Диверсность оборудования означает, что различные типы оборудования используются, чтобы выполнять избыточные функции. Функциональная диверсность означает, что различные методы используются для выполнения отдельных функций.

Стандарт IAEA. NS-G-1.3:2002

В стандарте рассматриваются различные аспекты применения принципа диверсности при разработке ИУС безопасности АЭС.

Указывается, что диверсность – это принцип контроля различных параметров с использованием разных технологий, разных логических схем или алгоритмов, или же разных исполнительных устройств с тем, чтобы обеспечить возможность обнаруживать значительное событие и реагировать на него несколькими разными способами. Принцип диверсности включает

разнообразие операторов, конструкции, программного обеспечения, функциональное разнообразие, разнообразие сигналов, оборудования и систем.

Указано, что следует уделять внимание обеспечению того, чтобы диверсность реально достигалась в завершенном проекте и сохранялась в течение всего жизненного цикла станции. Показано, что разработчику проекта следует тщательно анализировать проект с целью исключения возможного появления признаков одинаковости при обеспечении разнообразия применительно к таким компонентам, как материалы, элементы конструкции, аналогичные процессы изготовления, аналогичное программное обеспечение или неявное сходство в принципах работы или общих вспомогательных средствах.

Стандарт IEC 61508-2:2010 Ed.2

В стандарте указано на необходимость применения диверсности при проектировании аппаратного обеспечения (АО). Диверсность АО не требуется, если в процессе валидации и применения было продемонстрировано отсутствие проектных дефектов и защищенность от ООП. Уменьшение фактора ООП может быть достигнуто за счёт использования диверсных средств измерения и управления отказов разных каналов.

Кроме того, указано на необходимость применения диверсности при проектировании ПО в виде:

- диверсных техник мониторов с независимостью между мониторами и мониторируемыми функциями в одном компьютере, а также с разделением между компьютером-монитором и и мониторируемым компьютером;
- диверсности с имплементацией одной и различных спецификации требований к безопасности;
- программной диверсности, при которой параллельно выполняются версии программ с общими исходными данными, а их результаты сравниваются.

НП 306.5.02/3.035-2000

В документе указывается, что в ИУС, выполняющих функции аварийной защиты ядерного реактора, должен применяться метод повышения надежности путем использования различных

технических решений для выполнения одной и той же функции (принцип разнообразия - диверсности).

Соблюдение принципа разнообразия предусматривает различие:

– алгоритмов выполнения одной и той же функции;

– программ, реализующих соответствующий алгоритм, например, созданных с использованием разных языков, разных средств программирования, разными разработчиками и т.д.;

– технических средств, участвующих в реализации функции, например, основанных на разных принципах действия, использующих разную элементную базу, полученных от разных поставщиков и т.п.

Стандарт IEEE Std 7-4.3.2:2003

В данном стандарте:

– обосновывается необходимость применения диверсности в качестве дополнительной меры обеспечения безопасности, наряду с защитой в глубину;

– определяются некоторые виды диверсности;

– описывается методика определения необходимости применения диверсности;

– обосновывается необходимость оценки уровня внесенной диверсности.

NUREG/CR–7007

Документ NUREG/CR-6303 регламентирует виды и подвиды диверсности, описывает методику количественной оценки диверсности. Выделены следующие виды диверсности:

1) Проектная диверсность (Design), включая:

– различные технологии (different technologies);

– различные подходы при одной технологии (different approaches within a technology);

– различные архитектуры (different architectures);

2) Диверсность производителей оборудования (Equipment Manufacturer), включая:

– различные производители оборудования принципиально различного дизайна (different manufacturers of fundamentally different equipment designs)

– один производитель оборудования принципиально различного дизайна (same manufacturer of fundamentally different equipment designs);

– различные производители оборудования одного дизайна (different manufacturers of same equipment design);

– один производитель разных вариантов оборудования одного дизайна (same manufacturer of different versions of the same equipment design);

3) Диверсность оборудования логической обработки (Logic Processing Equipment), включая:

– разные архитектуры (different logic processing architectures);

– разные версии одной архитектуры (different logic processing versions in same architecture);

– разные компоненты (different component integration architectures);

– разные потоки данных (different data flow architectures);

4) Функциональная диверсность (Function), включая:

– разные механизмы реализации функции безопасности (different underlying mechanisms to accomplish safety function);

– разные цели, функции, логика и исполнительные средства (different purpose, function, control logic, or actuation means of same underlying mechanism);

– разная шкала времени (different response time scale);

5) Диверсность жизненного цикла (Life-cycle), включая:

– разные проектные компании (different design organizations/companies);

– разные команды менеджмента в одной компании (different management teams within the same company);

– различные дизайнеры, программисты (different designers, engineers, and/or programmers);

– разные команды валидации и имплементации (different implementation/validation teams (testers, installers, or certification personnel);

6) Сигнальная диверсность (Signal), включая:

– разные параметры, измеряемые на основе разных физических эффектов (different parameters sensed by different physical effects);

– разные параметры, измеряемые на основе одного физического эффекта (different parameters sensed by the same physical effects);

– одинаковые параметры, измеряемые избыточным множеством однотипных датчиков (same parameter sensed by a different redundant set of similar sensors);

7) Логическая диверсность (Logic), включая:

– различные алгоритмы, логика и архитектура (different algorithms, logic, and program architecture);

– различные время и порядок выполнения (different timing or order of execution);

– различные способы задания функций (different functional representations).

Программа исследований и разработок

Работа выполняется индивидуально и коллективно. Индивидуальная работа предусматривает подготовку каждым студентом обобщенной ER модели (сущность – связь) для формализованного описания документа нормативной базы.

Результаты выполнения индивидуального задания представляются в виде отчета.

Коллективное выполнение работы состоит в следующем. Студенты распределяются на три команды. Каждая команда получает задачу, связанную с подготовкой учебного проекта по сравнительной оценке двух *нормативных документов* (по указанию преподавателя).

Этапы создания учебного проекта:

1. Формирование команд. Распределение ролей в команде
2. Выбор группы методов.
3. Постановка целей.
4. Постановка задач.
5. Внутрикомандная работа.
6. Презентация результатов.

Сравнительная оценка должна быть основана на системе обоснованных критериев, позволяющих определить преимущества и недостатки подходов, описанных в нормативных документах, сферу их использования, пр.

Таблица 3.1. Варианты заданий для аналитического отчета

Вариант	Наименование стандарта по обеспечению безопасности
1	IEC 60880–2:2006
2	IEC 62340:2007
3	IEC 62340:2007
4	IAEA. NS-G-1.3:2002
5	IEC 61508-2:2010 Ed.2
6	НП 306.5.02/3.035-2000
7	IEEE Std 7-4.3.2:2003
8	NUREG/CR–7007
9	NUREG/CR–6006
Коллективная работа (сравнительный анализ вариантов)	
10	вариант 1, 2
11	вариант 3, 4
12	вариант 5, 6
13	вариант 5, 9
14	вариант 1, 4
15	вариант 4, 7

Требования к содержанию аналитического отчета

Отчет должен содержать:
- титульный лист;
- описание основных положений стандарта;
- область применения стандарта;
- формализированное описание стандарта в виде ER модели;
- перечень ссылочных материалов (дочерние стандарты);
- выводы.

Контрольные вопросы

1. Что понимается под диверсностью?
2. Дайте определения атрибутов и критериев диверсности?
3. Что позволяет обеспечить диверсность? За счет чего?
4. Назовите основные виды диверсности? В чем их отличие?
5. Как могут быть сгруппированы все существующие стандарты по диверсности? Каковы могут быть основные классификационные признаки?
6. В чем отличие аппаратной и программной диверсности?
7. Что такое функциональная диверсность?
8. Что понимается под диверсностью жизненного цикла?
9. Как связаны между собой стандарты по диверсности?

3.2 Практикум №2. Использование ИС оценивания диверсности систем в смарт грид

Форма занятия: практикум

Цель и задачи практикума

Целью является изучение методов и ИС оценивания диверсности ИУС смарт грид.

Учебные задачи:

– изучение критериев и атрибутов диверсности цифровых систем для обеспечения безопасности;

– анализ существующих подходов к использованию принципа диверсности при проектировании диверсных ИУС.

Практические задачи:

– получение навыков использования ИС оценивания диверсности систем в смарт грид.

Исследовательские задачи:

Исследовать предлагаемый подход к оценке диверсности на практическом примере.

Подготовка к практикуму

При подготовке к работе необходимо:

– уяснить цели и задачи;

– изучить теоретический материал, приведенный в описании.

Теоретический материал

Традиционные методы оценки диверсности не приводят к удовлетворительным результатам, когда исходное описание систем-альтернатив заведомо является неточным и неполным, а стремление получить всю информацию для оценки диверсности может привести к потере времени и средств, поскольку это может быть в принципе невозможно.

Кроме того, очень сложно определить значения атрибутов диверсности с использованием традиционных весовых коэффициентов и рангов. Причина – отсутствие необходимой статистики ООП, уникальность условий каждого проекта модернизации. Часть информации может быть представлена в виде выражений естественного языка, экспертных суждений и заключений.

В рамках данного подхода предложен метод обеспечения безопасности за счет выбора диверсной системы, который учитывает неопределенность, качественное описание систем.

Ниже приведено описание метода на примере выбора диверсной ИУС.

Описание стратегий диверсности ИУС.

Рациональный выбор пары основного и диверсного комплекта ИУС (ПТК) может быть представлен как стратегия диверсности.

Рассмотрим три типа стратегий диверсности.

Стратегия S_1 ориентирована на использование фундаментально различных технологий (цифровую или аналоговую) для систем, подсистем и компонентов, обеспечения избыточности в ИУС (ПТК).

Стратегия S_2 предполагает использование различных подходов “внутри” цифровой или аналоговой технологии.

Стратегия S_3 предполагает использование архитектурных вариаций как основу для ИУС (ПТК). В этом случае, основной комплект может быть выполнен с использованием ПЛИС на SRAM, а диверсный комплект на Flash- ПЛИС.

Для ПЛИС могут быть введены две дополнительные стратегии диверности S_4 и S_5.

Стратегия *S_4 представляет вариации “внутри”* SRAM (Flash) ПЛИС архитектуры (использование различных семейств).

Стратегия *S_5 представляет вариации “внутри” одного* семейства SRAM (Flash) ПЛИС (Stratix II ПЛИС и Stratix III ПЛИС). В общем случае, каждая стратегия диверсности S_i включает подмножество стратегий S_{ij}, где j – номер возможной альтернативы, относящейся к стратегии i данного типа.

Возможный вид дерева стратегий диверсности представлен на рис. 3.1.

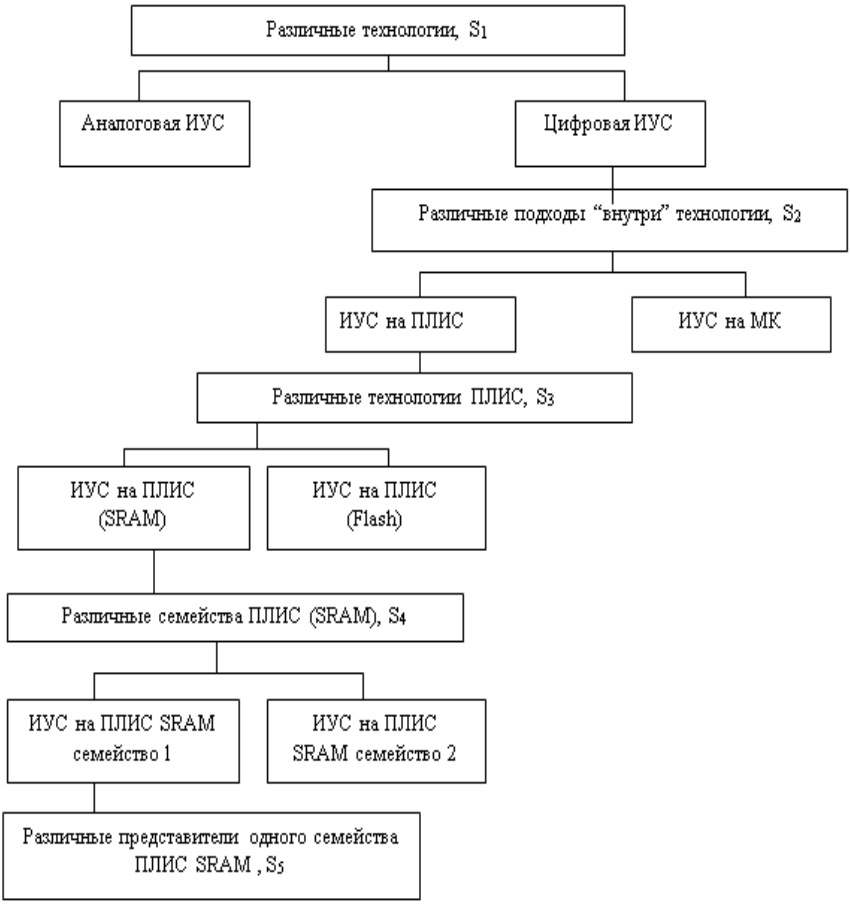


Рис. 3.1. Дерево стратегий диверсности ИУС

Этапы метода обеспечения безопасности за счет выбора диверсной системы представлены на рисунке 3.2.

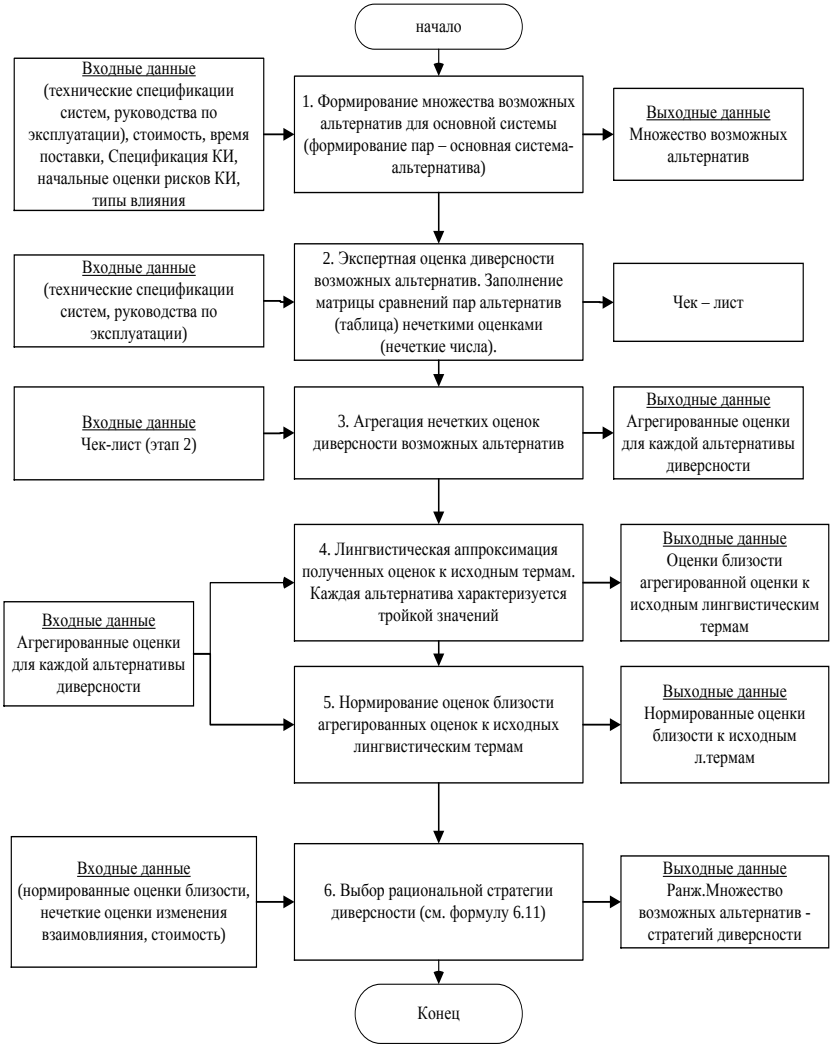


Рис. 3.2. Этапы метода обеспечения безопасности за счет выбора диверсной системы

Лингвистический подход к выбору рациональной стратегии диверсности учитывает качественную информацию, представленную в виде ЛП.

Для сравнения основного и диверсного комплекта ИУС (ПТК) эксперт учитывает ряд доступных свидетельств (фактов) для формирования субъективной уверенности в их сходстве (различии).

Основываясь на этих свидетельствах, эксперт оценивает сходство (близость) между основным и диверсным комплектом ИУС для каждой из стратегии с использованием лингвистических термов: SAME (S), NEARLY SAME (NS), DIFFERENT (D).

Рассмотрим этапы лингвистической оценки диверсности в условиях неопределенности.

Формирование множества стратегий диверсности.

Начальным этапом выбора является формирование множества возможных альтернатив для диверсного комплекта при фиксированном варианте первого комплекта ИУС (ПТК).

В данном примере, основной комплект системы выполнен на ПЛИС Flash (A3PE1500 от ProASIC 3/E семейства, Actel).

Возможные альтернативы для диверсного комплекта могут быть представлены как: S_{31} – основной комплект системы на Flash (A3PE1500, ProASIC 3/E family, Actel) и диверсный комплект – ПЛИС SRAM (EP1SGX40G, Cyclone IV GX family, Altera); S_{32} – основной комплект системы на Flash (A3PE1500, ProASIC 3/E family, Actel) и диверсный комплект – FPGA Antifuse (AX2000, Axcelerator family, Actel); S_{33} – основной комплект системы на Flash (A3PE1500, ProASIC 3/E family, Actel) и диверсный комплект – FPGA Antifuse (QL904M, QuickMIPS family, QuickLogic).

Экспертная оценка диверсности возможных альтернатив.

На этом этапе эксперты заполняют матрицу сравнений для оценки сходства (различия) между основным и диверсным комплектом ИУС (ПТК). Эксперт также определяет вес каждого критерия диверсности. В общем случае, вес критерия может быть представлен в разных квалиметрических шкалах. Так, например,

значение веса критерия может быть представлено в виде значений лингвистических переменных (Low, Medium, High), а также виде значений из интервала [0,1]. Чем больше величина весового коэффициента, тем больше влияние данного критерия на оценку диверсности. В рамках иллюстративного примера, значения весового коэффициента представлено в виде числа из интервала [0,1].

В таблице 3.2 представлен пример оценки диверсности для набора возможных альтернатив стратеги S_3 (различные ПЛИС технологии) и соответствующий набор критериев диверсности, применяемых для оценки диверсности.

Важно отметить, что в рамках данного метода предлагается дополнительный критерий диверсности – чувствительность системы-альтернативы к негативному влиянию от других систем в рамках КЭИ.

Таблица 3.2 – Пример сравнительной матрицы для S_3

Критерий диверсности	W_k, вес критерия диверсности	Альтернативы		
		Стратегия S_{31}, $ПЛИС_1$	Стратегия S_{32}, $ПЛИС_2$	Стратегия S_{33} $ПЛИС_3$
Дизайн				
Технологии	0,21	S	D	D
Подход (для одинаковой технологии)	0,19	S	NS	NS
Архитектура	0,6	D	S	D
Производитель компонентов				
Дизайн (для различных производителей)	0,5	S	D	D
Дизайн (для одного производителя)	0,5	D	D	NS

Продолжение таблицы 3.2

Критерий диверсности	W_k, вес критерия диверсности	Альтернативы		
		Стратегия S_{31}, $ПЛИС_1$	Стратегия S_{32}, $ПЛИС_2$	Стратегия S_{33} $ПЛИС_3$
Компоненты, реализующие логику процессов				
Логическая архитектура	0,3	D	D	S
Архитектура интеграции компонентов	0,7	S	D	NS
Функциональность				
Цель, функции, логика управления, органы управления	1	S	D	D
Жизненный цикл				
Команда проектировщиков	0,24	S	D	NS
Команда разработчиков	0,36	D	NS	NS
команда тестирования и валидации	0,4	S		D
Логика				
Алгоритмы, логика, программная архитектура	0,33	D	D	D
Время выполнения	0,47	D	NS	D
Функциональность алгоритмов	0,2	D	S	S

Продолжение таблицы 3.2

Критерий диверсности	W_k, вес критерия диверсности	Альтернативы		
		Стратегия S_{31}, ПЛИС$_1$	Стратегия S_{32}, ПЛИС$_2$	Стратегия S_{33} ПЛИС$_3$
Сигналы				
Параметры	0,6	D	NS	S
Используемые физические эффекты	0,4	NS	D	D
Чувствительность к негативному влиянию				
Физическое	0,2	D	D	S
Информационное	0,2	D	S	NS
Географическое	0,2	NS	D	S
Логическое	0,2	NS	D	S
Организаци-онное	0,2	NS	D	D

Эксперту необходимо использовать ЛП для оценки множества альтернатив S_{3j} для стратегии диверсности S_3. Нечеткие числа поддерживают семантику лингвистических термов. Нечеткое число в данном случае определяет область определения, в которой эксперт осуществляет лингвистическую оценку альтернатив. В рамках данного подхода семантика лингвистических термов представлена нечеткими треугольными числами M = <m, α, β>, с ФП вида:

$$\mu_M(x) = \begin{cases} 0, & for\ x \le m \le m - \alpha \\ 1 - \dfrac{m - x}{\alpha}, & for\ m - \alpha < x < m \\ 1, & for\ x = m \\ 0, & for\ x \ge m + \beta. \end{cases} \quad (3.1)$$

В рамках примера, определим следующую семантику для трех лингвистических термов (см. рисунок 6.5):

Nearly Same = (0,25; 0; 0,5), Same = (0,25, 0,5, 0,75),
Different = (0.5, 0,75, 1).

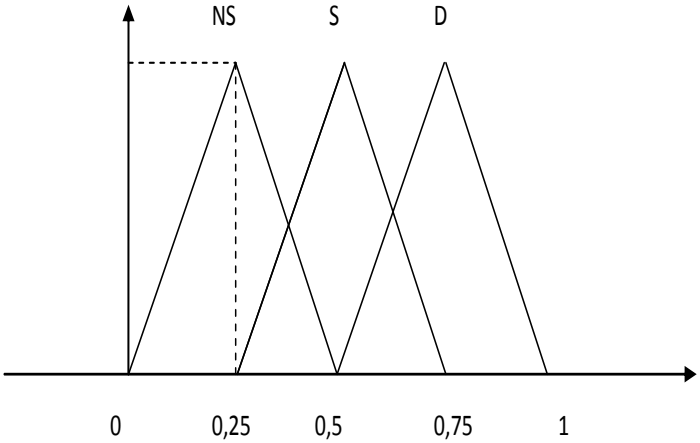


Рис. 3.3. Множество термов и определяющих их семантик

Этап агрегации

На данном этапе все лингвистические термы, полученные от экспертов, агрегируют для получения коллективной оценки для каждой из альтернатив. Это достигается путем вычисления нечеткой оценки диверсности D_{ij} как арифметического среднего:

$$D_{ij} = (\frac{1}{t}\sum_{i=1}^{t} w_k \times m_{ij}^t,\ \frac{1}{t}\sum_{i=1}^{t} w_k \times \alpha_{ij}^t,\ \frac{1}{t}\sum_{i=1}^{t} w_k \times \beta_{ij}^t)$$

где w_k – вес k – го критерия диверсности; $<m_{ij}^t, \alpha_{ij}^t, \beta_{ij}^t>$ - треугольное нечеткое число, представляющее одно из лингвистических термов {S, NS, D}, отнесенного *t*th экспертом для S_{ij} стратегии диверсности. Величина D_{ij} является расстоянием между атрибутами диверсности, описывающими основную и диверсную ИУС (ПТК). Следует отметить, что полученное нечеткое множество не совпадает ни с одним из первоначальных лингвистических термов. В этом случае (см. раздел 3), рекомендуется провести ЛА полученных результатов для их представления в рамках исходных лингвистических термов.

Таким образом, полученные нечеткие оценки диверсности D_{ij} для каждой из S_{ij} могут быть отображены к исходным лингвистическим термам (SAME, NEARLY SAME, DIFFERENT).

Метод использует расстояние между полученными нечеткими оценками диверсности, представленными нечеткими треугольными числами и первоначальными термами.

Это расстояние представляет степень совпадения коллективной оценки диверсности и каждого первоначального терма.

Например, расстояние между D_{ij} и выражениями SAME, NEARLY SAME, DIFFERENT может быть определено как:

$$d_{ij}^{(r)}(D_{ij},SAME) = \left[\sum_{j=1}^{3}(\mu_{Dij}^{j} - \mu_{same}^{j})^2\right]^{\frac{1}{2}};$$

$$d_{ij}^{(r)}(D_{ij},NEARLY\ SAME) = \left[\sum_{j=1}^{3}(\mu_{Dij}^{j} - \mu_{NS}^{j})^2\right]^{\frac{1}{2}};$$

$$d_{ij}^{(r)}(D_{ij},DIFFERENT) = \left[\sum_{j=1}^{3}(\mu_{Dij}^{j} - \mu_{different}^{j})^2\right]^{\frac{1}{2}}.$$

Таким образом, каждая стратегия диверсности характеризуется кортежем оценок вида $<d_{ij}^{(1)}, d_{ij}^{(2)}, d_{ij}^{(3)}>$, где $, d_{ij}^{(r)}$ – расстояние между полученным нечетким множеством и соответствующим первоначальным лингвистическим термом (SAME, NEARLY SAME, DIFFERENT).

Следует отметить, что каждое из расстояний $d_{ij}^{(r)}$ (j = 1,…J), где j – номер возможной альтернативы для стратегии диверсности S_i, является ненормированным. Чем ближе D_{ij} к *r*-th лингвистическому терму, тем меньше соответствующее расстояние $d_{ij}^{(r)}$. Если, $d_{ij}^{(r)}$ равно нулю, то это означает, что функция принадлежности полученной оценки диверсности полностью совпадает с функцией принадлежности *r*-th лингвистического терма.

В этом случае нецелесообразно проводить дальнейшую оценку расстояний до других термов, в виду их взаимоисключения.

Предположим, что $d_{ij}^{(3)}$ является наименьшей из полученных оценок D_{ij} и пусть α_{i1}, α_{i2}, α_{i3} представляют величины определяемые как отношение каждого полученного расстояния $d_{ij}^{(r)}$ к величине $d_{ij}^{(3)}$.

Тогда, $\alpha_{ij}^{(r)}$ (r= 1, 2, 3) могут быть определены как:

$$\alpha_{ij}^{(r)} = \frac{1}{\frac{d_{ij}^{(r)}}{d_{ij}^{(3)}}}, \; r = 1,2,3.$$

Если $d_{ij}^{(3)} = 0$ тогда $\alpha_{ij}^{(3)} = 1$ и остальные равны 0. Тогда $\alpha_{ij}^{(r)}$ (r = 1, 2, 3) могут быть нормированы как:

$$\beta_{ij}^{(r)} = \frac{\alpha_{ij}^{(r)}}{\sum_{r=1}^{3} \alpha_{ij}^{(r)}}, r = 1,2,3. \qquad (3.2)$$

Каждая величина $\beta_{ij}^{(r)}$ представляет степень принадлежности нечеткой оценки диверсности D_{ij} *r*t-му первоначальному лингвистическому терму. Следует отметить, что если оценка D_{ij} полностью совпадает с *r*-м лингвистическим термом, то $\beta_{ij}^{(r)} = 1$, при этом все остальные значения равны 0. Сумма $\beta_{ij}^{(r)}$ равна 1.

Таким образом, величина $\beta_{ij}^{(r)}$ может рассматриваться как степень уверенности эксперта в том, что полученная нечеткая оценка диверсности для каждой из стратегий диверсности принадлежит соответствующему *r-th* лингвистическому выражению.

Результаты, полученные в рамках иллюстративного примера для рассматриваемых стратегий диверсности, приведены в таблице 3.3.

Таблица 3.3 Оценки диверсности для рассматриваемых стратегий

Стратегия диверсности	Степень принадлежности D_{ij} первоначальным термам		
	Same	Nearly Same	Different
S_{31}	0, 36	0,28	0,38
S_{32}	0,12	0,39	0, 49
S_{33}	0,33	0, 63	0, 04

При выборе стратегии необходимо учесть, как введение диверсности повлияет на изменение оценки влияния состояния одной системы на изменение состояния безопасности другой. Для реализации выбора рекомендуется использовать оценку принадлежности стратегии к терму DIFFERENT.

Идея диверсности предполагает найти такую диверсную систему, которая будет менее уязвима к негативному влиянию от других систем или факторов. С учетом того, что негативное взаимовлияние от внешних систем на системы без диверсности, равнозначно, предполагается, что введение диверсности сделает одну из систем менее чувствительным к этому негативному воздействию. Все это приводит к различным оценкам взаимовлияния между субъектом влияния (фактор безопасности, внешняя система) и основной системой и между субъектом влияния (фактор безопасности, внешняя система) и диверсной системой.

Выбор рациональной стратегии диверности.

На данном этапе все стратегии диверсности ранжируются с учетом коллективной лингвистической оценки и стоимости C_{ij} реализации данной стратегии диверсности. Рациональная стратегия диверсности может быть определена с использованием критерия вида:

$$S_{ij}^{*} = \arg\max \frac{\beta_{ij}^{(r)}}{c_{ij}^{*}}, \qquad (3.3)$$

где $\beta_{ij}^{(r)}$ *представляет степень принадлежности* D_{ij} r_{th} начальному лингвистическому терму; C_{ij}^{*} - относительная

стоимость стратегии S_{ij} нормированная к $\sum C_{ij}$, ij – номер стратегии диверсности;

В соответствии с подходом, рациональной стратегией диверсности является стратегия S_{31}: основной комплект - FLASH (A3PE1500, ProASIC 3/E семейство, Actel) и диверсный комплект – ПЛИС SRAM – (EP1SGX40G, Cyclone IV GX семейство, Altera)).

Краткое описание ИС оценивания диверсности

ИС позволяет выбрать диверсную систему для заданной основной с целью минимизации негативного взаимовлияния между ними и повышения безопасности.

Для запуска приложения необходимо перейти по ссылке: https://diverchecker.herokuapp.com/ либо установить на Android устройство версии старше 4.4.x apk файл с приложением.

Основными операциями при работе с приложением являются:

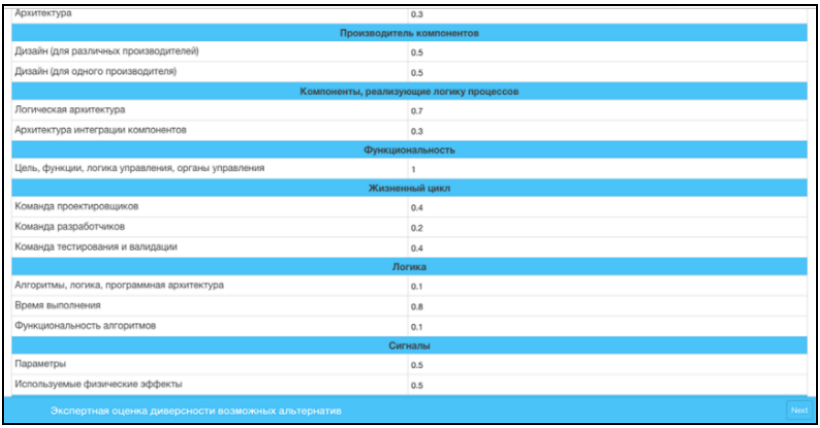
1. Открытие ссылки diverchecker и заполнение полей, описывающих основную систему. К основным полям относятся: “Name”, “Description”, “Link” and “Price”.

2. После ввода информации нажимается кнопка “Add characteristicks”.

Общий вид пользовательского интерфейса ИС приведен на рис. 3.4.

Рис. 3.4. Общий вид пользовательского интерфейса ИС

После этого пользователю необходимо ввести веса критериев диверсности систем. Важно отметить, что сумма весов должна быть равна 1.

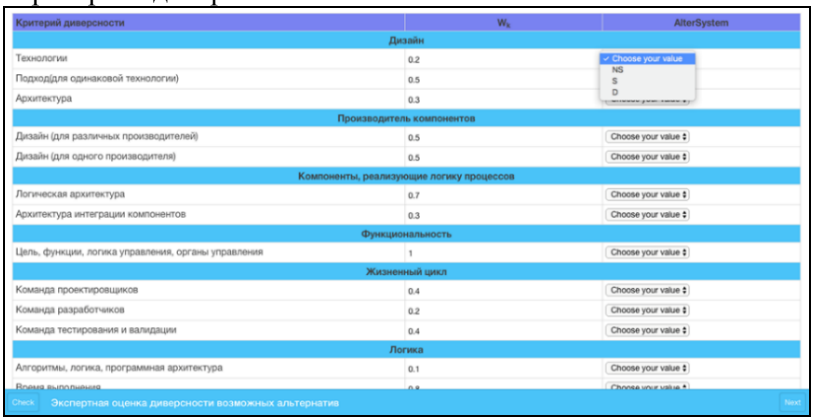


Архитектура	0.3
Производитель компонентов	
Дизайн (для различных производителей)	0.5
Дизайн (для одного производителя)	0.5
Компоненты, реализующие логику процессов	
Логическая архитектура	0.7
Архитектура интеграции компонентов	0.3
Функциональность	
Цель, функции, логика управления, органы управления	1
Жизненный цикл	
Команда проектировщиков	0.4
Команда разработчиков	0.2
Команда тестирования и валидации	0.4
Логика	
Алгоритмы, логика, программная архитектура	0.1
Время выполнения	0.8
Функциональность алгоритмов	0.1
Сигналы	
Параметры	0.5
Используемые физические эффекты	0.5

Экспертная оценка диверсности возможных альтернатив Next

Рис. 3.5. Ввод весов критериев диверсности

Далее, пользователю предлагается провести сравнительную оценку основной системы и ее возможной альтернативы. Пользователь заполняет таблицу (см. рис. 3.6), выбирая лингвистические термы (Same, Different, Nearly same) по каждому из критериев диверсности.



Критерий диверсности	W_k	AlterSystem
Дизайн		
Технологии	0.2	Choose your value
Подходідля одинаковой технологии)	0.5	NS, S, D
Архитектура	0.3	
Производитель компонентов		
Дизайн (для различных производителей)	0.5	Choose your value
Дизайн (для одного производителя)	0.5	Choose your value
Компоненты, реализующие логику процессов		
Логическая архитектура	0.7	Choose your value
Архитектура интеграции компонентов	0.3	Choose your value
Функциональность		
Цель, функции, логика управления, органы управления	1	Choose your value
Жизненный цикл		
Команда проектировщиков	0.4	Choose your value
Команда разработчиков	0.2	Choose your value
Команда тестирования и валидации	0.4	Choose your value
Логика		
Алгоритмы, логика, программная архитектура	0.1	Choose your value
Время выполнения	0.8	Choose your value

Check Экспертная оценка диверсности возможных альтернатив Next

Рис. 3.6. Сравнительная оценка основной системы и ее альтернативы

Далее, после нажатия кнопки “Check” появится окно с результатом (см. рис. 3.7).

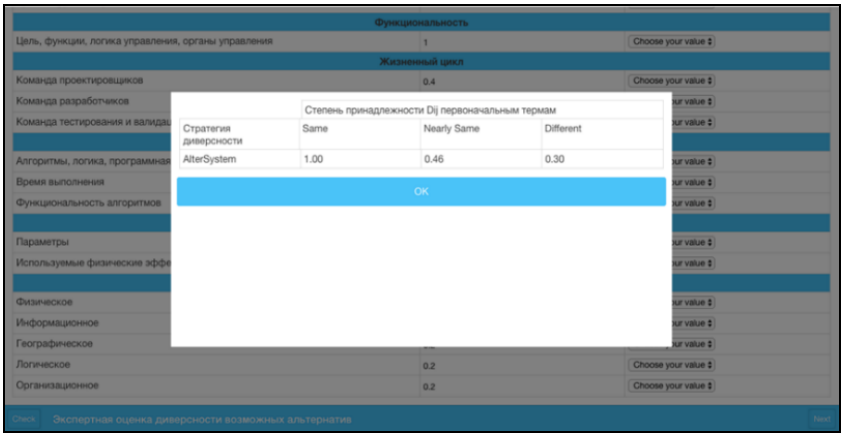


Рис. 3.7. Результат применения ИС

ИС позволяет автоматизировать выбор альтернативной системы с целью повышения безопасности КЭИ (ИУС) с учетом стоимости и снижения негативного влияния между системами. Результаты ИС – оценка сходства системы-альтернативы, выраженная как степень принадлежности трем лингвистическим переменным сходства, с учетом ее стоимости.

Программа исследований и разработок

Работа выполняется индивидуально. Индивидуальная работа предусматривает подготовку каждым студентом аналитического отчета по результатам сравнительного анализа стратегий диверсности, сформированных самостоятельно студентом с учетом вариантов задания.

Таблица 3.4. Варианты заданий

№ варианта	Основная система	Диверсная система	Примечание
1.	Аналоговая (S12)	Цифровая (S11)	
2.	ИУС на ПЛИС	ИУС на МК	
3.	S_{31}	S_{32}	См. пример
4.	S_{32}	S_{33}	См. пример
5.	S_{31}	S_{33}	См. пример
6.	S_{41}	S_{42}	
7.	S_{21}	S_{22}	
8.	ИУС на МК1	ИУС на МК2	
9.	ИУС на SRAM 1	ИУС на SRAM 2	
10.	S_{51}	S_{52}	

Результаты выполнения индивидуального задания представляются в виде отчета.

Требования к содержанию аналитического отчета

Отчет должен содержать:
- цели и задачи исследований;
- описание стратегий диверсности;
- описание этапов метода оценивания диверсности;
- результаты сравнительной оценки по выбору диверсной системы;
- выводы, рекомендации по снижению угроз.

Контрольные вопросы

1. Назовите существующие подходы к оцениванию диверсности систем?
2. Перечислите основные преимущества и недостатки известных методов оценивания диверсности ИУС?
3. Назовите основные этапы метода оценивания диверсности систем с использованием лингвистической информации?
4. Какой критерий сравнительной оценки, используемой в методе?
5. Что является входными данными метода?
6. В каком виде представляется полученное решение?
7. Перечислите известные ИС оценивания диверсности?
8. Назовите основные особенности ИС, поддерживающего применение данного метода?

4 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ

4.1 Пояснения к учебной программе

Самостоятельную работу над дисциплиной «**Основы анализа и обеспечения безопасности смарт грид**» (**«Fundamentals of safety analysis and assurance of smart grid»**) следует начинать с изучения учебной программы, которая приведена в данном Приложении. Эта программа включает следующие элементы.

Объект изучения – смарт грид системы и их ИУС.

Предмет изучения – концепции, общие принципы, методы, технологии, инструментальные средства оценивания и обеспечения надежности, безопасности смарт грид систем их ИУС.

Требования к исходным знаниям и навыкам, которые необходимо иметь перед началом изучения:

– принципы и методы системного анализа;

– теория вероятностей и математической статистики;

– теория надежности;

– теория байесовских сетей доверия;

– теория нечетких множеств;

– базовые знания в области современных компьютерных систем и информационных технологий.

Целью изучения дисциплины является приобретение студентами теоретических знаний и навыков оценивания надежности и безопасности при проектировании систем в смарт грид, использование ИС оценивания и обеспечения безопасности.

В результате ее изучения обучаемые должны научиться:

– проводить анализ информации и синтезировать на основе этого качественно новую информацию;

– формулировать, четко и ясно задавать вопросы и соответственно уметь грамотно отвечать на поставленные вопросы;

– мыслить креативно и критически;

– предпринимать исследовательские действия и оценивать получаемые результаты с использованием качественных и количественных показателей;

– формулировать возможные практические решения проблемы, эффективно использовать время и доступные ресурсы для достижения целей дисциплины;

– демонстрировать гибкость, инициативу, умение выражать свое мнение;

– совершенствовать и развивать свой интеллектуальный и общекультурный уровень;

– реализовывать способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности;

– применять перспективные методы оценивания надежности и безопасности смарт грид;

– применять ИС оценивания надежности и безопасности.

Вследствие изучения дисциплины аспиранты обязаны:

1) теоретический компонент:

– получить базовые представления о сфере проблем, связанных с информационными технологиями, используемыми при проектировании, оценках надежности и безопасности смарт грид (ИУС);

– иметь представление о методах, принципах и подходах, используемых при анализе безопасности систем смарт грид (ИУС).

2) познавательный компонент:

– знать фундаментальные положения в области «зеленых» технологий, используемых при проектировании ИУС;

– знать основные принципы риск анализа в сложных динамических системах, подходы к оптимизации параметров ИУС;

– знать методы нечеткого анализа надежности и безопасности сложных систем;

3) практический компонент:

– уметь использовать методы анализа надежности и безопасности смарт грид (ИУС);

– уметь использовать методы нечеткого анализа безопасности.

Структура и содержание модулей. Дисциплина включает три модуля:

МОДУЛЬ 1. МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ОЦЕНИВАНИЯ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ СМАРТ ГРИД

Лекции

ТЕМА 1. Введение в теорию надежности и безопасности смарт грид систем (ИУС).

ТЕМА 2. Обзор основных методов и подходов к оцениванию надежности смарт грид (ИУС).

ТЕМА 3. Анализ и оценка безопасности в смарт грид (ИУС).

Семинар (4 ч). Обзор и применение методов анализа надежности и безопасности смарт грид

Практикум (4 ч). Ознакомление с инструментальными средствами оценивания надежности смарт грид на примере ИС Cafta

Лабораторные работы

Лабораторная работа №1. Анализ надежности систем в смарт грид с использованием ИС Cafta (4 ч.)

Цель работы: оценить основные параметры надежности систем в смарт грид с использованием современных ИС оценки надежности.

Лабораторная работа №2. Интеграция методов оценивания надежности и безопасности (Cafta & Netica) (4 ч.)

Цель работы: исследовать особенности интеграции метод оценивания надежности и безопасности смарт грид для решения задач оценивания безопасности с учетом параметров надежности систем в смарт грид

МОДУЛЬ 2. НЕЧЕТКИЕ МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА АНАЛИЗА ДЕГРАДАЦИИ В СИСТЕМАХ СМАРТ ГРИД

ТЕМА 1. Обзор методов анализа многоуровневой деградации смарт грид (ИУС).

ТЕМА 2. Обзор нечетких методов и подходов анализа деградации смарт грид (ИУС).

ТЕМА 3. Обзор инструментальных средств анализа деградации смарт грид (ИУС).

Практикум 1. Анализ методов оценивания деградации систем в смарт грид (4 ч.)

Практикум 2. Анализ деградации систем смарт грид с использованием нечетких методов (4 ч.)

МОДУЛЬ 3. МЕТОДЫ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СМАРТ ГРИД

Лекции

ТЕМА 1. Обзор нормативной базы обеспечения безопасности в сферах, связанных с безопасностью.

ТЕМА 2. Обзор основных методов обеспечения безопасности в смарт грид (ИУС).

ТЕМА 3. Обзор инструментальных средств обеспечения безопасности смарт грид (ИУС).

Практикум 1. Изучение нормативной базы по диверсности систем в смарт грид (ИУС) (4 ч.)

Практикум 2. Использование ИС оценивания диверсности систем в смарт грид (4 ч.)

Методы оценки

Экзамен (100 %).

По окончании курса проводится 90-минутный экзамен.

Отчетность по дисциплине включает отчеты по каждому виду практического занятия, а также экзамен, который включает типовые вопросы и задачи.

4.2 Подготовка к занятиям и экзамену

При подготовке к лабораторным занятиям следует обратить внимание на уяснение целей и задач (учебных или теоретических, практических и исследовательских) и знаний, которые нужны для их выполнения. Особое внимание следует уделить формулировке выводов по результатам исследований при оформлении отчета. При самостоятельной подготовке к лабораторным работам важно правильно спланировать как свою индивидуальную, так и коллективную работу, организовать отбор и анализ необходимой литературы, подготовку к ответам на вопросы, приведенные в каждом разделе.

Следует обратить внимание на вопросы, вынесенные на самостоятельное изучение, которые приводятся в программе и уточняются преподавателем.

4.3 Вопросы для самостоятельной работы

1. Назовите ключевые инструментальные средства анализа надежности и безопасности смарт грид (ИУС)?
2. Назовите основные регулятивные документы (стандарты, положения, пр.) регламентирующие разработку вопросы обеспечения безопасности ИУС?
3. В чем основное отличие между методами оценивания надежности и безопасности смарт грид (ИУС)?
4. Каковы особенности применения методов нечеткого оценивания деградации систем смарт грид?
5. Назовите основные документы (стандарты), регламентирующие применение принципа диверсности для обеспечения безопасности ИУС?
6. Назовите основные технологии, используемые при реализации проектных решений ИУС. Почему важно проводить оценку безопасности проектных решений
7. В чем основное отличие методов нечеткого оценивания деградации от диаграмм влияния?
8. Каковы возможные подходы к интеграции методов оценивания безопасности и надежности смарт грид систем

ЛИТЕРАТУРА

1. Харченко В.С., Скляр В.В., Брежнев Е.В. Безопасность информационно-управляющих систем и инфраструктур. Модели, методы и технологии. Palmarium academic publishing, ФРГ. - 2013. - 529 с.

2. IAEA Nuclear Energy Series No. NG-T-3.8

3. Janaka Ekanayake etc. Smart grid technology and applications, A John Wiley & Sons, Ltd., Publication. - 2012. - 293 p.

4. Billinton R., Allan R. N., Reliability Evaluation of Power Systems (2nd Edition). New York: Plenum. - 2006.

5. Billinton R., Bagen I. Generating capacity adequacy evaluation of small stand-alone power systems containing solar energy. //Reliability Engineering & System Safety. - 2010. - 91(4). - P.438-443.

6. Billinton R., Allan R. N. Reliability Evaluation of Power Systems. Plenum Press, New York. - 1996. - 534 p.

7. Meeuwsen J. J., Kling W. L. Substation reliability evaluation including switching actions with redundant components // IEEE Transactions on Power Delivery. - 1997. - Vol.12,No.4. - P.1472-1479.

8. IEEE Committee Report. IEEE reliability test system // IEEE Transactions on Power Apparatus and Systems. - 1979. - Vol.PAS-98, No.6. - P.2047-2054.

9. Billinton R., Kumar S., Chowdhury N., Chu K., Khan E., Kos P., Nourbakhsh G., Oteng-Adjei J.

10. A reliability test system for educational purposes ñ Basic results. // IEEE Transactions on Power Systems. - 1990. - Vol.5, No.1. - P.319-325.

11. RAESAAR P. Simplified assessing of substation-originated outages in analysis of transmission system reliability. / Oil Shale. Estonian Academy Publishers. - 2007. - Vol.24,No.2, Special ISSN 0208-189X. - P.308-317

12. Towards An Ontology-Based Approach to Safety Management in Cooperative Intelligent Transportation Systems. / D.-J., Chen, F. Asplund, K.Östberg, E. Brezhniev, V.Kharchenko //Dependability and Complex Systems (DepCoS-RELCOMEX): proceedings of X International conf., Brunow (Poland), 29 June – 3 July 2015. - Brunow. - 2015. - P.107-115.

13. Kharchenko, V. Resilience Assurance for Software-Based Space Systems with Online Patching: Two Cases. / V. Kharchenko, Y. Ponochovnyi, A. Boyarchuk, E. Brezhnev //Proceedings of XI international conf. Dependability and Complex Systems (DepCoS-RELCOMEX), Brunow (Poland), 27 June – July 1, 2016. – Brunow, 2016. – P. 267-278.

14. Yastrebenetsky M., Kharchenko V. Reliability and Safety of Nuclear Power Plant Instrumentation and Control Systems: New Challenges and Solutions. /Proceedings of the 2016 Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management (SMRLO), Beer Sheva, Israel, February 15-18, 2016. - P.47-55.

15. Brezhnev E. MSS Models of Smart Grids with Multi-level Degradation and Recovery/ E. Brezhnev, H. Fesenko, V. Kharchenko, V. Levashenko, E. Zaitseva// Green IT Engineering: Concept, Models, Complex Systems Architectures/Studies in Systems. Decision and Control / V. Kharchenko, et al.; edited by V. Kharchenko, Yur. Kondratenko, Jan. Kacprzyk. – Switzerland: Springer International Publishing, 2017. – Part IV. – P. 209-228.

16. Брежнев Е.В., Харченко В.С. Методология обеспечения безопасности критических инфраструктур в условиях неопределенности: концепция и принципы. // Радіоелектронні і комп'ютерні системи. – 2015. – № 1(71). – С.25–32.

17. Брежнев Е.В. Метод оценивания рисков каскадных аварий (отказов) с использованием динамических матриц критичности. //Наука і техніка Повітряних Сил Збройних Сил України. - 2015. - № 1 (18). - С.187-190.

18. Zadeh L. and Kacprzyk J. Computing with Words in Information/Intelligent Systems – Part 1: Foundation; Part 2: Applications. Heidelberg, Germany: Physica-Verlag. - 1991. - Vol.1. - P.187-201.

19. Руководство пользователя Netica [Электронный ресурс]. - www.norsys.com

20. V. Novak, Mathematical fuzzy logic in modeling of natural language semantics, in: P. Wang, D. Ruan, E. Kerre (Eds.), Fuzzy Logic – A Spectrum of Theoretical & Practical Issues, Elsevier, Berlin - 2015.

21. The MathWorks. [online]. Fuzzy Logic Toolbox. Dec 16, 2005. - http://www.mathworks.com/products/fuzzylogic/

22. R. Belohlavek, V. Vychodil, Attribute implications in a fuzzy setting, in: B. Ganter, L. Kwuida (Eds.), ICFCA 2006, Lecture Notes in Artificial Intelligence, vol. 3874, Springer-Verlag, Heidelberg. - 2015.

23. Perfilieva I., Fuzzy transforms: a challenge to conventional transforms, in: P.W. Hawkes (Ed.), Advances in Images and Electron Physics, vol. 147, Elsevier Academic Press, San Diego. - 2015.

24. Uziel Sandler, Lev Tsitolovsky Neural Cell Behavior and Fuzzy Logic. Springer. - 2015.

25. Ganga, D.M., Carpinetti, L. A fuzzy logic approach to supply chain performance management. Int. J. Production Economics 134. - 2015.

26. Kharchenko V.. Diversity for Safety and Security of Embedded and Cyber Physical Systems: Fundamentals Review and Industrial Cases" / Proceeding of Baltic Electronic Conference (BEC), Tallinn, Estonia. - October 5-9, 2016. – 9 p.

27. Kharchenko V., Sachenko A., Kochan V., et al. Mobile Post-Emergency Monitoring System for Nuclear Power Plants. / Proceedings of the 12th ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer (ICTERI), Kyiv, Ukraine. - May 23-25, 2016. – 14p.

28. Kharchenko V., Duzhyi V., Sklyar V., Volkoviy A. Diversity assessment of multi-version NPP I&C Systems: NUREG7007 and CLB-based techniques. /Proceeding of EWDT Symposium, Rostov-Don, Russia, September 26-30, 2013. - P.6.

29. Иванченко О.В., Харченко В.С. Метод причинно-следственной декомпозиции аварий и инцидентов критических инфраструктур. // Радіоелектронні і комп'ютерні системи. - 2014. - С.12-17.

АНОТАЦІЯ

УДК 004.9+004.052:621.38

Брежнєв Є.В. **Основи аналізу та забезпечення безпеки смарт грид /** За ред. Харченка В.С. – Міністерство освіти і науки України, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», 2017. – 134 с.

Викладені матеріали практичної частини начального курсу “Основи аналізу та забезпечення безпеки смарт грид” (Fundamentals of smart grid safety analysis and assurance), підготовленого в рамках проекту Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

Курс присвячений теорії та практиці оцінювання та забезпечення надійності та безпеки смарт грид та їх інформаційно-керуючих систем. Приводиться навчальна програма курсу, опис семінарів, практикумів, методичні рекомендації щодо самостійного вивчення курсу.

Книга призначена для магістрів, аспірантів університетів, що навчаються за напрямками комп’ютерних наук, комп’ютерної та програмної інженерії, при вивченні методів та засобів оцінювання ризиків, безпеки смарт грид, а також може бути корисна викладачам, що проводять заняття з відповідних курсів.

Бібл. – 29 найменувань, рисунків – 75, таблиць – 13.

ЗМІСТ

ABSTRACT

UDC 004.9+004.052:621.38

Brezhnev E.V. Fundamentals of smart grid safety analysis and assurance. Practicum / Edited by Kharchenko V.S. – Department of Education and Science of Ukraine, National Aerospace University named after N. E. Zhukovsky "KhAI", Kharkiv, 2017. – 134 p.

Practical materials of study course "Fundamentals of smart grid safety analysis and assurance " given in this book are developed within проекту Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (reference number 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR).

The course is devoted to the theory and practice of reliability and safety assessment and assurance of smart grid and their I&C systems. There are the following: syllabus, description of seminars, practical works and recommendations for independent learning of course.

The book is supposed to be used by PhD students of universities that study computer science, computer and program engineering when studying methods and tools for safety, reliability assessment and assurance of smart grid. It could be very useful for lecturers and professors who conduct classes on corresponding courses.

Ref. – 29 items, tables-13, figures – 75

CONTENT

ПРИЛОЖЕНИЕ. УЧЕБНАЯ ПРОГРАММА

DESCRIPTION OF THE COURSE

TITLE OF THE COURSE	Code
Fundamentals of smart grid safety analysis and assurance	**CM4A**

Teacher(s)	Department
Coordinating: Dr. Brezhnev Eugene	Computer Systems and Networks

Study cycle	Level of the module	Type of the module
PhD	A	Full-time tuition

Form of delivery	Duration	Langage(s)
Full-time tuition	One semester	English

Prerequisites	
Prerequisites: – Computer Systems and System Analysis; – Probability Theory and Foundations of Mathematical Statistics; – Reliability Theory Foundations; – Mobile application Foundations; – Modeling Foundation knowledge and skills.	**Co-requisites (if necessary):**

Credits of the module	Total student workload	Contact hours	Individual work hours
3	90	58	32

Aim of the module (course unit): competences foreseeen by the study programme		
The aim of course is to create a knowledge acquisition about theory and practice of smart grid safety, reliability analysis and assurance. Acquisition of knowledge, engineering methodology on safety and reliability analysis and skills for application and application of methods for practical tasks during smart systems (I&C) development.		
Learning outcomes of module (course unit)	**Teaching/learning methods**	**Assessment methods**
At the end of course, the successful student will be able to: 1. Analyze and evaluate the main features and underlying IT of smart grid (I&C) reliability and safety assessment	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
2. Assimilate, evaluate and analyze information related to safety and reliability analysis	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
3. Use methods for safety and reliability analysis for solving the practical tasks	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
4. Use the software tools for smart grid (I&C) safety analysis and assurance	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
5. Analyze the modern IT—based I&C systems in respect to their safety assurance (diversity)	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire

Themes	Contact work hours							Time and tasks for individual work	
	Lectures	Consultations	Seminars	Practiacl work	Laboratory work	Placements	Total contact work	Individual work	Tasks
Module 1 Methods and software tools for smart grid reliability and safety assessment									
1. **Introduction to theory of smart grid reliability and safety** 1.1 General characteristics of course and specialty. Basic conceptions and definitions of smart grid 1.2 Smart grid safety and reliability challenges 1.3 Smart grid vulnerabilities. Relations between Safety and reliability	2						**2**	4	1.4 Smart grid vulnerability classification 1.5 I&C reliability assessment tools overview
2. Review of main methods and approaches to reliability assessment of smart grid (I&C) 2.1 Classification of existing methods for smart grid reliability classification 2.2 I&C reliability assessment 2.3 I&C failure classification	2			4	4		**2**	4	2.4. FMECA-based method for safety assessment

3. **Analysis and assessment of smart grid safety** 3.1. Smart grid risk analysis framework 3.2 Smart grid risk analysis methods and tools. Advantages and shortages 3.3. Smart grid risk simulations tools	2		4		4		18		
In total per module	6		4	4	8		22	8	
Module 2 Fuzzy methods and tools of smart grid degradation assessment									
1 Overview of methods of smart grid (I&C) multistate degradation SEI fuzzy safety analysis methods 1.1Foundation of fuzzy sets for systems engineering 1.2 Analysis and classification of existing fuzzy methods and approaches for degradation assessment 1.3 Methods Limitations, peculiarities of application	2							6	1.4 Soft computing for smart grid safety analysis. Computing with words
2. **Review of fuzzy methods and approaches for smart grid (I&C) degradation analysis** 2.1 Introduction to Fuzzy models. 2.2 Operation with fuzzy numbers	2							6	2.4 Application of fuzzy probabilities for Markovian models

2.3 Application of fuzzy numbers for degradation analysis									
3. **Overview of software tools for smart grid (I&C) degradation analysis.** 3.1 Classification of existing tools for fuzzy degradation assessment 3.2 Fuzzy Systems Software:Current Research Trends and Prospects 3.3 Case study: application of fuzzy tools for smart grid degradation analysis	2			6				6	3.4 Software for Soft Computing
In total per module	6			12			**18**	12	
Module 3 Methods and software tools for smart grid safety assurance									
1**. Review of normative basis for safety assurance** 1.1 Analysis of areas of diversity application 1.2 Classification of diversity standards 1.3 Shortages of normative basis	2							6	1.4 Application of diversity in aviation safety assurance
2. Review of methods of smart grid (I&C) safety assurance 2.1 Methods classification 2.2 Overview of methods for I&C safety assurance 2.3 Overview of . methods for I&C diversity assessment	2							6	2.4 Comparative analysis of method for I&C safety assurance

3. Review of software Tools for smart grid safety assurance 3.1 Existing tools classification 3.2 Tools shortage and limitations 3.3 Tool-based Case study development approach	2			6				6	3.4 Software tool integration approaches
In total per module	6			12			**18**	12	
Total/per course	18		4	26	8		58	32	

Assessment strategy	**Weight in %**	**Dead-lines**	**Assessment criteria**
Lecture activity, including fulfilling special self-tasks	10	7,14	**85% – 100%** Outstanding work, showing a full grasp of all the questions answered. **70% – 84%** Perfect or near perfect answers to a high proportion of the questions answered. There should be a thorough understanding and appreciation of the material. **60% – 69%** A very good knowledge of much of the important material, possibly excellent in places, but with a limited account of some significant topics. **50% – 59%** There should be a good grasp of several important topics, but with only a limited understanding or ability in places. There may be significant omissions. **45% – 49%** Students will show some relevant knowledge of some of the issues involved, but with a good grasp of only a minority of the material. Some topics may be answered well, but others will be either omitted or incorrect. **40% – 44%** There should be some work

			of some merit. There may be a few topics answered partly or there may be scattered or perfunctory knowledge across a larger range. **20% – 39%** There should be substantial deficiencies, or no answers, across large parts of the topics set, but with a little relevant and correct material in places. **0% – 19%** Very little or nothing that is correct and relevant.
Learning in laboratories	30	7,14	**85% – 100%** An outstanding piece of work, superbly organized and presented, excellent achievement of the objectives, evidence of original thought. **70% – 84%** Students will show a thorough understanding and appreciation of the material, producing work without significant error or omission. Objectives achieved well. Excellent organization and presentation. **60% – 69%** Students will show a clear understanding of the issues involved and the work should be well written and well organised. Good work towards the objectives. The exercise should show evidence that the student has thought about the topic and has not simply reproduced standard solutions or arguments. **50% – 59%** The work should show evidence that the student has a reasonable understanding of the basic material. There may be some signs of weakness, but overall the grasp of the topic should be sound. The presentation and organization should be reasonably clear, and the objectives should at least be partially achieved. **45% – 49%** Students will show some

			appreciation of the issues involved. The exercise will indicate a basic understanding of the topic, but will not have gone beyond this, and there may well be signs of confusion about more complex material. There should be fair work towards the laboratory work objectives. **40% – 44%** There should be some work towards the laboratory work objectives, but significant issues are likely to be neglected, and there will be little or no appreciation of the complexity of the problem. **20% – 39%** The work may contain some correct and relevant material, but most issues are neglected or are covered incorrectly. There should be some signs of appreciation of the laboratory work requirements. **0% – 19%** Very little or nothing that is correct and relevant and no real appreciation of the laboratory work requirements.
Module Evaluation Quest	60	8,16	The score corresponds to the percentage of correct answers to the test questions

Author	Year of issue	Title	No of perio-dical or volume	Place of printing. Printing house or internet link
Compulsory literature				
E.Brezhnev, V. Kharchenko, J. Vain, A. Boyarchuk	2015	Brezhniev, E. Cyber diversity for digital substations under uncertainties: assurance and assessment		Proceedings of XIX international conference, 16-20 July, 2015. - Zakynthos Island (Greece), 2015. - P. 507-512.
Popov, P.T.	2015	Stochastic	-	Proceedings of the 34th

		Modeling of Safety and Security of the e-Motor, an ASIL-D Device.		International Conf. on Computer Safety, Reliability, and Security, SAFECOMP 2015 23-25 September, Delft, The Netherlands.
V. Kharchenko, E. Brezhnev, V.Sklyar, V. Duzhyi	2015	FPGA Platform-Based NPP I&C Systems: Case Study of Diversity Assessment and Selection	-	Proceedings of IX International Topical Meeting, 23-26 February, 2015. – Charlotte (USA), 2015. – P. 1.
E. Brezhnev, V. Kharchenko, G. Fesenko, V. Levashenko, E. Zaitseva	2015	approach Smart grid substation availability assessment: Recovered MSS-based	-	Proceedings of XXV Conference, 7-10 September, 2015. – Zurich (Switzerland), 2015. – P. 1477-1484.
E. Brezhnev, B. Chernetskiy	2016	Risk Matrix-Based Method for Critical Infrastructure Safety Assessment Taking into Account Interdependencies	-	Proceedings of XX International Conf., 14-17 July, 2016. - Corfu Island (Greece), 2016. – Режим доступу: http://www.matec-conferences.org/articles/matecconf/pdf/2016/39/matecconf_cscc2
D.-J., Chen, F. Asplund, K.Östberg, E. Brezhniev, V.Kharchenko	2015	Towards An Ontology-Based Approach to Safety Management in Cooperative Intelligent Transportation Systems	-	Proceedings of X International conf., Brunow (Poland), 29 June – 3 July 2015. - Brunow, 2015. – P. 107–115.

V. Kharchenko, Y. Ponochovnyi, A. Boyarchuk, E. Brezhnev	2016	Resilience Assurance for Software-Based Space Systems with Online Patching: Two Cases	-	Proceedings of XI international conf., Brunow (Poland), 27 June – July 1, 2016. – Brunow, 2016. – P. 267-278.
O. Tarasyuk, A. Gorbenko, A. Romanovsky, V. Kharchenko, V. Ruban.	2015	The Impact of Consistency on System Latency in Fault Tolerant Internet Computing	Vol. 9038, 2015. – P. 179–192.	Lecture Notes in Computer Science
V. Kharchenko, E. Brezhnev	2015	Smart Grid Substation Availability Assessment: Recovered MSS-Based Approach		ESREL 2015 25th European Safety and Reliability Conference / Proceeding of the 25th European Safety and Reliability Conference
Popov, P. T.	2013	Bayesian reliability assessment of legacy safety-critical systems upgraded with fault-tolerant off-the-shelf software.	p. 98-113.	http://openaccess.city.ac.uk/13228/1/RESS_Popov_2012_v4.0_clean_final.pdf
Additional literature				
Jönsson H.	2007	Risk and Vulnerability Analysis of Complex Systems. A basis for proactive emergency management,	-	Department of Safety Engineering and System Safety Faculty of Engineering
F. Di Giandomenic	2008	Architecting Dependable Systems	Vol. 5135, 5	Lecture Notes in Computer Science

F. Di Giandomenic	2004	Dependability Modeling & Evaluation of Multiple-Phased Systems using DEEM in	Vol. 53, N. 4	IEEE Transactions on Reliability,
Vidmar P.	2005	Deterministic approach in tunnel safety assessment	№ 23(2)	Risk analysis.
F. Di Giandomenic	2005	A Modeling Methodology for Hierarchical control Systems and its Application	Vol. 10, N. 3	Journal of the Brazilian Computer Society, special Issue on Dependable Computing
L. Nordstrom	2008	Assessment of Information Security Levels in Power Communication Systems Using Evidential Reasoning	Issue 3	IEEE Transactions on Power Delivery
Zadeh L.	1965	Fuzzy sets	Vol. 8.	Inf. Control.
Svendsen, N.K. & Wolthusen, S.D.	2007	Connectivity models of interdependency in mixed-type critical infrastructure networks.	# 12	Information Security Technical Report

СОДЕРЖАНИЕ

Брежнєв Євген Віталійович

ОСНОВИ АНАЛІЗУ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СМАРТ ГРИД
Практикум
(російською мовою)

Редактор Харченко В.С.

Комп'ютерна верстка
Л.Д. Харченко

Зв. план, 2017
Підписаний до друку 03.04.2017
Формат 60х84 1/16. Папір офс. №2. Офс. друк.
Умов. друк. арк. 71,76. Уч.-вид. л. 73,52. Наклад 100 прим.
Замовлення 42. Ціна вільна

Національний аерокосмічний університет ім. М. Є. Жуковського
"Харківський авіаційний інститут"
61070, Харків-70, вул. Чкалова, 17
http://www.khai.edu

Віддруковано ФОП Лисенко І.Б.
61070, Харків-70, вул. Чкалова, 17, моторний корпус, к. 147
Свідоцтво про внесення суб'єкта видавничої справи в державний реєстр видавців, виготовлювачів і розповсюджувачів видавничої продукції
ДК №2607 от 11.09.06 р.