электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056

Разработка нейронечёткой сети для анализа информационных рисков

***Миков Д.А.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Булдакова Т.И., д.т.н, профессор
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
v.a.matveev@bmstu.ru

В последнее время в анализе рисков информационной безопасности всё большую распространённость получают системы с элементами искусственного интеллекта - нечёткие модели и нейронные сети.

Основное преимущество нечётких моделей по сравнению с традиционными математическими моделями связано с возможностью использования для их разработки значительно меньших объёмов информации о системе, при этом информация может носить приближённый, нечёткий характер, что является особенно эффективным для такого важного, многофакторного и сложного процесса как анализ информационных рисков [1].

Основу нечётких моделей составляет система правил, которая обычно формируется на базе экспертных знаний об информационной системе. Указанный метод называется приобретением знаний и является эффективным в том случае, если эксперт полностью обладает знаниями о системе и может выразить эти знания в словесной форме и передать их. В случае с информационными рисками знания эксперта часто являются неполными, неточными, слабо поддающимися формулированию и могут даже содержать в себе противоречия. Кроме того, эти знания субъективны, то есть мнения отдельных людей о функционировании одной и той же информационной системы могут различаться. С учётом всего сказанного, представляется целесообразным, чтобы в основе модели лежала объективная информация о системе. Такой информацией являются результаты измерения значений её входов и выходов.

Процесс приобретения знаний на основе этих данных называется извлечением знаний. Подобной возможностью обладают искусственные нейронные сети. Но основным недостатком нейронных сетей при использовании для анализа информационных рисков

является то, что их параметры не несут никакой информации, кроме числовой, и содержащиеся в них знания недоступны для интерпретации человеком – подобную сеть можно назвать сетью типа «чёрный ящик».

Данные недостатки позволяет обойти объединение возможностей нечёткого моделирования и нейронных сетей – так называемые нейронечёткие сети (ННС). ННС представляет собой особую эквивалентную форму нечёткой модели. Настройка данной сети может быть произведена на основе выборки измерений входных и выходного параметров моделируемой системы, с использованием метода обратного распространения ошибки или других методов, применяемых для нейронных сетей. Растущий интерес к ННС обусловлен следующими их неоспоримыми преимуществами по сравнению с обычными нечёткими моделями:

1) ННС обеспечивают возможность оптимизации (настройки) параметров нечётких моделей на основе данных измерения входов и выходов реальных систем;

2) ННС позволяют корректировать недостаточно точные нечёткие модели, формируемые экспертами;

3) ННС дают возможность расширения формируемых экспертами нечётких моделей на те области пространства входов, экспертные знания о которых отсутствуют.

По сравнению с обычными искусственными нейронными сетями ННС также обладают рядом существенных преимуществ:

1) структура и параметры ННС (множества типа «большой» и «малый», лингвистические правила) являются понятными человеку, а также допускают обобщение знаний, содержащихся в зашумлённых измеряемых данных о моделируемой системе, и представление их в форме хорошо интерпретируемых лингвистических правил;

2) при наличии предварительных или частичных знаний о моделируемой системе их легко можно отразить в ННС (в нейронных сетях это сделать крайне сложно);

3) в случае ННС определение структуры сети представляет собой значительно более простую задачу, чем в случае нейронных сетей, где обычно используется метод проб и ошибок [2].

Чтобы разработать и использовать ННС для анализа рисков информационной безопасности, необходимо определить, какие данные следует подавать на вход системы. Из определения риска информационной безопасности следует, что величина риска $\boldsymbol{R}$ есть функция от угрозы информационной безопасности $\boldsymbol{T}$, потенциально возможного ущерба (стоимости информации, ресурса, актива) $\boldsymbol{A}$ и уязвимости информационной системы $\boldsymbol{V}$:

$$R = f\,(T, A, V)$$

Поэтому входными данными будут служить значения 3 нечётких переменных на отрезке [0, 1], описанные лингвистическим терм-множеством (очень низкий, низкий, средний, высокий, очень высокий):

1) угроза;

2) ущерб;

3) уязвимость.

Уровни шкалы при оценке угроз, ущерба и уязвимостей приведены в таблице.

Уровни шкалы	Угрозы	Ущерб	Уязвимости
Очень низкий (от 0 до 0,2)	Событие практически никогда не происходит	Незначительные потери материальных средств и ресурсов, которые быстро восполняются, или незначительное влияние на репутацию	Уязвимость, которой можно пренебречь
Низкий (от 0,2 до 0,4)	Событие случается редко	Более заметные потери материальных активов, более существенное влияние на репутацию или ущемление интересов	Незначительная уязвимость, которую легко устранить
Средний (от 0,4 до 0,6)	Событие вполне возможно при определённом стечении обстоятельств	Достаточные потери материальных активов или ресурсов или достаточный урон репутации и интересам	Умеренная уязвимость
Высокий (от 0,6 до 0,8)	Скорее всего, событие произойдёт при организации атаки	Значительный урон репутации и интересам, что может представлять угрозу для продолжения деятельности	Серьёзная уязвимость, ликвидация которой возможна, но связана со значительными затратами
Очень высокий (от 0,8 до 1)	Событие, вероятнее всего, произойдёт при организации атаки	Разрушительные последствия и невозможность ведения деятельности	Критическая уязвимость, которая ставит под сомнение возможность её устранения

В итоге на выходе системы по входным данным будет получена оценка уровня риска информационной безопасности на отрезке [0, 1], описанная расширенным лингвистическим терм-множеством (пренебрежимо низкий, очень низкий, низкий, ниже среднего, умеренный, выше среднего, высокий, очень высокий, критический).

Шкала измерения уровня информационных рисков будет выглядеть следующим образом:

1) пренебрежимо низкий (0) – риском можно пренебречь;

2) очень низкий (0,125) – если сведения расцениваются как очень низкий риск, необходимо определить, существует ли необходимость в корректирующих действиях, или есть возможность принять этот риск;

3) низкий (0,25) – уровень риска позволяет работать, но имеются предпосылки к нарушению нормальной работы;

4) ниже среднего (0,375) – необходимо разработать и применить план корректирующих действий в течение приемлемого периода времени;

5) умеренный (0,5) – уровень риска не позволяет стабильно работать, имеется настоятельная необходимость в корректирующих действиях, изменяющих режим работы в сторону уменьшения риска;

6) выше среднего (0,625) – система может продолжать работу, но корректирующий план действий необходимо применить как можно быстрее;

7) высокий (0,75) – уровень риска такой, что бизнес-процессы находятся в неустойчивом состоянии;

8) очень высокий (0,875) – необходимо незамедлительно принять меры по уменьшению риска;

9) критический (1) – уровень риска очень большой и является недопустимым для организации, что требует прекращения эксплуатации системы и принятия радикальных мер по уменьшению риска [3].

Обучение и функционирование ННС можно разбить на 8 этапов (рис. 1).

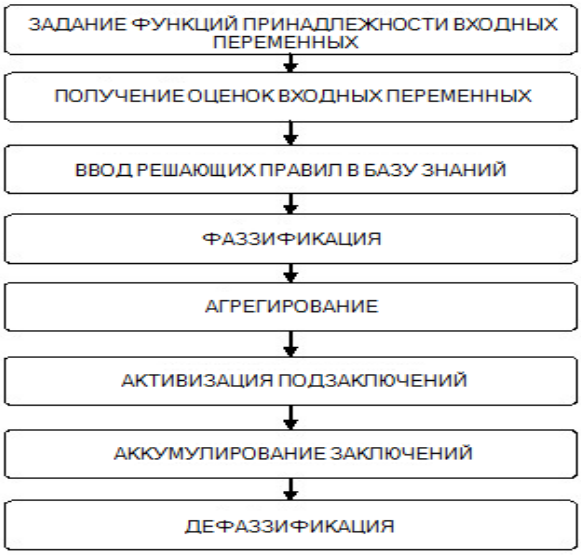

Рис. 1. Основные этапы обучения и функционирования нейронечёткой сети

Задание функций принадлежности входных переменных предполагает определение вида функций принадлежности для каждой из входных лингвистических переменных на оси возможных значений риска. Кроме этого, на данном этапе необходимо задать параметры выбранных функций принадлежности. Для выполнения этих процедур разработаны специализированные программы, графический интерфейс которых существенно облегчает работу на этом этапе.

Наиболее эффективным инструментом разработки является редактор FIS программного комплекса MATLAB. Редактор FIS обладает графическим интерфейсом и позволяет вызывать все другие редакторы и программы просмотра систем нечёткого вывода. Графический интерфейс редактора обладает максимальным удобством и гибкостью [4].

Для нечёткой модели анализа информационных рисков выбраны следующие параметры:

1) 3 входные (угроза, ущерб, уязвимость) и 1 выходная (риск) переменные;

2) тип системы нечёткого вывода – Сугено (для создания ННС);

3) And method (Метод логической конъюнкции) – prod (метод алгебраического произведения);

4) Or method (Метод логической дизъюнкции) – probor (метод алгебраической суммы);

5) Implication (Метод вывода заключения) – min (метод минимального значения);

6) Aggregation (Метод агрегирования) – max (метод максимального значения);

7) Defuzzification (Метод дефаззификации) – wtaver (метод взвешенного среднего).

Для 3 входных переменных (угроза, ущерб, уязвимость) выбрано 5 нечётких классов (очень низкий, низкий, средний, высокий, очень высокий) и трапецеидальная функция принадлежности (рис. 2).

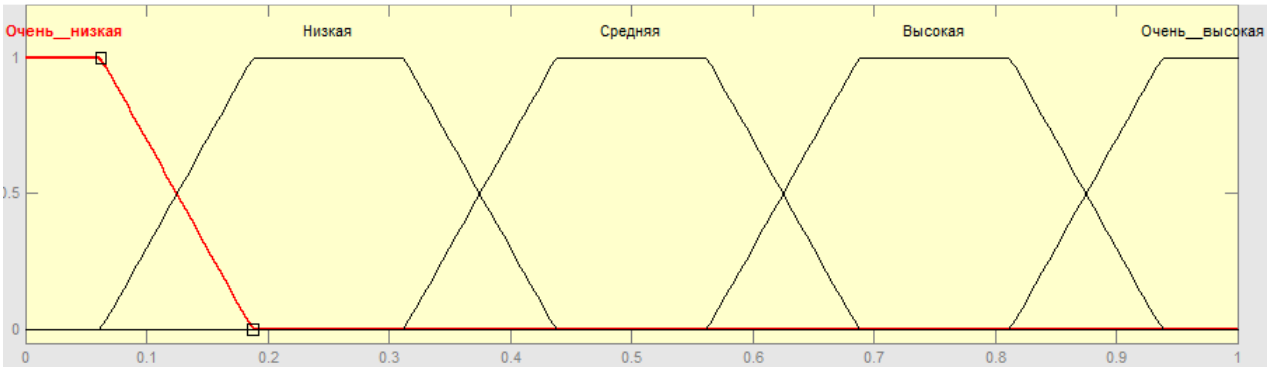

Рис. 2. Функция принадлежности входных переменных

Для выходной переменной (риск) выбрано 9 нечётких классов (пренебрежимо низкий, очень низкий, низкий, ниже среднего, умеренный, выше среднего, высокий, очень высокий, критический), которые в нечёткой системе типа Сугено принимают упомянутые выше фиксированные значения на отрезке [0,1], поэтому функция принадлежности для выходной переменной отсутствует.

Также нечёткая модель анализа информационных рисков содержит правила нечёткого вывода ЕСЛИ...ТО для связи входных и выходных данных (рис. 3).

1. If (Угроза is Очень__низкая) and (Ущерб is Очень__низкий) and (Уязвимость is Очень__низкая) then (Риск is Пренебрежимо__низкий) (1)
2. If (Угроза is Очень__низкая) and (Ущерб is Очень__низкий) and (Уязвимость is Низкая) then (Риск is Пренебрежимо__низкий) (1)
3. If (Угроза is Очень__низкая) and (Ущерб is Очень__низкий) and (Уязвимость is Средняя) then (Риск is Очень__низкий) (1)
4. If (Угроза is Очень__низкая) and (Ущерб is Очень__низкий) and (Уязвимость is Высокая) then (Риск is Низкий) (1)
5. If (Угроза is Очень__низкая) and (Ущерб is Очень__низкий) and (Уязвимость is Очень__высокая) then (Риск is Низкий) (1)
6. If (Угроза is Очень__низкая) and (Ущерб is Низкий) and (Уязвимость is Очень__низкая) then (Риск is Пренебрежимо__низкий) (1)
7. If (Угроза is Очень__низкая) and (Ущерб is Низкий) and (Уязвимость is Низкая) then (Риск is Очень__низкий) (1)
8. If (Угроза is Очень__низкая) and (Ущерб is Низкий) and (Уязвимость is Средняя) then (Риск is Низкий) (1)
9. If (Угроза is Очень__низкая) and (Ущерб is Низкий) and (Уязвимость is Высокая) then (Риск is Низкий) (1)
10. If (Угроза is Очень__низкая) and (Ущерб is Низкий) and (Уязвимость is Очень__высокая) then (Риск is Ниже__среднего) (1)
11. If (Угроза is Очень__низкая) and (Ущерб is Средний) and (Уязвимость is Очень__низкая) then (Риск is Очень__низкий) (1)
12. If (Угроза is Очень__низкая) and (Ущерб is Средний) and (Уязвимость is Низкая) then (Риск is Низкий) (1)
13. If (Угроза is Очень__низкая) and (Ущерб is Средний) and (Уязвимость is Средняя) then (Риск is Низкий) (1)
14. If (Угроза is Очень__низкая) and (Ущерб is Средний) and (Уязвимость is Высокая) then (Риск is Ниже__среднего) (1)
15. If (Угроза is Очень__низкая) and (Ущерб is Средний) and (Уязвимость is Очень__высокая) then (Риск is Умеренный) (1)
16. If (Угроза is Очень__низкая) and (Ущерб is Высокий) and (Уязвимость is Очень__низкая) then (Риск is Низкий) (1)

Рис. 3. Правила нечёткого вывода ЕСЛИ...ТО

Всего нечёткая модель должна содержать 125 таких правил для всех возможных сочетаний нечётких классов входных переменных.

Для создания гибридной сети необходимо предварительно создать обучающие данные, которые представляют собой числовую матрицу размерности $m \times (n+1)$, в которой количество строк m соответствует объёму выборки, первые n столбцов – значениям входных переменных модели, а последний столбец – значению выходной переменной. В случае с ННС для анализа информационных рисков количество столбцов равно 4, количество строк – 1331, в каждой из которых риск равен среднему арифметическому из значений угрозы, ущерба и уязвимости.

Перед обучением гибридной сети необходимо задать параметры обучения. Для создаваемой ННС выбран гибридный (hybrid) метод обучения, представляющий собой комбинацию метода наименьших квадратов и метода убывания обратного градиента. Количество циклов обучения (Epochs) – 1000.

Для исследования построенной модели гибридной сети используется программа просмотра правил. Для получения интересующего значения выходной переменной необходимо задать конкретные значения входных переменных аналогично общим рекомендациям систем нечёткого вывода. По умолчанию все входные переменные равны

0,5. При этом на графике функций принадлежности выходной переменной указано искомое значение риска – 0,495. В качестве иллюстрации работы ННС необходимо задать конкретные значения входных переменных. Например, если угроза – 0,68, ущерб – 0,74, уязвимость – 0,72, то риск – 0,745, что соответствует значению «высокий» по шкале уровней риска (рис. 4).

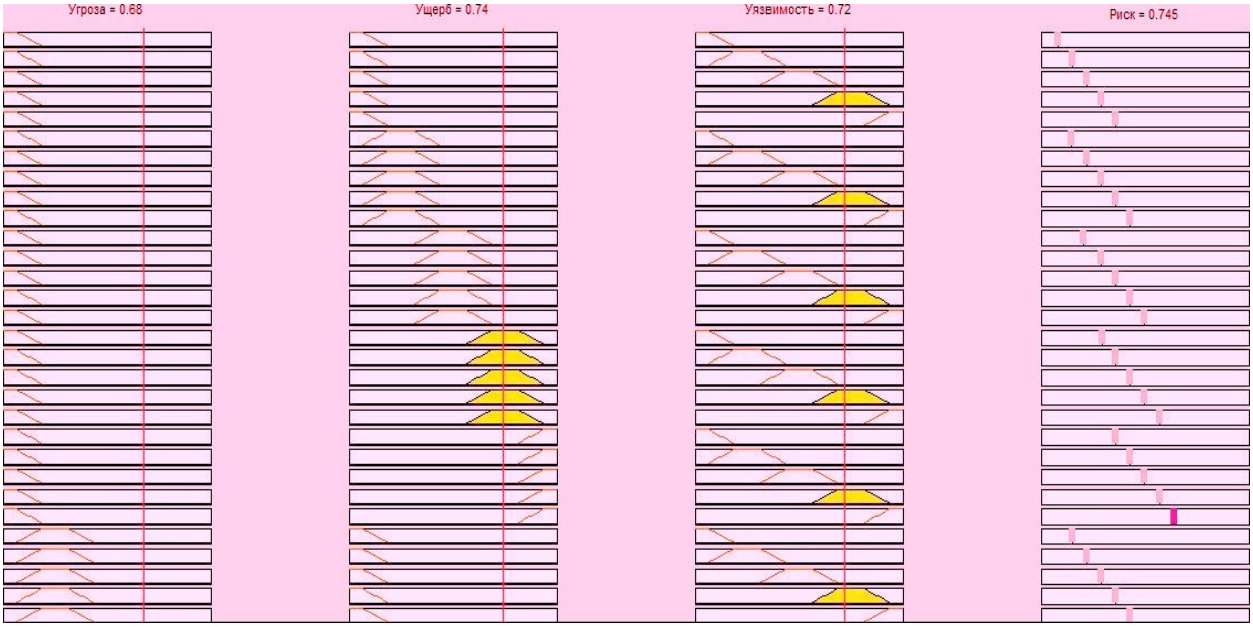

Рис. 4. Тестирование построенной и обученной нейронечёткой сети

Для оценки входных переменных следует использовать данные датчиков (например, системы обнаружения вторжений, антивирусы, межсетевые экраны) о потенциально опасной активности, общем уровне сетевой активности и нагрузки на тот или иной участок автоматизированной системы и т.д., а также экспертные оценки количественных показателей функционирования системы информационной безопасности.

Построенная ННС имеет гибкие настройки, удобна и проста в применении, а также точно и наглядно отображает зависимость уровня информационного риска от значений угроз информационной безопасности, потенциально возможного ущерба и уязвимостей информационной системы, для определения которых достаточно использовать оценки входных переменных на отрезке [0,1].

Список литературы

1. Булдакова Т.И., Миков Д.А. Анализ методов оценки информационных рисков // Безопасные информационные технологии: труды Всероссийской конференции. М.: Изд-во МГТУ им. Н.Э. Баумана, 2012. С. 120-122.

2. Круглов В.В., Дли М.И., Голунов Р.Ю. Нечёткая логика и искусственные нейронные сети. М.: Физматлит, 2001. 221 с.
3. Булдакова Т.И., Миков Д.А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 11. DOI: 10.7463/1113.0645489.
4. Леоненков А.В. Нечёткое моделирование в среде MATLAB и fuzzyTECH. СПб.: БХВ-Петербург, 2005. 736 с.