Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(МОСКОВСКИЙ ПОЛИТЕХ)**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

**Отчет по проектной деятельности** «Моделирование нейро-нечеткой продукционной сети ANFIS для оценки риска ИБ предприятия»

Выполнил: студент 4 курса группы 171-361

Шестаков Павел Александрович

Куратор проекта: / ,

*подпись ФИО, должность*

Студент: / , /

*подпись ФИО, группа*

Москва 2021 г.

Содержание:

**Аннотация**

Управление информационной безопасностью, как циклический процесс, требующий постоянного проведения анализа состояний информационной системы, зачастую осложнен неполнотой и неточностью данных, получаемых в процессе сбора. При этом, процесс принятия управленческих решений на основе экспертных оценок зачастую малоэффективен ввиду своего субъективного характера.

В данной работе рассматривается вопрос моделирования системы поддержки принятия решений по управлению информационной безопасностью. Одним из возможных методов является компиляция теории нечетких множеств и многослойных нейронных сетей — нейро-нечеткие продукционные сети ANFIS.

**Участники и их роли.**

**1.** Студент группы 171-361, Шестаков П.А. Вклад участника: Анализ научной литературы по теме — 160 часов. Написание научной статьи по теме около 30 часов. Изучение возможностей MATLAB и моделирование ННС — 7 часов. Разработка сайта проекта — 4 часа. Написание отчёта по результатам проектной деятельности — 3 часа.

**Общее задание.**

Основной **целью** данной работы является моделирование нейро-нечеткой продукционной сети ANFIS для оценки рисков ИБ предприятия.

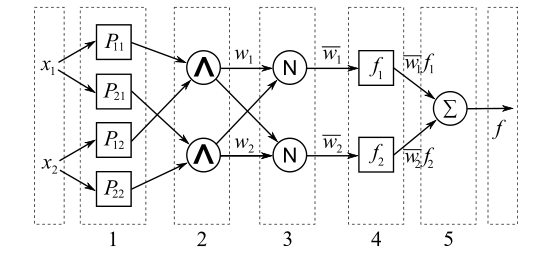
Оценка рисков, как один из элементов управления ИБ, часто основана на экспертном мнении или рассчитана помощью того или иного математического аппарата, позволяет обнаружить наиболее уязвимые информационные активы предприятия и спрогнозировать последствия реализации угроз в отношении этих информационных активов. Однако, экспертная оценка, на мой взгляд, является слабым звеном в системе управления ИБ из-за субъективности и следующей из неё малоэффективности, а используемые в процессе управления ИБ математические модели и алгоритмы в основном основаны на теории вероятностей, которая оперирует точными числовыми значениями, которые не всегда можно вычислить или получить.

Применение теории нечетких множеств позволяет манипулировать неточными и многозначными лингвистическими переменными, определяя степень их принадлежности к тому или иному нечеткому множеству с помощью функций принадлежности.

Сформированные на основе теории нечетких множеств нечеткие регуляторы имеют применение во множестве сфер, от видео- и фототехники до систем контроля очистных сооружений, благодаря преимуществам в адаптации, масштабируемости, гибкости и саморегулировании систем управления.

Построение разработанной нейро-нечеткой сети проводится на основе системы нейро-нечеткого вывода ANFIS (adaptive neuro-fuzzy inference system), посредством применения специализированного пакета Neuro-Fuzzy Designer программного средства MATLAB.

ANFIS представляет собой нейронную сеть с несколькими входами и одним выходом, которые, в свою очередь, являются нечеткими лингвистическими переменными. При этом термы входных и выходных лингвистических переменных описываются функциями принадлежности. Примерную схему этой сети можно увидеть на рисунке ниже.

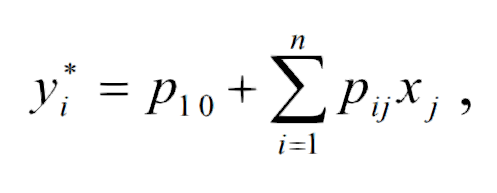


**Теоретическая модель нейро-нечеткой сети.**

Рассмотрим вариант реализации сети Anfis с применением алгоритма нечеткого вывода Сугено-Такаги. В модели вывода Сугено-Такаги используется набор правил:

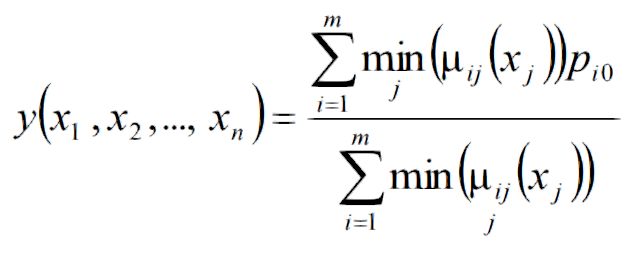
Ri : ЕСЛИ x1 это Ai1, ...И xn это Ain, ТО y = f(x),  
где X = (x1, x2, x3, ..., xn),  
f(x) — некоторая четкая функция, например, полином первого порядка.

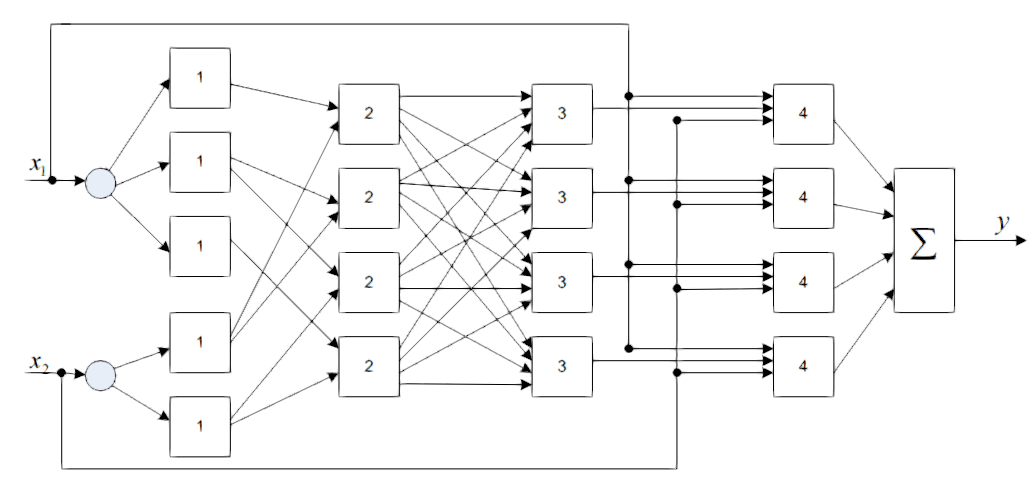
Определяются уровни "отсечения" ai для левой части каждого из правил согласно выражению ai = minj(Aij(xj)), i = 1, ..., m, j = 1, ..., n и рассчитываются "индивидуальные" выходы правил Ri, i = 1, ..., m:



где pi0, pij – коэффициенты полинома или цифровые веса, которые уточняются в процессе анализа данных.

Блок дефаззификации осуществляет переход от нечеткого значения лингвистической переменной (управление) к числовому значению. В случае упрощенного алгоритма нечеткого вывода (алгоритм Сугено нулевого порядка), когда yi = f(X) = pi0, i = 1, ..., m следует



На следующем рисунке изображена сеть ANFIS с двумя входными лингвистическими переменными и четырьмя нечеткими правилами.  


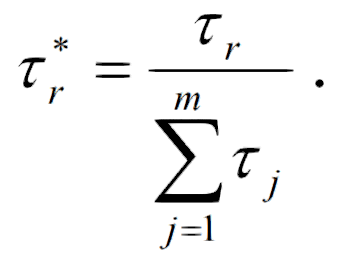
Разберем подробнее сеть ANFIS по слоям.

**Слой 1.** Входы сети соединены только со своими термами. Количество узлов первого слоя равно сумме мощностей терм-множеств входных переменных, где операция фаззификации выполнена на синглетонной базе.

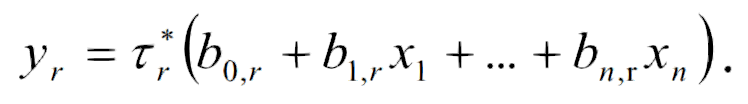
**Слой 2.** Количество узлов второго слоя m. Каждый узел этого слоя соответствует одному нечеткому предиктивному правилу.

Узел второго слоя соединен с теми узлами первого слоя, которые формирует посылки соответствующего правила. Следовательно, каждый узел второго слоя может принимать от 1 до n сигналов. Выходом узла является степень выполнения правила, которая рассчитывается как произведение входных сигналов (по Ларсену). Обозначим выходы узлов этого слоя τr, r = 1, ..., m̅, где m̅ — количество нечетких правил.

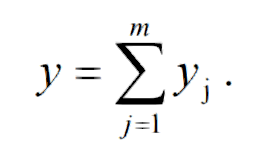
**Слой 3.** Количество узлов третьего слоя равно m̅. Каждый узел этого слоя рассчитывает относительную степень выполнения нечеткого правила (нормализация) по формуле



**Слой 4.** Количество узлов слоя также равно m. Каждый узел соединен с одним из узлов третьего слоя, а также со всеми входами сети. Узел четвертого слоя рассчитывает вклад одного нечеткого правила в выход сети по формуле



**Слой 5.** Единственный узел этого слоя суммирует вклады всех правил.



Настройка сети ANFIS с двумя входными лингвистическими переменными и четырьмя нечеткими правилами выполняется комбинацией градиентного спуска в виде алгоритмов обратного распространения ошибки и метода наименьших квадратов (хотя допустимо использовать только метод обратного распространения ошибки).

Алгоритм ОРО настраивает параметры антецедентов (предпосылок), т.е. функций принадлежности фаззификатора. МНК оценивает коэффициенты заключения правил, так как они линейно связаны с выходом сети. Каждая итерация процедуры настройки выполняется в два этапа

На первом этапе на входы подается обучающая выборка и по невязке между желаемым и действительным поведением сети МНК находятся оптимальные параметры узлов четвертого слоя. На втором этапе остаточная невязка передается с выхода сети на входы и методом ОРО модифицируются параметры узлов первого слоя. При этом найденные на предыдущем этапе коэффициенты заключения правил не изменяются. Итерационная процедура настройки продолжается, пока невязка превышает заранее установленное значение. Для настройки функций принадлежности фаззификатора, кроме метода ОРО, могут использоваться и другие алгоритмы оптимизации.

**Результат работы.**

Построение разработанной нейро-нечеткой сети проводится на основе системы нейро-нечеткого вывода ANFIS (adaptive neuro-fuzzy inference system), посредством применения специализированного пакета Neuro-Fuzzy Designer программного средства MATLAB. ANFIS представляет собой нейронную сеть с несколькими входами и одним выходом, которые, в свою очередь, являются нечеткими лингвистическими переменными. При этом термы входных и выходных лингвистических переменных описываются функциями принадлежности.

Трансформация модуля нечеткого вывода в нейро-нечеткую сеть выполняется с помощью поочередного преобразования блока фаззификации, базы правил и блока дефаззификации во фрагменты нейро-нечеткой сети. Обучение нейро-нечеткой сети предполагает наличие обучающей выборки, представляющей собой вектор из точных значений входных и выходной лингвистических переменных.

При определении входных лингвистических переменных, соответствующих факторам риска информационной безопасности предприятия, могут быть использованы следующие терм-множества:

Т1 = {Низкий (Н); Средний (С); Высокий (В)},

Т2 = {Очень низкий (ОчН); Низкий (Н); Средний (С); Высокий (В); Очень высокий (ОчВ)}.

При определении входных лингвистических переменных, соответствующие показателям риска, могут быть использованы терм-множества:

Т3 = {Низкая очевидность риска (НОР); Средняя очевидность риска (CОР); Высокая очевидность риска (ВОР)};

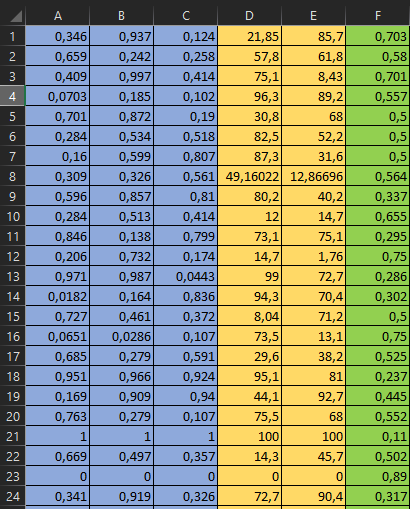
Т4 = {Очень низкая очевидность риска (ОчНОР); Низкая очевидность риска (НОР); Средняя очевидность риска (СОР); Высокая очевидность риска (ВОР); Очень высокая очевидность риска (ОчВОР)}.

| **Переменная** | **Наименование лингвистической переменной** | **Терм-множество** |
| --- | --- | --- |
| x1 | Программно-аппаратный уровень защиты | Т1 = {Н, С, В} |
| x2 | Уровень организационной защиты | Т1 = {Н, С, В} |
| x3 | Уровень правовой защиты | Т1 = {Н, С, В} |
| x4 | Мотивация источника угроз | Т2 = {ОчН, Н, С, В, ОчВ} |
| x5 | Возможности источника угроз | Т2 = {ОчН, Н, С, В, ОчВ} |

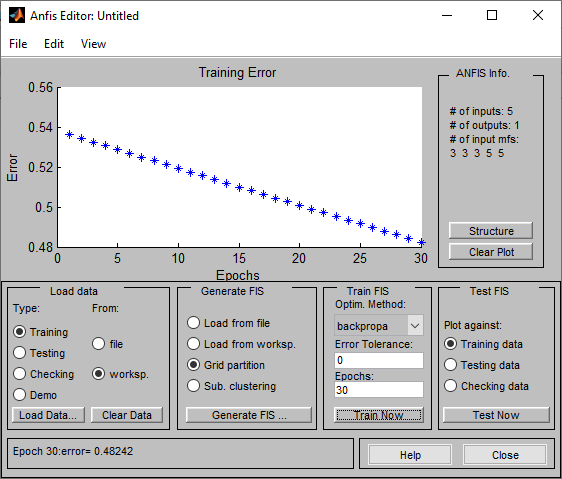
| **Переменная** | **Наименование лингвистической переменной** | **Терм-множество** |
| --- | --- | --- |
| y1 | Риск снижения эффективности защиты | Т3 = {НОР; СОР; ВОР} |
| y2 | Риск возникновения потенциальных угроз | Т4 = {ОчНОР; НОР; СОР; ВОР; ОчВОР} |
| y3 | Риск ИБ организации | Т4 = {ОчНОР; НОР; СОР; ВОР; ОчВОР} |

Обучение нейро-нечеткой сети было выполнено на основе обучающей выборки, содержащей 118 наборов, представляющих собой вектор значений факторов риска и значений уровня риска (входные и выходные лингвистические переменные, соответственно). Данные не были получены с помощью независимой экспертной оценки и, ввиду своей субъективности, несут показательный характер. При обучении нейро-нечеткой сети использовался метод обратного распространения ошибки.

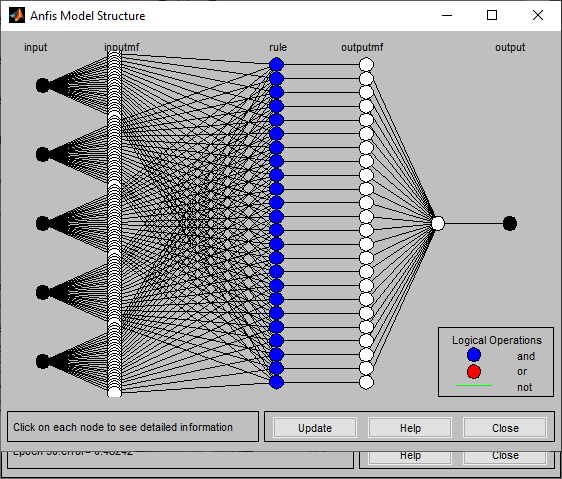
*Фрагмент обучающей выборки.*



*Процесс обучения нейро-нечеткой сети методом обратного распространения ошибки.*



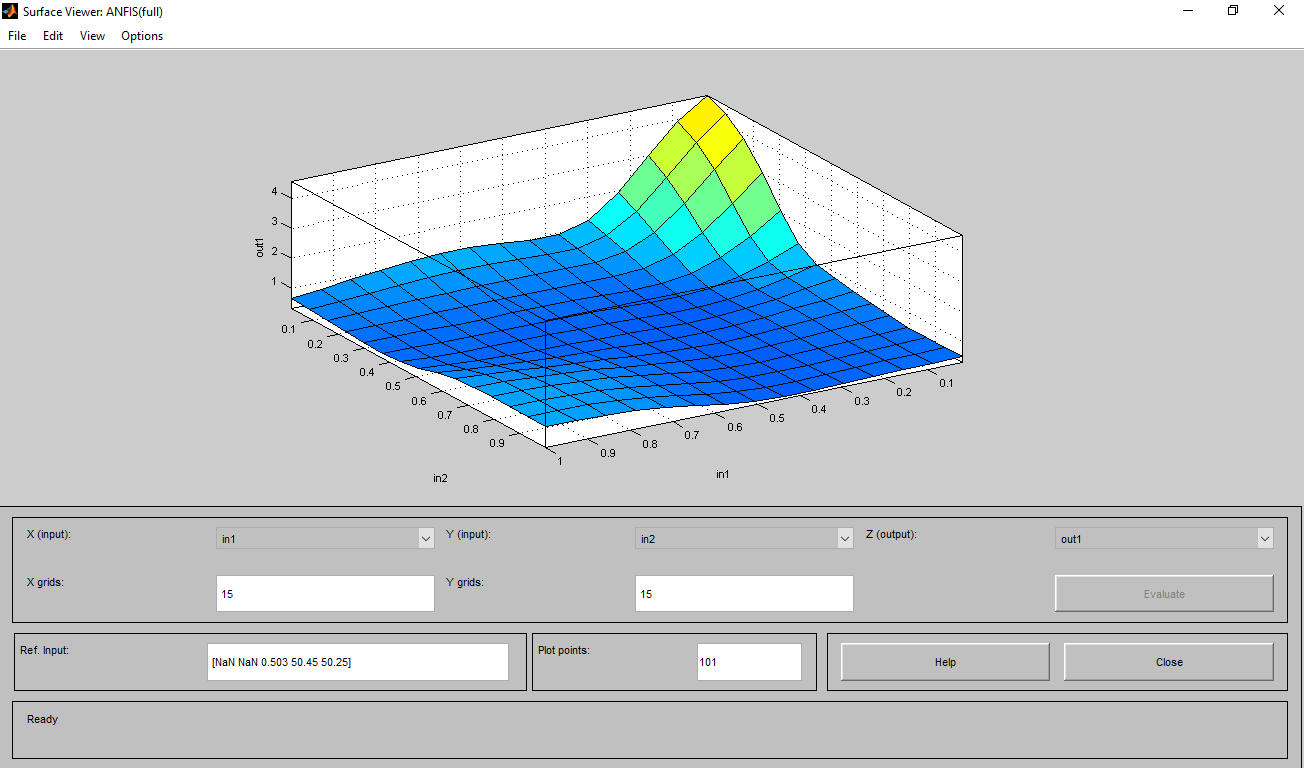
В процессе моделирования была сформирована нейро-нечеткая сеть со следующей структурой



В результате моделирования были сформированы следующие нечеткие правила, представленные в виде функций принадлежности входных и выходной лингвистических переменных.



На рисунке ниже представлена поверхность нейро-нечеткой сети, показывающая зависимость выходной переменной y3 от входных переменных x1 и x2.



**Заключение**

Предложенная нечеткая нейронная продукционная сеть в качестве модели системы поддержки принятия решения, на мой взгляд, позволяет сформировать более объективный подход к управлению ИБ, чем подход, основанный на экспертной оценке, благодаря высокой масштабируемости и гибкости системы, заключающейся в индивидуальном подборе параметров к любой интересующей ситуации.