ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»**

Институт компьютерных наук и технологий

Высшая школа интеллектуальных систем и суперкомпьютерных технологий

Дисциплина «Гибридные интеллектуальные системы и мягкие вычисления»

**ОТЧЕТ**

**Лабораторная работа №2**

на тему:

«Адаптивная нейро-нечеткая система оценки рисков информационной безопасности организации»

Выполнил:

студент группы 3540901/02001

Бараев Дамир Рашидович

«\_\_» \_\_\_\_\_\_\_\_\_\_ 2021г., \_\_\_\_\_\_\_\_\_\_

(подпись)

(подпись)

Проверила:

Бендерская Елена Николаевна

«\_\_» \_\_\_\_\_\_\_\_\_\_ 2021г., \_\_\_\_\_\_\_\_\_\_

Санкт-Петербург 2021

Оглавление

[1. Постановка задачи, связанной с рассматриваемой системы 3](#_Toc68133072)

[2. Описание теоретической базы рассматриваемой системы. 3](#_Toc68133073)

[2.1. Нечеткая логика 3](#_Toc68133074)

[2.2. Базовая архитектура нечеткой логической системы 6](#_Toc68133075)

[2.3. Адаптивная нейро-нечеткая система вывода (ANFIS) 7](#_Toc68133080)

[3. Моделирование алгоритма ANFIS в среде MatLab 7](#_Toc68133081)

[3.1. Метод быстрейшего спуска 11](#_Toc68133082)

[3.2. Гибридный метод 12](#_Toc68133083)

[4. Вывод 14](#_Toc68133084)

[5. СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 15](#_Toc68133085)

Постановка задачи, связанной с рассматриваемой системы

В статье обосновывается важность применения оценки рисков при реализации системы обеспечения информационной безопасности. Рассматриваются наиболее распространенные методики оценки риска и предлагается использовать для этих целей теорию нечеткой логики. Рассматриваются наиболее распространенные методы оптимизации параметров нечетких моделей и обосновываются преимущества применения методов, основанных на использовании нейро-нечетких сетей (ННС). Описывается процесс преобразования элементов нечеткой модели, таких как блок фаззификации, блок базы правил и блок дефаззификации во фрагменты нейронной сети. Результатом данного процесса является нейро-нечеткая сеть, соответствующая нечеткой модели.

В статье представлен контроль хаотической цепочки с помощью искусственной нейронной сети (ANN). Контроль и синхронизация двух одинаковых хаотических цепочек поставок, которые имеют различные начальные условия с использованием адаптивной системы нейро-нечеткого вывода (ANFIS). Контроллеры ANN и ANFIS проходят обучение в соответствии с моделью. Тем самым Преимущества классических и интеллектуальных методов управления объединены.

Описание теоретической базы рассматриваемой системы.

* 1. Нечеткая логика

Нечёткая логика (англ. fuzzy logic) — раздел математики, являющийся обобщением классической логики и теории множеств, базирующийся на понятии нечёткого множества, впервые введённого Лотфи Заде в 1965 году как объекта с функцией принадлежности элемента к множеству, принимающей любые значения в интервале [0, 1], а не только 0 или 1.

Внедрение информационных технологий и вычислительных средств в производство и управление современными предприятиями является эффективным инструментом, способствующим повышению производительности труда. Однако ИТ-инфраструктура предприятия зачастую приобретает неструктурированный характер, что приводит к неконтролируемому росту уязвимостей и рисков информационной безопасности (ИБ) предприятия в целом. Информационная безопасность – это «защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб».

Предложенная нечеткая продукционная модель (НПМ) включает семь входных лингвистических переменных (рисунок 1), характеризующих факторы риска, четыре выходных лингвистических переменных (рисунок 2), характеризующих риски различных областей информационной безопасности, а также четыре базы правил (рисунок 3).

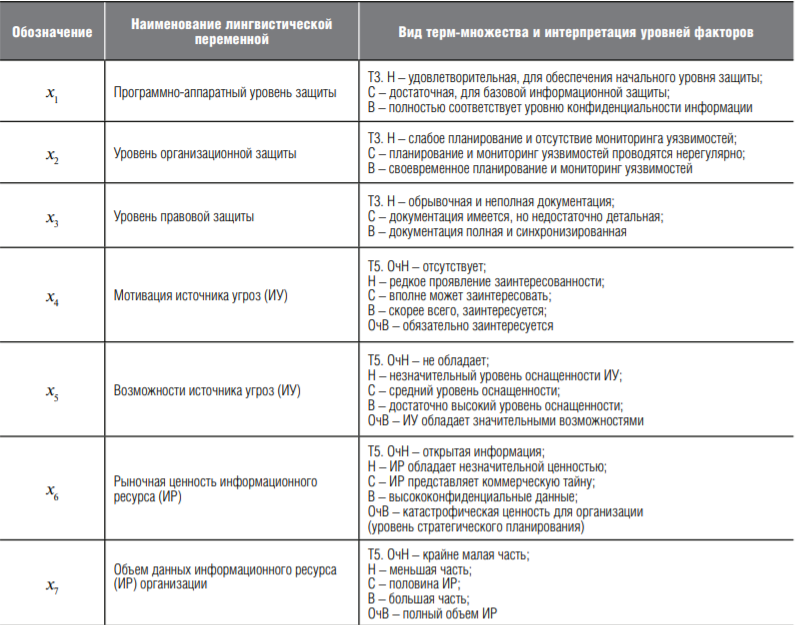


Рисунок 1 - Факторы риска информационной безопасности организации

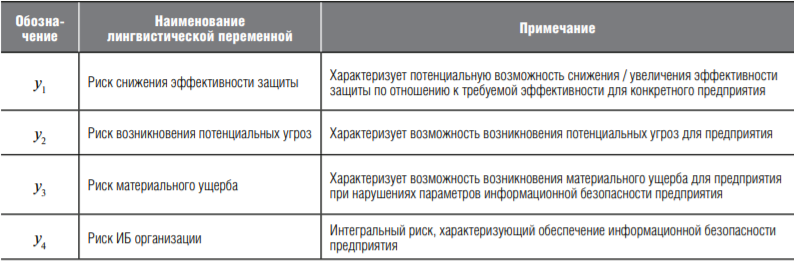


Рисунок 2 - Показатели риска информационной безопасности организации

Чтобы построить нечеткую модель, необходимо определить все ее эле менты: базу правил, число и тип функций принадлежности для каждой переменной модели, параметры функций принадлежности, логические операторы и т.п. Структура нечеткой продукционной модели оценки рисков ИБ организации приведена на рисунке 3.

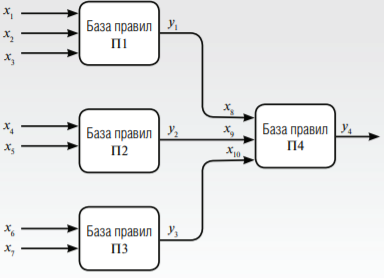


Рисунок 3 - Структура нечеткой продукционной модели

Построенная модель основана на экспертных знаниях о моделируемой системе обеспечения информационной безопасности (СОИБ). Получение информации о системе проводилось с привлечением эксперта предметной области, после чего выполнялось преобразование полученной информации в нечеткую модель. Такой метод является эффективным в том случае, если эксперт владеет всей полнотой знаний о СОИБ. На практике знания экспертов часто являются недостаточно полными и точными, а иногда даже содержат противоречия. Следовательно, необходимо, чтобы модель была основана на объективной информации о системе, в качестве которой могут выступать данные о результатах измерений значений входов и выходов системы. Данные обстоятельства предопределяют актуальность разработки нечеткой самонастраивающейся модели оценки рисков СОИБ. Под настройкой нечеткой модели, прежде всего, понимается процесс определения параметров функций принадлежности входных и выходных лингвистических переменных, при которых минимизируется ошибка выходов модели по отношению к наблюдаемой моделируемой системе. Для настройки модели, т.е. оптимизации ее параметров, чаще всего применяются следующие методы:

* методы, основанные на использовании нейронечетких сетей;
* поисковые методы;
* методы, основанные на кластеризации.

Методы первой группы связаны с преобразованием нечеткой модели в нейро-нечеткую сеть (ННС) и применением для настройки параметров модели методов обучения сети, основанных на измерениях входных и выходных данных системы. Методы второй группы представляют собой методы прямого поиска оптимальных параметров нечеткой модели. Процесс поиска может быть как упорядоченным, так и неупорядоченным (метод проб и ошибок). Наиболее часто используемым методом упорядоченного поиска является метод, основанный на применении генетических алгоритмов. Методы, основанные на кластеризации, сочетают настройку параметров модели и ее структуризацию. Они применяются для построения самоорганизующихся нечетких моделей, которые самостоятельно определяют свои существенные входные параметры, задают оптимальное число нечетких множеств для входных и выходных лингвистических переменных и устанавливают форму и число правил.

В настоящее время наиболее изученными являются методы первой группы, которые позволяют:

* обеспечить возможность оптимизации (настройки) параметров функций принадлежности лингвистических переменных на основе измерений входных и выходных зависимостей реальной системы;
* корректировать нечеткие модели, которые недостаточно точно сформированы экспертами;
* расширять формируемые экспертами нечеткие модели на области исследуемой системы, о которых знания экспертов ограничены.

Перечисленные особенности объясняют целесообразность применения методов, основанных на использовании нейро-нечетких сетей, для настройки нечеткой модели оценки рисков информационной безопасности организации.

* 1. Базовая архитектура нечеткой логической системы

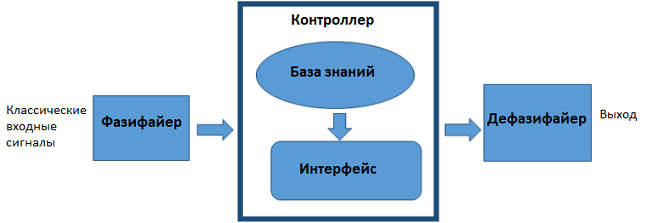
****

Рисунок 4 - Архитектура нечеткой логики

Фазифаер (Fuzzifier или оператор размытия) принимает измеренные переменные в качестве входных данных и преобразует числовые значения в лингвистические переменные. Он преобразует физические значения, а также сигналы ошибок в нормализованное нечеткое подмножество, которое состоит из интервала для диапазона входных значений и функций принадлежности, которые описывают вероятность состояния входных переменных. Входной сигнал в основном разделен на пять состояний, таких как: большой положительный, средний положительный, малый, средний отрицательный и большой отрицательный.

Контроллер состоит из базы правил и механизма вывода. База правил — это множество правил, где каждому подзаключению сопоставлен определенный весовой коэффициент. База правил хранит функции принадлежности и нечеткие правила, полученные путем знания работы системы в среде. Механизм вывода выполняет обработку полученных функций принадлежности и нечетких правил. Другими словами, механизм вывода формирует выходные данные на основе лингвистической информации.

Дефазифаер (Defuzzifier или оператор восстановления чёткости) выполняет обратный процесс фазифаера. Другими словами, он преобразует нечеткие значения в нормальные числовые или физические сигналы и отправляет их в физическую систему для управления работой системы.

Гибридная сеть архитектуры ANFIS может быть обучена с помощью алгоритма обратного распространения ошибки.

2. 3. Адаптивная нейро-нечеткая система вывода (ANFIS)

Адаптивная нейро-нечеткая система вывода (adaptive network-based fuzzy inference system), ANFIS — это искусственная нейронная сеть, основанная на нечеткой системе вывода Такаги-Сугено. Это универсальная интеллектуальная вычислительная методология, способная аппроксимировать любую реальную непрерывную функцию на компактном множестве с любой степенью точности.

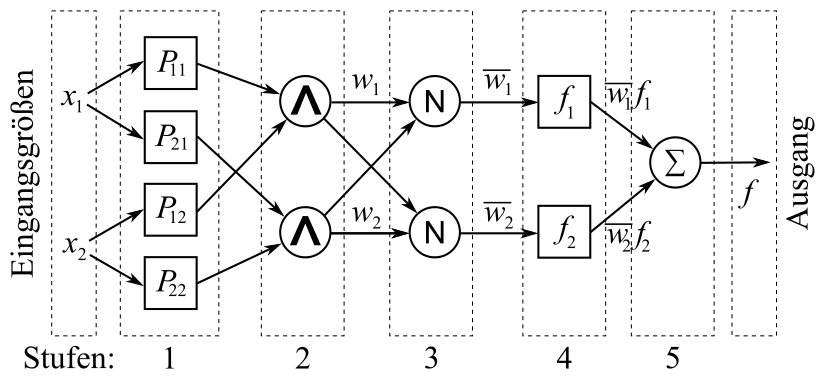


Рисунок 5 - Модель ANFIS

Обычно модель представляется пятью слоями. Нейроны 1-го слоя вычисляют функции принадлежности нечётких термов. Каждый нейрон слоя 2 вычисляет произведение входов. Выход нейрона представляет уровень активации правила. Слой 3 вычисляет нормированные уровни активации правил. Слой 4 вычисляет заключения правил. Слой 5 представлен единственным узлом, вычисляющим сумму своих аргументов. Вычисляется результат нечёткого вывода.

Моделирование алгоритма ANFIS в среде MatLab

Реализация алгоритма в MatLab осуществляется с помощью инструмента “Neuro-Fuzzy Designer”. Инструмент Neuro-Fuzzy Designer позволяет спроектировать, обучить и протестировать адаптивные нейронечеткие системы вывода (ANFIS) с помощью обучающих данных ввода/вывода.

Для моделирования нейронной сети был взят датасет цепочки поставок компонентов для компьютера. На основе входных данных я решил вычислять цену на продукцию с помощью ANFIS. Задача довольно тривиальная и может решаться с помощью не сложной формулы. Я решил провести моделирование для более простой задачи, потому что не было найдено подходящего датасета. Из датасета на вход я взял вид продукции, тип упаковок, вес, производителя, и путь доставки.

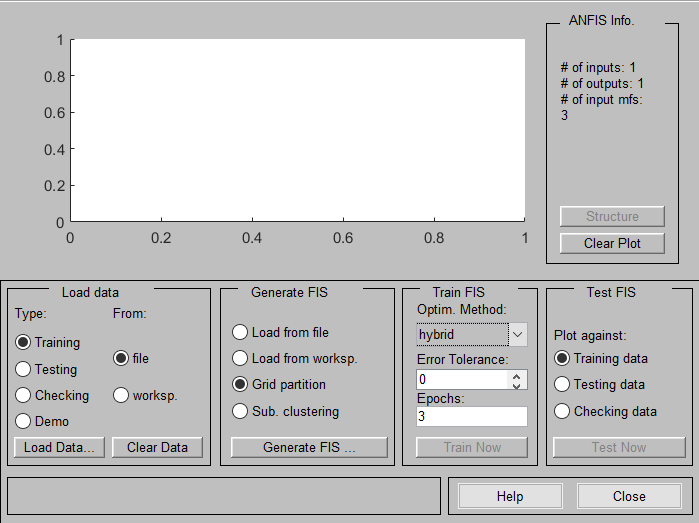


Рисунок 6 - Интерфейс Neuro-Fuzzy Designer

Первым делом нужно cгенерировать структуру FIS (Рис. 4). Генерируем модель с помощью разделения сетки (Grid partition).

* В разделе Input, в Number of MFs, задают количество входных функций принадлежности.
* В MF Type выбирается входной тип функции принадлежности.
* В разделе Output, в MF Type, выбирается выходной тип функции принадлежности.

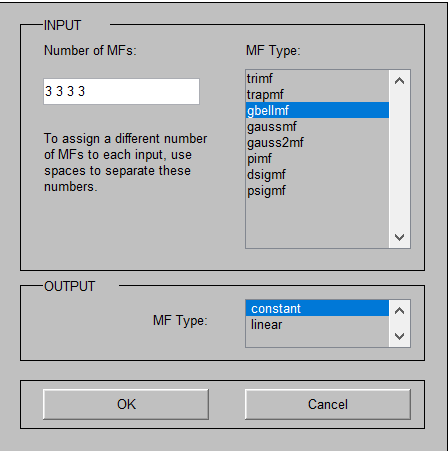


Рисунок 7 - Генерация структуры FIS

Для своих данных я попробовал все входные типы функции принадлежности.

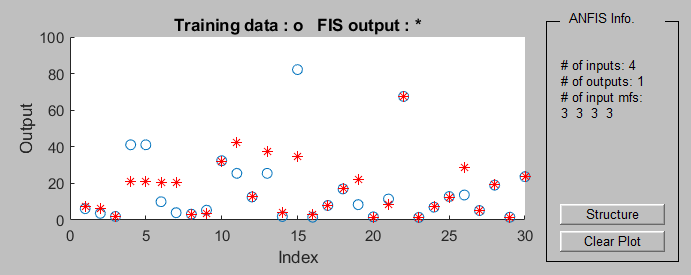


Рисунок 8 - Проверка данных. Тип функции принадлежности - trimf, количество эпох - 5

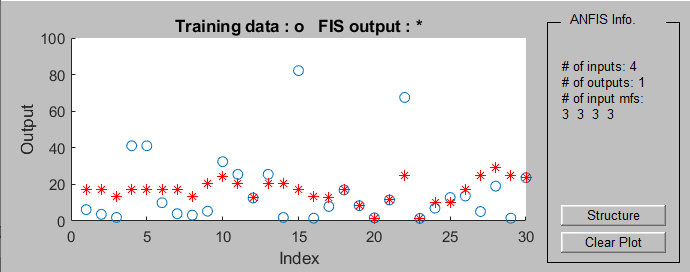


Рисунок 9 - Проверка данных. Тип функции принадлежности - trapmf, количество эпох – 5

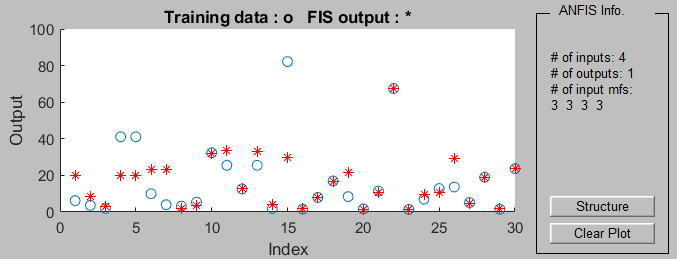


Рисунок 10 - Проверка данных. Тип функции принадлежности - gbellmf, количество эпох – 5

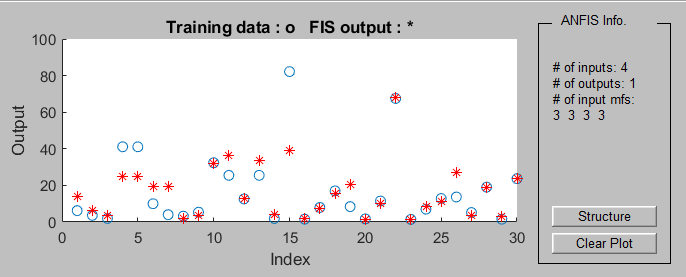


Рисунок 11 - Проверка данных. Тип функции принадлежности - gaussmf, количество эпох – 5

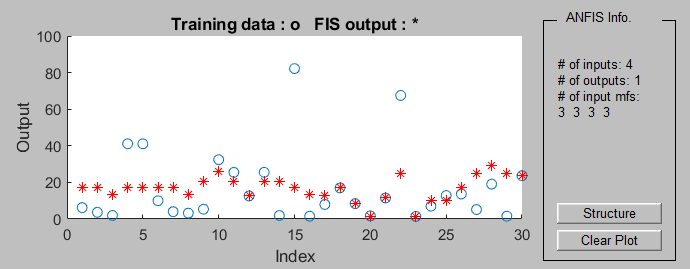


Рисунок 12 - Проверка данных. Тип функции принадлежности - pimf, количество эпох – 5

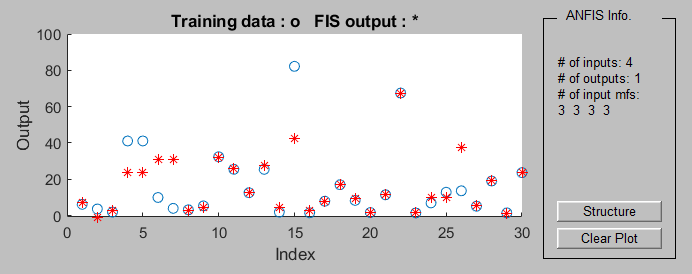


Рисунок 13 - Проверка данных. Тип функции принадлежности - dsigmf, количество эпох – 5

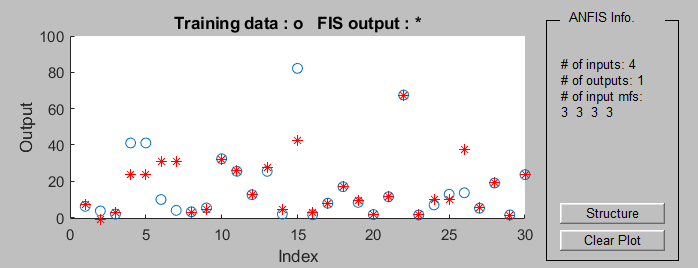


Рисунок 14 - Проверка данных. Тип функции принадлежности - psigmf, количество эпох – 5

Для обучения было выбрано 5 эпох. Результаты примерно везде одинаковые кроме функции принадлежности – pimf и trapmf.

Для дальнейших тестов выбрал функцию принадлежности – trimf. Т.к было больше совпадений чем при использование других функций принадлежности.

* 1. Метод быстрейшего спуска

Neuro-Fuzzy Designer позволяет настраивать метод оптимизации, номер учебных эпох и учебной ошибочной цели. Предлагается два метода оптимизации: Обратная связь для всех параметров (метод быстрейшего спуска), Гибридный метод, состоящий из обратной связи для параметров, сопоставленных с входными функциями принадлежности и оценкой методом наименьших квадратов для параметров, сопоставлен с выходными функциями принадлежности.

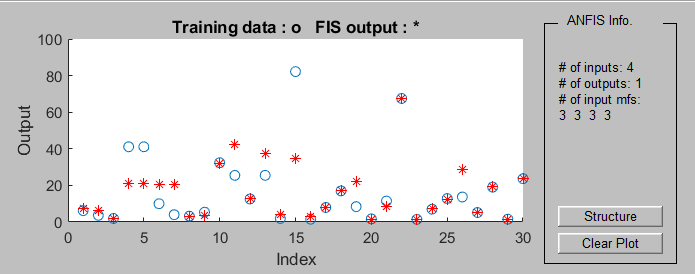


Рисунок 15 - Проверка данных. Метод быстрейшего спуска, количество эпох – 5

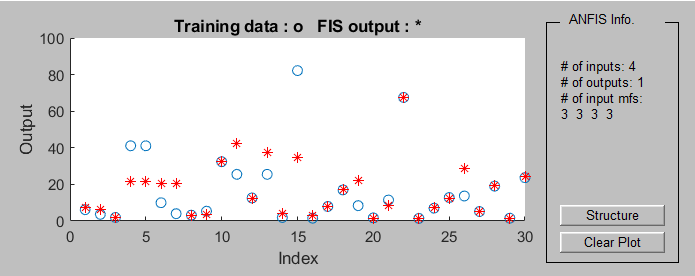


Рис. 13 Проверка данных. Метод быстрейшего спуска, количество эпох – 10

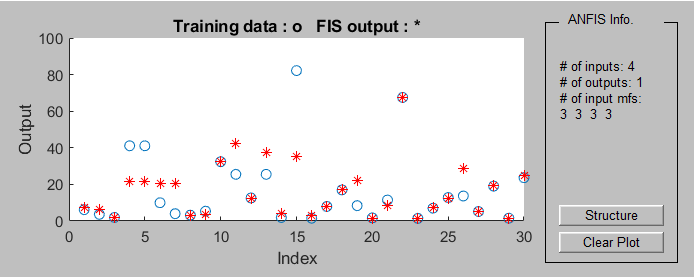


Рисунок 16 - Проверка данных. Метод быстрейшего спуска, количество эпох – 15

* 1. Гибридный метод

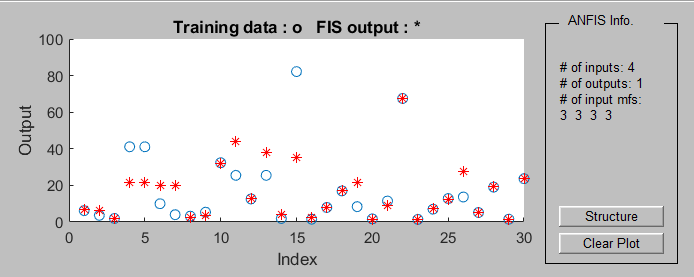


Рисунок 17 - Проверка данных. Гибридный метод, количество эпох – 5

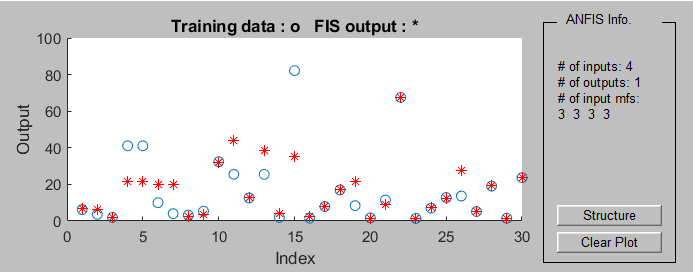


Рисунок 18 - Проверка данных. Гибридный метод, количество эпох – 10

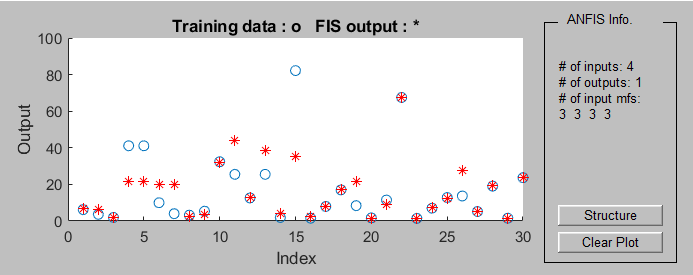


Рисунок 19 - Проверка данных. Гибридный метод, количество эпох – 15

Результат, при изменении количества эпох, изменяется не сильно.

При тестировании результатов я подставил входные данные те же на каких сеть обучалась.

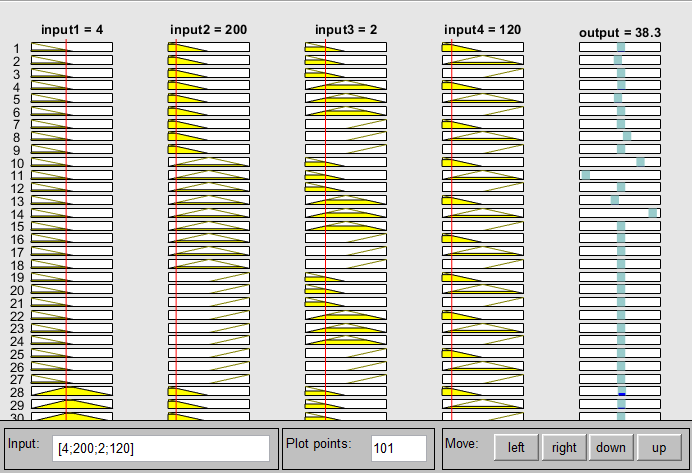


Рисунок 20 - Тестирование

Погрешность составила в среднем 12ед.

Вывод

В ходе работы была рассмотрена и протестирована нейронная сеть на основе системы нечеткого вывода. Модель нейронной сети является не сложной и может построится с помощью стандартных инструментов MatLab. Так же она легко настраиваемая и результаты её работы достаточно точны.

Я выделил несколько плюсов после изучения и использования ANFIS:

* Прост в реализации.
* Полезна при огромных входных данных.
* Универсальный оценщик.
* Более быстрая сходимость, чем у обычных нейронных сетей.
* Компактная модель.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. An adaptive neuro-fuzzy inference system for assessment of risks to an organization’s information security; Sergey Glushenko.

URL: https://www.researchgate.net/publication/318031809\_An\_adaptive\_neuro-fuzzy\_inference\_system\_for\_assessment\_of\_risks\_to\_an\_organization's\_information\_security

2. ANFIS - [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/ANFIS (дата обращения: 18.03.2021).

3. Что такое нечеткая логика (fuzzy logic): принцип работы, примеры, применение » Digitrode.ru - [Электронный ресурс]. URL: http://digitrode.ru/articles/1242-chto-takoe-nechetkaya-logika-fuzzy-logic-princip-raboty-primery-primenenie.html

(дата обращения: 18.03.2021).

4. Gershteyn Y., Perman L. Matlab: ANFIS Toolbox. – 2003.