ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»

Адаптивная нейро-нечеткая система оценки рисков информационной безопасности организации

Выполнил:
Студент группы 3540901/02001 Бараев Д.Р.

Руководитель:
Доцент К.Т.Н. Бендерская Е.Н.

POLYTECH
Peter the Great St.Petersburg Polytechnic University

Постановка задачи

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.

POLYTECH
Peter the Great St.Petersburg Polytechnic University

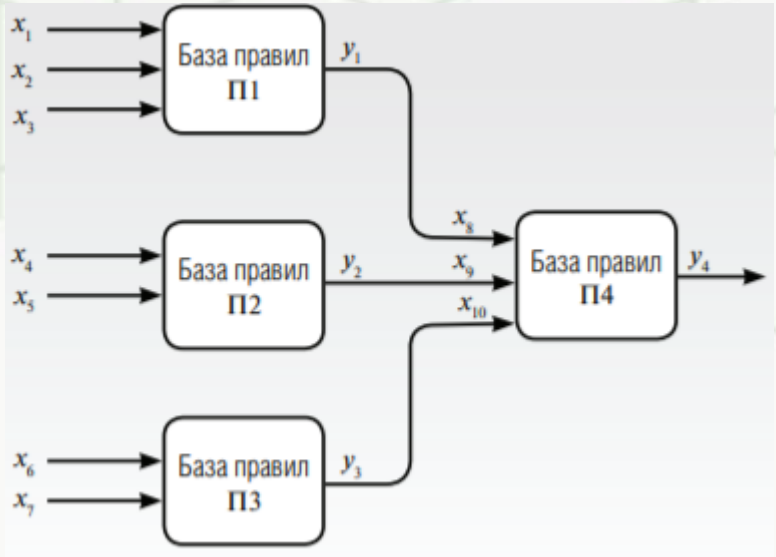
Постановка задачи

Обозначение	Наименование лингвистической переменной	Вид терм-множества и интерпретация уровней факторов
x_1	Программно-аппаратный уровень защиты	Т3. Н – удовлетворительная, для обеспечения начального уровня защиты; С – достаточная, для базовой информационной защиты; В – полностью соответствует уровню конфиденциальности информации
x_2	Уровень организационной защиты	Т3. Н – слабое планирование и отсутствие мониторинга уязвимостей; С – планирование и мониторинг уязвимостей проводятся нерегулярно; В – своевременное планирование и мониторинг уязвимостей
x_3	Уровень правовой защиты	Т3. Н – обрывочная и неполная документация; С – документация имеется, но недостаточно детальная; В – документация полная и синхронизированная
x_4	Мотивация источника угроз (ИУ)	Т5. ОчН – отсутствует; Н – редкое проявление заинтересованности; С – вполне может заинтересовать; В – скорее всего, заинтересуется; ОчВ – обязательно заинтересуется
x_5	Возможности источника угроз (ИУ)	Т5. ОчН – не обладает; Н – незначительный уровень оснащенности ИУ; С – средний уровень оснащенности; В – достаточно высокий уровень оснащенности; ОчВ – ИУ обладает значительными возможностями
x_6	Рыночная ценность информационного ресурса (ИР)	Т5. ОчН – открытая информация; Н – ИР обладает незначительной ценностью; С – ИР представляет коммерческую тайну; В – высококонфиденциальные данные; ОчВ – катастрофическая ценность для организации (уровень стратегического планирования)
x_7	Объем данных информационного ресурса (ИР) организации	Т5. ОчН – крайне малая часть; Н – меньшая часть; С – половина ИР; В – большая часть; ОчВ – полный объем ИР

Факторы риска информационной безопасности организации

Обозначение	Наименование лингвистической переменной	Примечание
y_1	Риск снижения эффективности защиты	Характеризует потенциальную возможность снижения / увеличения эффективности защиты по отношению к требуемой эффективности для конкретного предприятия
y_2	Риск возникновения потенциальных угроз	Характеризует возможность возникновения потенциальных угроз для предприятия
y_3	Риск материального ущерба	Характеризует возможность возникновения материального ущерба для предприятия при нарушениях параметров информационной безопасности предприятия
y_4	Риск ИБ организации	Интегральный риск, характеризующий обеспечение информационной безопасности предприятия

Показатели риска информационной безопасности организации



Структура нечеткой продукционной модели

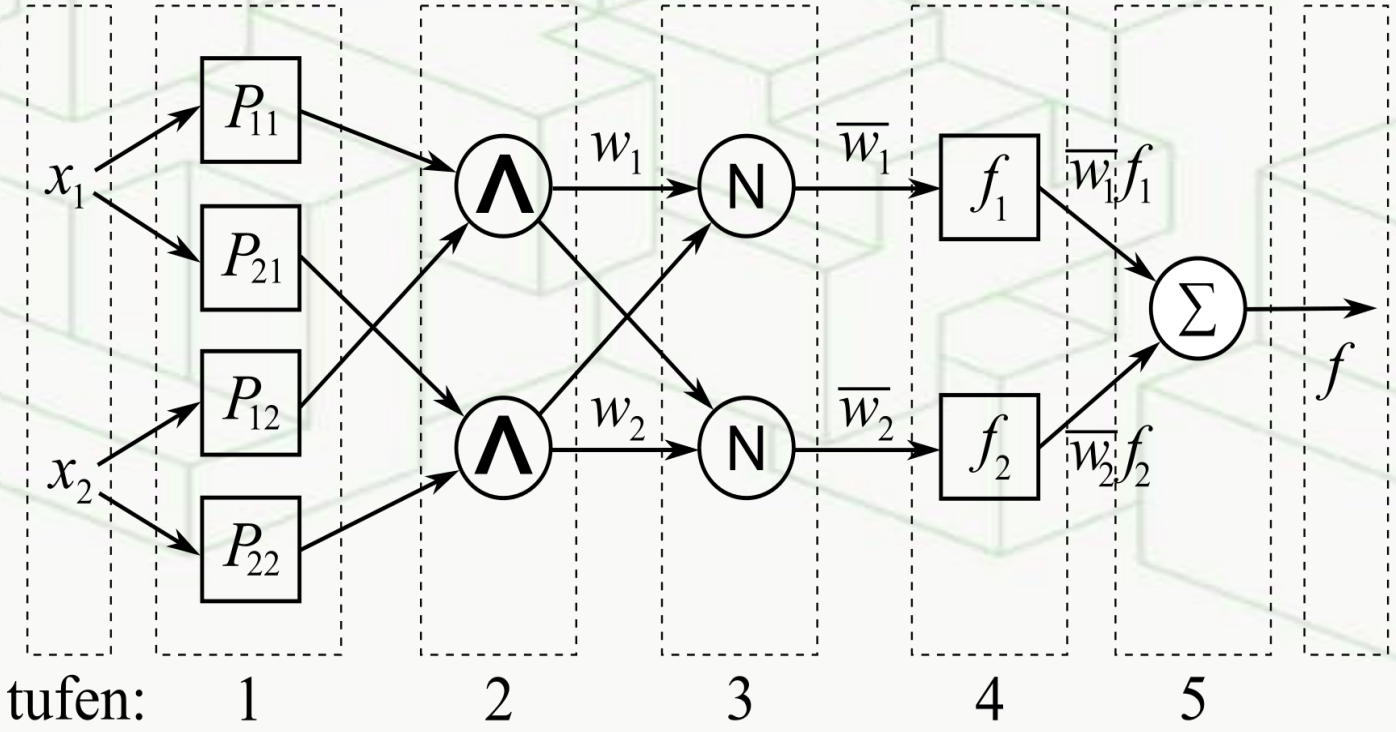
Базовая архитектура нечеткой логической системы

POLYTECH
Peter the Great St.Petersburg Polytechnic University

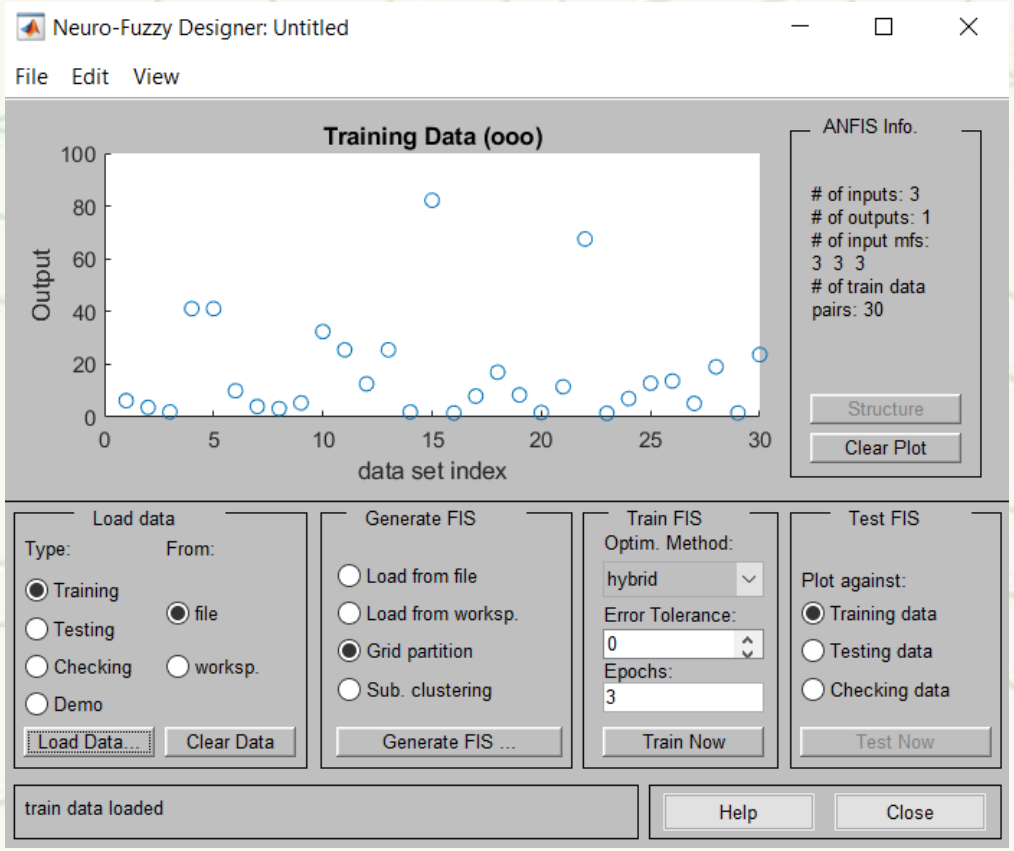
Модель ANFIS

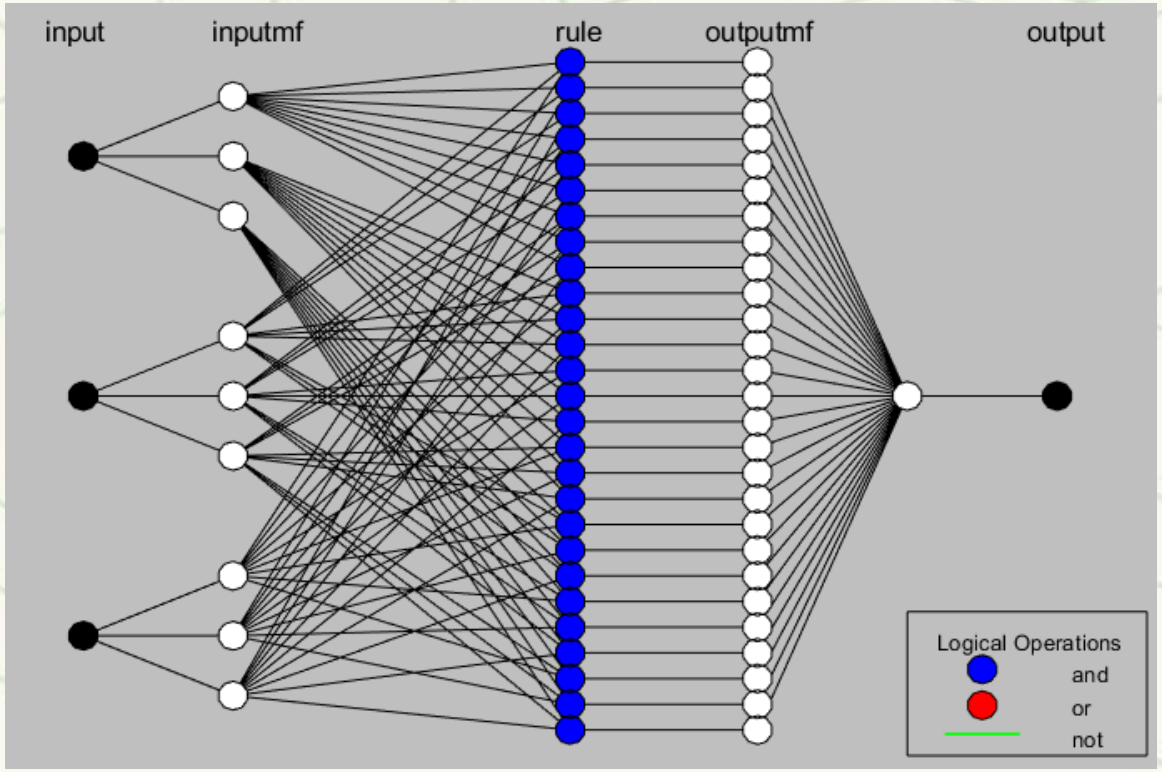
- ANFIS считается универсальным оценщиком
- Вывод такой системы соответствует набору нечетких правил «если-то» (if-then)

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



Построение ANFIS в MatLab





Проверка результатов

Входные данные из обучающей выборки

Экспериментальные данные

POLYTECH
Peter the Great St.Petersburg Polytechnic University

Выводы

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.