

среднее время восстановления работоспособного состояния объекта после отказа  $T_v$ . Если для конкретной КСУ имеем определенное МТТФ (Mean operating Time To Failure) - средняя наработка до первого отказа  $T_{cp}$ , то коэффициент  $K = T_{cp} / (T_{cp} + T_v)$  характеризует функционирование КСУ при наличии отказа и необходимости восстановления работоспособного состояния КСУ. Если коэффициент  $K$  приближенно равен 1, то это означает, что время  $T_v$  пренебрежимо мало по сравнению с  $T_{cp}$ . На основе анализа функционирования сложных систем можно сформулировать принципы создания ROC-ориентированной КСУ:

оперативная диагностика текущего состояния КСУ, позволяющая в автоматизированном режиме определять причины и место неполадок.

оперативное восстановление работоспособности КСУ с использованием программно-аппаратных средств, заложенных при проектировании КСУ.

Поставленные задачи могут быть решены путем моделирования КСУ с использованием интеллектуальных средств, в частности применением нейронечетких методов на основе ANFIS (adaptive network-based fuzzy inference system) – адаптивная нейронечеткая система логического вывода. Преимуществом данного метода является интеграция принципов нейронных сетей с нечеткой логикой. Вывод такой системы соответствует набору нечетких правил «если-то» (if-then), которые имеют способность к обучению.

Для текущей оценки состояния КСУ в системе ANFIS вводим лингвистическую переменную «Дефект» и термы данной переменной: {«нет», «легкий», «умеренный», «сильный», «разрушительный»}.

Различные виды отказов КСУ характеризуются классификационными признаками, которые будем рассматривать как нечеткие диагностические признаки. Каждый рассматриваемый признак – это нечеткое множество и определено лингвистически. Рассмотрим следующие диагностические признаки, которые описывают состояние дефекта.

1. Область возникновения отказов = {«значительная», «средняя», «незначительная»}.

2. Характер изменения параметров во время отказа = {«значительный (внезапный)», «средний», «незначительный (постепенный)»}.

3. Характер существования отказа во времени = {«значительный (длительный)», «средней длительности», «незначительный (кратковременный)»}.

4. Возможность обнаружения = {«сложная», «средняя», «несложная»}.

5. Обусловленность другими отказами (зависимость) = {«значительная», «средняя», «незначительная»}.

6. Возможность восстановления работоспособности после отказа = {«сложная», «средняя», «несложная»}.

7. Причина возникновения = {«сложная», «средняя», «несложная»}.

8. Тяжесть последствий = {«значительная», «средняя», «незначительная»}.

Для реализации диагностических алгоритмов применяем MatLab, а системы нечеткого вывода на основе адаптивных сетей (ANFIS) используются для решения проблем, связанных с идентификацией параметров. ANFIS представляет собой графическое сетевое представление нечетких систем типа Сугено, наделенных возможностями нейронного обучения. Сеть состоит из узлов с определенными функциями, собранными по слоям. ANFIS может построить сетевую реализацию правил IF / THEN. Все расчеты могут быть представлены в виде диаграммы. ANFIS обычно имеет 5 слоев нейронов, из которых нейроны в одном слое имеют одно и то же семейство функций.

При определении технического состояния сложных технических объектов основным критическим фактором является время принятия решения для локализации возникшей неисправности. Применение гибридной экспертной системы диагностирования с нейронечеткой сетевой базой знаний обеспечивает поддержку решений в ситуациях, для которых алгоритм диагностирования не известен и формируется по исходным данным в виде продукционных правил.

#### Список использованных источников

1. Кривуля Г. Экспертная диагностика компьютерных систем с использованием нейро-нечеткой базы знаний / Кривуля Г., Липчанский А., Е. Шеремет EWDTS'2014: продолжение. международной конференции. 15-17 сентября 2016 года. - Ереван, - с. 619-622
2. Кривуля, Г. Экспертно-оценочная модель диагностических признаков компьютерной системы / Г. Кривуля, А. Шкиль, Д. Кучеренко, А. Липчанский, Е. Шеремет // EWDTS'2014: Материалы международного конф., 26-29 сентября 2014 г. - Киев, Украина, 2014 г. - с. 286-289.

*Каменев О. Ю., к.т.н., доцент,  
Липко А. О., к.т.н., доцент (УкрДУЗТ)*

#### ВЕРИФІКАЦІЯ ПРОГРАМНИХ ЗАСОБІВ, РЕАЛІЗОВАНИХ МООВОЮ РЕЛЕЙНО- КОНТАКТНОЇ ЛОГІКИ

Значною складовою забезпечення надійного й безпечного функціонування автоматизованих систем керування (АСК) відповідальними технологічними

процесами є належне забезпечення програмних засобів.

Відома класична технологія верифікації прикладного програмного забезпечення (ПЗ) АСК є тестування на підставі складених програм і методик. У той же час використання ПЗ із відкритим кодом, що реалізується мовою релейно-контактної логіки, дозволяє реалізувати статичні методи дослідження та підтвердження безпеки використання. Пов'язано це з тим, що відповідні програмні засоби є інтуїтивно й інтерфейсно зрозумілими для спеціаліста-технолога в галузі використання АСК, що може навіть не мати навичок програмування. Такі засоби є аналогічними до класичних електричних кіл, що реалізують електромагнітні реле в якості логічних елементів. Спеціальні символи, що є мнемонічними повторювачами обмоток і контактів реле (фронтних і тилових), поєднані за різними схемами («I», «АБО», у порядку інверсії тощо), дозволяють реалізувати аналіз логіки функціонування відповідної схеми керування без динамічного відтворення роботи самої АСК [1].

Методика і програма статичної верифікації подібного ПЗ на предмет безпечності полягає, перш за все, у відслідковуванні протікання віртуальних електричних струмів по мнемонічним каналам віртуальної релейно-контактної схеми. При цьому процес верифікації розділяється на дві основні складові: перевірку надійності й працездатності ПЗ; перевірку безпечності використання ПЗ.

Перевірка I (група перевірок) полягає у верифікації відповідності вхідних, вихідних і внутрішніх змінних технічному завданню на реалізацію АСК. При цьому відслідковується правильність виконання вихідних команд залежно від поточного вхідного алфавіту та множини проміжних змінних. За модельованим станом проміжних внутрішніх змінних, що безпосередньо формують вихідні сигнали, оцінюється відповідність ПЗ поставленим до нього вимогам.

Перевірка II (група перевірок) полягає в примусовому формуванні помилкового вхідного алфавіту, що відтворює можливі небезпечні стани оточуючих об'єктів керування та контролю. Логіка функціонування безпечних АСК (що реалізується засобами ПЗ) має виключати небезпечне формування вихідних сигналів відповідальних кіл при будь-яких порушеннях алгоритмів подачі вхідних змінних, незалежно від поточного стану внутрішніх змінних. Отже, верифікація ПЗ на предмет безпечності полягає в формуванні всіх можливих комбінацій вхідного алфавіту, який сигналізує про порушення зовнішніх умов безпеки, при наступній перевірці безпечного формування «захисної» множини вихідних змінних [2].

Найбільш актуально та гостро проблема верифікації програмних засобів, реалізованих на мові релейно-контактної логіки, відчувається в сфері транспорту та енергетики, в якій використовуються резервовані програмовані логічні контролери. У рамках реалізації

програм і методик верифікації ПЗ формуються спеціалізовані інструментальні засоби, що прискорюють та частково автоматизують зазначений процес. Таким чином, одночасно вирішуються дві проблеми – верифікації ПЗ та мінімізації суб'єктивної складової людського фактору в цьому процесі.

#### Список використаних джерел

1. Development and investigation of methods of graphic-functional modeling of distribute systems / A. Bojnik, O. Progonnii // Eastern-European Journal of Enterprise Technologies. – Kharkov: Technology Center, 2018. – № 4/4(94). – P. 59-69.
2. Mathematical models in computer control systems railways and parallel computing Spring-Source. Monograph. / S. Listrovoy, S. Panchenko and oth. // Kharkiv: FOP Brovin O., 2017, 300 p.

*Родіонов С. В., к.т.н., доцент (УкрДУЗТ)*

#### ПРОВЕДЕННЯ ОЦІНКИ ЕФЕКТИВНОСТІ РАНГОВОГО ВИЯВЛЯЧА РАДІОСИГНАЛІВ В УМОВАХ ХАОТИЧНИХ ІМПУЛЬСНИХ РАДІОЗАВАД

В зв'язку зі збільшенням кількості мобільних радіозасобів, в тому числі і на залізничному транспорті, ускладнюється задача забезпечення їх електромагнітної сумісності, яка породжена дією різноманітних завад від різних джерел. Так радіостанції поїзного та станційного радіозв'язку зазнають впливу імпульсних завад від електромагнітного поля, яке створюється на електрифікованих ділянках залізниць, розташованих поблизу радіолокаційних станцій та інших радіозасобів. Вплив таких завад на роботу поїзних радіостанцій може привести до часткової втрати зв'язку між посадовими особами та як наслідок до втрати управління процесом перевезення. Це стає особливо актуальним при використанні систем передачі даних.

Проведена оцінка завадостійкості різних виявлячів дискретних сигналів в умовах впливу хаотичних імпульсних завад (ХІЗ). Розглянути дві різноманітні моделі впливу ХІЗ та шуму на класичний та ранговий виявлячи. У якості параметрів по яким здійснювалась порівняльна оцінка вибрана ймовірність правильного виявлення сигналу  $D$  при різних параметрах впливу завади а саме: ймовірності появи завадового імпульсу у будь-якому каналі виявляча  $\gamma$  та відношення дисперсії завади до дисперсії шуму  $b$ . Для порівняння ефективності обох типів виявлячів також проведений розрахунок їх втрат в необхідному пороговому відношенні сигнал – завада для забезпечення заданих ймовірностей правильного та хибного виявлення