НАУЧНОЕ ИЗДАНИЕ МГТУ ИМ. Н. Э. БАУМАНА
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС77 - 48211. Государственная регистрация №0421200025. ISSN 1994-0408
электронный научно-технический журнал

Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели

 # 11, ноябрь 2013
DOI: 10.7463/1113.0645489

Булдакова Т. И., Миков Д. А.

УДК 004.056.53

Россия, МГТУ им. Н.Э. Баумана
buldakova@bmstu.ru
mikovda@yandex.ru

Введение

Общепринятым подходом к оценке работоспособности автоматизированных систем (АС) является моделирование, основанное на создании и исследовании моделей, описывающих функционирование этих систем. Применение подобных моделей позволяет проанализировать и оптимизировать процессы сбора, хранения и обработки информации, а также выбрать технологии защиты данных [1-3]. Математическая модель системы, отражая физическую суть ее процессов функционирования, позволяет адекватно оценить различные характеристики АС. Однако классические методы моделирования требуют подачи на вход модели чётких числовых значений.

Процесс анализа защищенности автоматизированных систем отличается тем, что при оценке информационных рисков в качестве исходных данных часто используются нечёткие значения в виде экспертных оценок. Это обусловливает необходимость применения нечётких моделей, основное преимущество которых связано с возможностью использования для их разработки значительно меньших объёмов информации о моделируемой системе, по сравнению с традиционными математическими моделями. При этом информация может носить приближённый, нечёткий характер, что является эффективным для такого сложного и неоднозначного процесса как оценка рисков в автоматизированных системах [4-6].

Целью данной работы является создание модели, позволяющей оценивать информационные риски в условиях неполных и неоднозначных данных об их составляющих и свойствах.

1 Выбор типа модели

Для разработки нечеткой модели, пригодной для оценки информационных рисков, необходимо проанализировать возможности существующих моделей, основанных на теории нечётких множеств.

Под нечётким множеством A, определённым на X, понимается совокупность $A = \{(x, \mu_A(x)) | x \in X\}$, где X – область значений, а $\mu_A(x)$ – функция принадлежности, характеризующая степень принадлежности элемента x нечёткому множеству A. При этом выделяют три случая:

1) $\mu_A(x) = 1$ - полная принадлежность элемента x к нечёткому множеству A, т.е. $x \in A$;

2) $\mu_A(x) = 0$ - отсутствие принадлежности элемента x к нечёткому множеству A, т.е. $x \notin A$;

3) $0 < \mu_A(x) < 1$ - частичная принадлежность элемента x к нечёткому множеству A.

Как правило, нечёткие модели разрабатываются для систем нечёткого управления, поэтому типичная структура состоит из 3 блоков [7, 8]:

1) блок фаззификации (занимается вычислением степени принадлежности чётких входных параметров модели входным нечётким множествам);

2) блок вывода (основным элементом является база правил – набор логических правил, которые задают причинно-следственные отношения между входными и выходными величинами);

3) блок дефаззификации (вычисление чёткого выходного значения на основе результирующей функции принадлежности, которая рассчитывается механизмом вывода в блоке вывода).

Различные типы нечетких моделей отличаются способом реализации указанных блоков.

В настоящее время наиболее часто используемым типом нечёткой модели является модель Мамдани [9]. В рамках метода Мамдани моделируемая система рассматривается как «чёрный ящик», характеризующийся недостаточностью информации о происходящих внутри него физических явлениях. Модель выполняет такое отображение входов (вектор X) в выход Y, которое обеспечивает как можно более точную аппроксимацию реальной системы (например, в смысле средней абсолютной погрешности). Указанное отображение предполагает существование некоторой геометрической поверхности (поверхности отображения) в пространстве, задаваемом декартовым произведением $X \times Y$. Модель Мамдани представляет собой множество правил:

ЕСЛИ (x есть A) ТО (y есть B),

где A, B – нечёткие множества. Каждое правило задаёт в указанном пространстве некоторую нечёткую точку. На основе множества нечётких точек формируется нечёткий график, механизм интерполяции между точками в котором зависит от используемого аппарата нечёткой логики.

Были разработаны и другие типы нечётких моделей, среди которых наиболее важными являются модели Такаги-Сугено-Канга (TSK-модели). От моделей Мамдани модели Такаги-Сугено-Канга отличаются формой правил [10, 11]. В случае TSK-модели правила имеют вид:

ЕСЛИ (x есть A) ТО ($y = f(x)$),

где вместо нечёткого множества заключение каждого правила содержит функцию $f(x)$, которая может быть нелинейной, хотя обычно используются линейные функции вида $y = ax + b$.

Поскольку в модели Такаги-Сугено-Канга получаемое заключение имеет более сложное математическое представление и обладает меньшей обозримостью, чем заключение в модели Мамдани, то для оценки информационных рисков в большей степени подходит модель Мамдани, так как в данном процессе обозримость общей картины состояния рисков важнее, чем точность значения.

Однако, в случае с информационными рисками модель Мамдани должна строиться на основе знаний эксперта, которые 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 АС могут различаться. В результате модель Мамдани, построенная по неполным и субъективным экспертным данным, может оказаться неадекватной.

Повысить адекватность модели можно за счет использования объективной информации, к которой относятся результаты измерения значений входов и выходов системы. Способностью извлечения знаний из зарегистрированных данных типа «вход – выход» и аппроксимации исходных зависимостей обладают нейронные сети [10, 12, 13]. Поэтому при оценке информационных рисков предлагается дополнить возможности нечётких моделей за счет использования преимуществ нейросетевых методов.

Тогда нейро-нечёткая сеть будет представлять собой особую эквивалентную форму нечёткой модели. Настройка данной сети может быть произведена на основе обучающей выборки, содержащей значения измерений входных и выходного параметров моделируемой системы, с использованием метода обратного распространения ошибки или других методов,

применяемых для нейронных сетей. По сравнению с обычными нечёткими моделями, нейро-нечёткие сети (ННС) обладают следующими преимуществами:

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

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

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

Методика преобразования нечёткой модели в нейро-нечёткую сеть является достаточно сложной и зависит от типа модели [7, 10, 14, 15].

Поэтому далее рассмотрим процесс преобразования различных элементов нечёткой модели Мамдани в элементы нейронной сети и алгоритмы вычисления производных, применяемые в градиентных методах обучения [12, 13, 15].

2 Преобразование нечёткой модели в нейро-нечёткую сеть

ННС моделирует работу трех блоков: блока фаззификации, блока вывода с базой правил и блока дефаззификации. Рассмотрим особенности реализации указанных блоков в ННС.

В процессе обучения сети выполняется настройка параметров функции принадлежности, с учётом этого необходимо определить производные выходных значений блока фаззификации. Для моделирования функций принадлежности рекомендуется использовать только непрерывно дифференцируемые GRB-функции (гауссова радиальная базисная функция).

Выходное значение GRB-функции со многими входами является близким к 1, только если входной вектор x расположен вблизи от центра функции, задаваемого при помощи вектора c. Данная функция эффективно выполняет оценку сложных условий в нечётких правилах вида:

ЕСЛИ (x_1 близок к c_1) И ... И (x_p близок к c_p) ТО (y близок к y_0).

Возможна также замена кусочно-линейных функций принадлежности на GRB-функции (сохраняя равенство площадей заменяемых функций) и построение нейро-нечётких сетей исключительно на основе GRB-функций.

Вычисление производных $\partial\mu/\partial c$ и $\partial\mu/\partial\delta$, где μ – функция принадлежности, c – центр GRB-функции, δ – величина охвата ветвей GRB-функции, в этом случае является простым.

Различные исследования показали, что обучение нейро-нечётких сетей с кусочно-линейными функциями принадлежности является столь же эффективным, как и в случае сетей с непрерывно дифференцируемыми функциями принадлежности [7, 8, 14, 15]. Единственным условием, ограничивающим возможность применения определённой функции принадлежности в нейро-нечёткой сети, является возможность вычисления производной этой функции и конечное значение производной.

Выходными значениями блока фаззификации являются степени принадлежности входных значений x_i нечётким множествам A_{ij} со своей лингвистической областью определения. Указанные выходные значения одновременно представляют собой степени выполнения подусловий, содержащихся в части ЕСЛИ (...) нечётких правил вида:

$$\text{ЕСЛИ } (x_1 = A_{11}) \text{ И } (x_2 = A_{21}) \text{ И } \ldots \text{ И } (x_p = A_{p1})$$

$$\text{ИЛИ } (x_1 = A_{12}) \text{ И } (x_2 = A_{22}) \text{ И } \ldots \text{ И } (x_p = A_{p2})$$

$$\text{ИЛИ } \ldots \text{ ТО } (y = B_1).$$

Блок базы правил определяет результирующую степень выполнения всего сложного условия (антецедента правила) на основе степеней выполнения подусловий, находящихся в части ЕСЛИ (...) правил, а также на основе типов используемых в этой части логических операторов (И, ИЛИ). В свою очередь, указанная степень активизирует функцию принадлежности B_l, находящуюся в заключении (консеквенте) правил.

Обычно используется метод вывода типа MAX - MIN. Для выполнения операций И, ИЛИ могут использоваться t-нормы и s-нормы либо другие операторы. Каждое правило выполняет активизацию одного из выходных нечётких множеств B_l. Поскольку одно и то же нечёткое множество B_l может активизироваться несколькими правилами, то для получения окончательной формы активизированной функции принадлежности $\mu B_l(y)$ выходного нечёткого множества B_l необходимо выполнить композицию их заключений, для чего, как правило, используется оператор MAX.

Сеть, соответствующая базе правил, содержит нейроны, которые выполняют логические операции. Вычисление производных выходных значений по входным (для этих нейронов) значениям обычно не составляет труда, за исключением случая операторов MAX или MIN, присутствующих в сети независимо либо в составе других операторов.

MAX-нейрон даёт отклик на изменение Δx_i входа x_i в виде изменения Δy выхода, только если:

$$x_i = MAX\left(x_1, \ldots, x_p\right).$$

Изменения других входов не приводят к формированию отклика. Поэтому значение производной по указанному выше входу равно 1, а по всем остальным параметрам равно 0. Аналогично, для MIN-нейрона производные вычисляются по формуле:

$$y = MIN\left(x_1, \ldots, x_p\right), \quad \frac{\partial y}{\partial x_i} = \begin{cases} 1, \textit{если } y = x_i, \\ 0, \textit{если } y \neq x_i. \end{cases}$$

Если несколько входов имеют одинаковые значения, которые при этом являются максимальными (минимальными), то значения производных по каждому из этих параметров будут равны 1.

Входными параметрами блока дефаззификации являются степени активизации $\mu B_l(y)$ нечётких множеств B_l на выходе модели. Структура нейронной сети, соответствующей данному блоку, зависит от выбранного метода дефаззификации и степени сложности этого метода. Простейшим, очень эффективным и часто используемым методом дефаззификации является метод одноточечных множеств.

Одноточечные множества используются в качестве замены выходных множеств, и их расположение совпадает с пиками функции принадлежности либо с их центрами тяжести yB_l. В этом случае значение на выходе модели вычисляется по следующей формуле:

$$y = \frac{\sum_{l=1}^{q} \mu B_l \cdot yB_l}{\sum_{l=1}^{q} \mu B_l}.$$

Производные в такой сети вычисляются просто. В случае если в знаменателе формулы суммарная степень принадлежности элементов yB_l всегда равна 1, то $m = 1$, тогда оператор деления l / m можно отбросить.

Для исследования значимости отдельных правил модели необходимо использовать коэффициенты доверия u_i, принимающие значения в интервале [0, 1], вводя их в те ветви сети, где происходит преобразование выходов правил. Если в результате обучения сети на основе входных и выходных данных о системе значения некоторых коэффициентов оказываются близкими к нулю, то соответствующие данным коэффициентам правила не являются существенными, и их можно исключить. Описанная процедура позволяет выполнить настройку реляционных моделей [10].

3 Применение нейро-нечёткой сети для оценки информационных рисков

Чтобы использовать нейро-нечёткую сеть для оценки рисков информационной безопасности, необходимо определить, какие данные следует подавать на вход системы. Из определения риска информационной безопасности следует, что величина риска R есть функция от потенциально возможного ущерба (стоимости информации, ресурса или актива) A, угрозы информационной безопасности T и уязвимости информационной системы V:

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

Таким образом, входными факторами будут служить экспертные оценки трех нечётких переменных («угроза», «ущерб», «уязвимость»), описанных лингвистическими терм-множествами {очень низкий, низкий, средний, высокий, очень высокий} (табл. 1).

Таблица 1 - Уровни шкалы при оценке угроз, ущерба и уязвимостей

Уровни шкалы	Угрозы	Ущерб	Уязвимости
Очень низкий	Событие практически никогда не происходит	Незначительные потери материальных средств и ресурсов, которые быстро восполняются, или незначительное влияние на репутацию	Уязвимость, которой можно пренебречь
Низкий	Событие случается редко	Более заметные потери материальных активов, более существенное влияние на репутацию или ущемление интересов	Незначительная уязвимость, которую легко устранить
Средний	Событие вполне возможно при определённом стечении обстоятельств	Достаточные потери материальных активов или ресурсов или достаточный урон репутации и интересам	Умеренная уязвимость
Высокий	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	Событие, вероятнее всего, произойдёт при организации атаки	Разрушительные последствия и невозможность ведения деятельности	Критическая уязвимость, которая ставит под сомнение возможность её устранения

Помимо экспертных оценок, дополнительно следует использовать и данные системы обнаружения вторжений, антивирусов, межсетевых экранов о потенциально опасной активности, общем уровне сетевой активности и нагрузки на тот или иной участок автоматизированной системы.

В результате на выходе системы будет получена оценка уровня риска информационной безопасности, которую можно описать расширенным лингвистическим терм-множеством, например,

{пренебрежимо низкий, очень низкий, низкий, ниже среднего, умеренный,

выше среднего, высокий, очень высокий, критический}.

В этом случае шкала измерения уровня информационных рисков будет выглядеть следующим образом:

1) пренебрежимо низкий – риском можно пренебречь;

2) очень низкий – необходимо определить, существует ли необходимость в корректирующих действиях, или есть возможность принять этот риск;

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

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

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

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

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

8) очень высокий – необходимо незамедлительно принять меры по уменьшению риска;

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

Рассмотрим пример применения нейро-нечёткой сети для оценки информационных рисков в автоматизированной системе. Для наглядности на рисунке 1 указаны три входные переменные (угрозы, ущерб, уязвимости). Выходом является риск информационной безопасности.

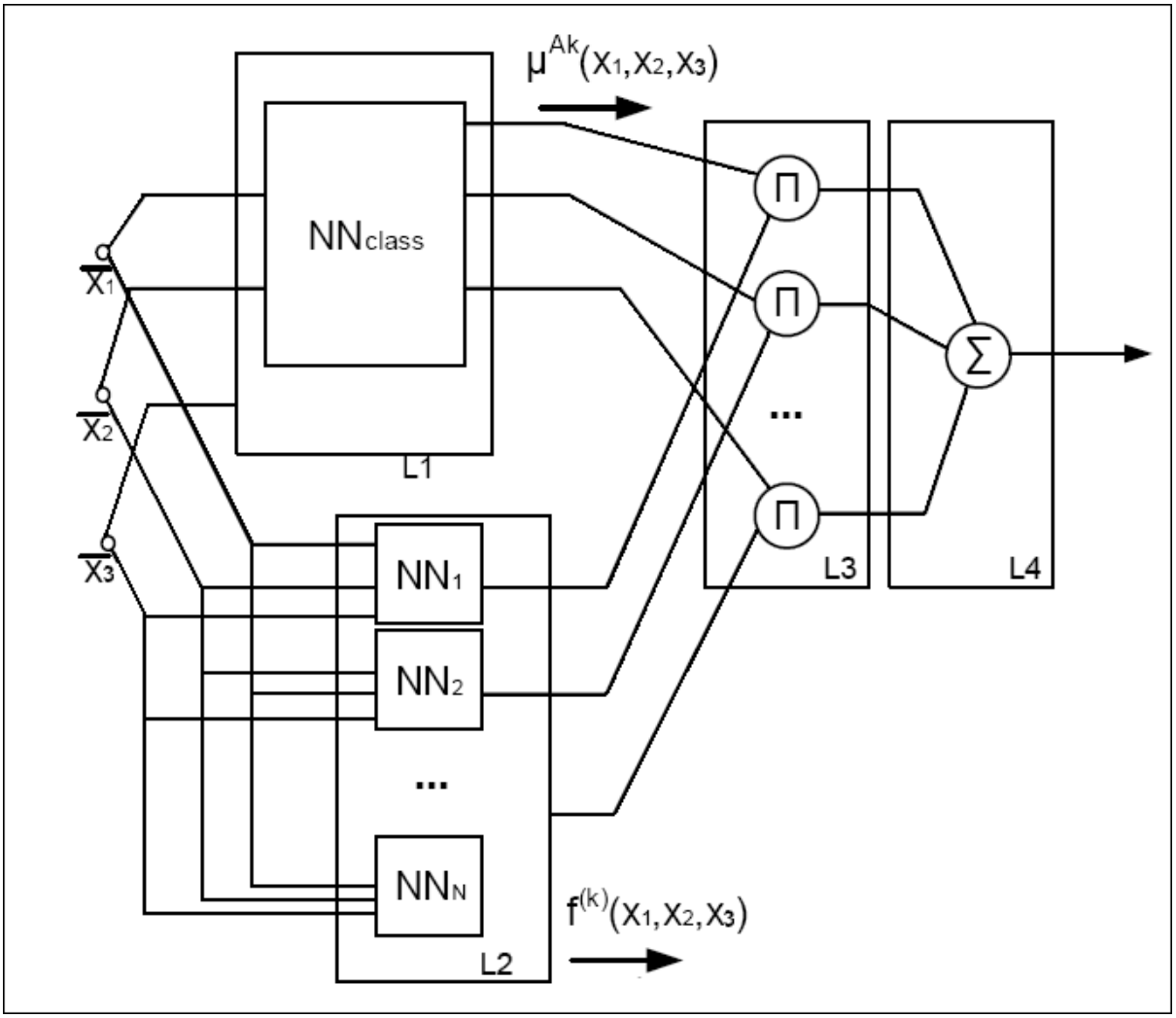

Рисунок 1 - Нейро-нечёткая сеть для оценки информационных рисков в АС

Блок, обозначенный на схеме как NN_{class} (слой L_1), предназначен для решения задачи кластеризации, то есть задания функций принадлежности входных данных пяти нечётким классам. Например, функция принадлежности нечёткому классу «очень низкий» может быть обозначена красной линией (рисунок 2).

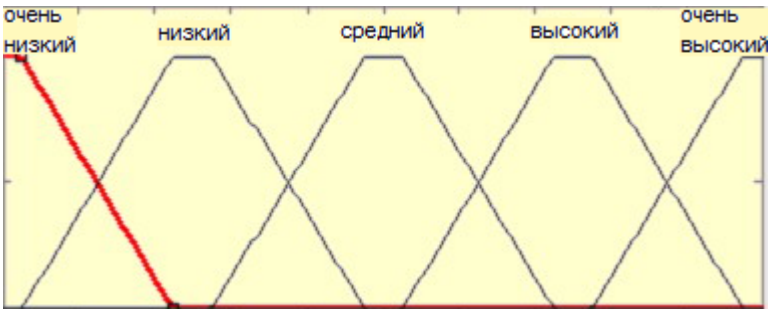

Рисунок 2 - Пример функции принадлежности входных данных

Задача блока кластеризации заключается в разделении множества входных данных (x_1 – угрозы, x_2 – ущерб, x_3 – уязвимости) на 5 нечётких классов (очень низкий, низкий, средний, высокий, очень высокий), каждый из которых выступает в роли условия для одного из нечётких правил ЕСЛИ...ТО. Этот блок реализуется с помощью нейронной сети, имеющей 3 входа (x_1, x_2, x_3) и 125 выходов для всех возможных вариантов сочетаний нечётких классов. Для обучения сети на вход подаются наборы входных данных и одновременно информация о том, к какому классу принадлежит каждое поданное на вход значение. На втором этапе проверяется то, насколько корректно обучена сеть.

Блоки, обозначенные как $NN_1, NN_2, \ldots, NN_N$ (слой L_2), реализуют заключения соответствующих нечётких правил ЕСЛИ...ТО. Например, ЕСЛИ (x_1 – очень высокий, x_2 – очень высокий, x_3 – очень высокий), ТО (y – критический). Для этого также используются нейронные сети. Каждая сеть имеет 3 входа и 1 выход. Эти сети обучаются аналогично, но только после сети NN_{class}, так как имеет существенное значение то, какая сеть должна обучаться по конкретной реализации входного вектора.

Для обучения представленной структуры входные данные должны быть разделены на репрезентативные классы, на базе которых будут формироваться правила. Непосредственное обучение систем будет производиться с помощью рекуррентного метода наименьших квадратов. Структура нейрона при этом будет иметь вид, изображённый на рисунке 3.

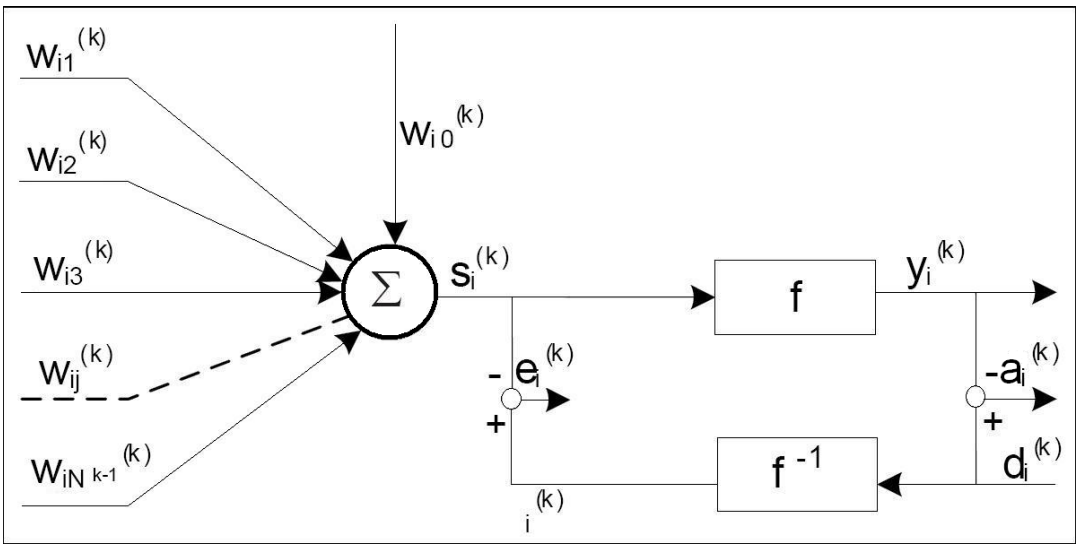

Рисунок 3 - Структура нейрона

Здесь $w_i^{(k)}$ – входные сигналы нейрона, а $w_{i0}^{(k)}$ – пороговое значение чувствительности нейрона. Взвешенная сумма $s_i^{(k)}$ всех входных сигналов нейрона преобразуется с помощью функции активации f, что генерирует выходной сигнал $y_i^{(k)}$. Коррекция обучения может быть выполнена с помощью подачи реального сигнала $d_i^{(k)}$ на функцию деактивации f^{-1}, преобразующей его в значение $i^{(k)}$, добавляемое затем к взвешенной сумме с помощью оператора $e_i^{(k)}$, разницу между реальным и эталонным сигналами определяет оператор $a_i^{(k)}$.

Процесс обучения и функционирования ННС представлен на рисунке 4.

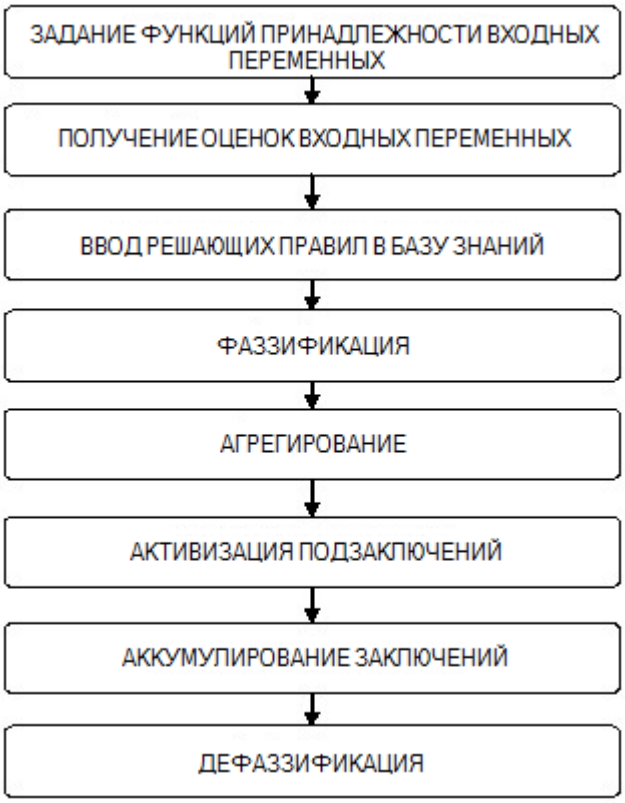

Рисунок 4 - Основные этапы функционирования нейро-нечёткой сети

Рассмотренная ННС обладает способностью к обучению, то есть уточнению оценки риска по результатам сравнения с результатами анализа инцидентов безопасности за прошедший период. Помимо этого, ННС оказывается приспособленной для проведения непрерывного анализа рисков и итерационного выполнения этапа анализа.

Заключение

Представленный прототип нейро-нечёткой сети позволяет не только решать задачи по управлению информационными рисками, но и существенно расширить возможности методов моделирования. Он позволяет снять ограничения на число учитываемых входных переменных и адекватно использовать качественные и количественные оценки входных параметров, полученные от экспертов в области информационной безопасности.

Применение ННС позволяет решить проблему заведомой неполноты информации о составляющих риска и их неоднозначных свойств. При применении ННС отсутствует необходимость создания детальной модели автоматизированной системы для осуществления анализа информационных рисков. Система позволяет агрегировать данные из различных источников и хорошо приспособлена для итерационного непрерывного анализа рисков информационной безопасности.

Список литературы

1. Булдакова Т.И., Миков Д.А. Метод повышения адекватности оценок информационных рисков // Вестник МГТУ. Сер. Приборостроение. Спец. вып. № 5 : Информатика и системы управления. 2012. С. 261-271.

2. Булдакова Т.И., Джалолов А.Ш. Анализ информационных процессов и выбор технологий обработки и защиты данных в ситуационных центрах // Научно-техническая информация. Сер. 1. 2012. № 6. С. 16-22.

3. Buldakova T.I., Dzalolov A.Sh. Analysis of Data Processes and Choices of Data-processing and Security Technologies in Situation Centers // Scientific and Technical Information Processing. 2012. Vol. 39, no 2. P. 127-132. DOI: 10.3103/S0147688212020116

4. Мельников В.В. Безопасность информации в автоматизированных системах. М.: Финансы и статистика, 2003. 368 с.

5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. М.: ИД «ФОРУМ»: ИНФРА-М, 2008. 416 с.

6. Балашов П.А., Кислов Р.И., Безгузиков В.П. Оценка рисков информационной безопасности на основе нечёткой логики // Безопасность компьютерных систем. Конфидент: Информационно-методический журнал. 2003. № 6. С. 60-65.

7. Ярушкина Н.Г. Основы теории нечетких и гибридных систем. М.: Финансы и статистика, 2004. 320 с.

8. Пупков К. А., Егупов Н. Д., Гаврилов А. И. и др. Методы робастного, нейро-нечеткого и адаптивного управления / Под ред. Н.Г. Егупова. М.: Изд-во МГТУ им. Н.Э. Баумана, 2001. 744 с.

9. Mamdani E.H., Assilian S. An Experiment in Linguistic Synthesis with Fuzzy Logic Controller // Int. J. Man-Machine Studies. 1975. Vol. 7, no. 1. P.1-13.

10. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы. М: Горячая линия-Телеком, 2008. 452 с.

11. Takagi T., Sugeno M. Fuzzy identification of systems and its applications to modeling and control // IEEE Transactions on Systems, Man and Cybernetics. 1985. Vol. SMC-15, no 1. P. 116-132. DOI: 10.1109/TSMC.1985.6313399

12. Хайкин С. Нейронные сети: полный курс: пер. с англ. М.: Издательский дом «Вильямс», 2006. 1104 с.

13. Булдакова Т.И. Нейросетевая защита ресурсов автоматизированных систем от несанкционированного доступа // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 5. DOI: 10.7463/0513.0566210

14. Нестерук Ф.Г., Осовецкий Л.Г., Нестерук Г.Ф., Воскресенский С.И. К моделированию адаптивной системы информационной безопасности // Перспективные информационные технологии и интеллектуальные системы. 2004. № 4. С. 25-31.
15. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. М.: Горячая линия-Телеком, 2007. 284 с.

SCIENTIFIC PERIODICAL OF THE BAUMAN MSTU
SCIENCE and EDUCATION
EL № FS77 - 48211. №0421200025. ISSN 1994-0408
electronic scientific and technical journal

Estimating information risks in computer-aided systems using a neuro-fuzzy model

 # 11, November 2013
DOI: 10.7463/1113.0645489

Buldakova T.I., Mikov D.A.

Bauman Moscow State Technical University, 105005, Moscow, Russian Federation
buldakova@bmstu.ru
mikovda@yandex.ru

A modeling problem of information risks in computer-aided systems was considered in this paper. It was shown that a usage of fuzzy models is a promising approach to solving this problem because their development requires far less information about the system. Analysis of various types of fuzzy models was carried out; their main features were emphasized. The Mamdani model was recognized as the most suitable for estimating information risks. Combination of fuzzy and neural network modeling was proposed; that means the creation of neuro-fuzzy networks by transforming the Mamdani fuzzy model to a self-learning neural network, which operates on the basis of fuzzy logical apparatus and fuzzy sets. An example of a neuro-fuzzy network for an assessment of information risks was presented.

Publications with keywords: neuro-fuzzy system, information risks, assessment methods
Publications with words: neuro-fuzzy system, information risks, assessment methods

References

1. Buldakova T.I., Mikov D.A. Metod povysheniya adekvatnosti otsenok informatsionnykh riskov [Method for improving the adequacy of information-risk assessments]. *Vestnik MGTU. Ser. Priborostroenie* [Herald of the Bauman MSTU. Ser. Instrument Engineering]. Spec. iss. no. 5 : *Informatika i sistemy upravleniya* [Information and Control Systems], 2012, pp. 261-271.

2. Buldakova T.I., Dzhalolov A.Sh. Analiz informatsionnykh protsessov i vybor tekhnologiy obrabotki i zashchity dannykh v situatsionnykh tsentrakh [Analysis of data processes and choice of technologies for data processing and security technologies in situational centers]. *Nauchno-tekhnicheskaya informatsiya*. [Scientific and technical information]. Ser. 1, 2012, no. 6, pp. 16-22.

3. Buldakova T.I., Dzalolov A.Sh. Analysis of Data Processes and Choices of Data-processing and Security Technologies in Situation Centers. *Scientific and Technical Information Processing*, 2012, vol. 39, no 2, pp. 127-132. DOI: 10.3103/S0147688212020116

4. Mel'nikov V.V. Bezopasnost' informatsii v avtomatizirovannykh sistemakh [Security of information in the automated systems]. Moscow, Finansy i statistika, 2003. 368 p.

5. Shan'gin V.F. *Informatsionnaya bezopasnost' komp'yuternykh sistem i setey* [Information security of computer systems and networks]. Moscow, Publishing House "FORUM": INFRA-M, 2008. 416 p.

6. Balashov P.A., Kislov R.I., Bezguzikov V.P. Otsenka riskov informatsionnoy bezopasnosti na osnove nechetkoy logiki [Risk assessment of information security based on fuzzy logic]. *Bezopasnost' komp'yuternykh sistem. Konfident: Informatsionno-metodicheskiy zhurnal* [Security of computer systems. Confident: Information and methodical magazine], 2003, no. 6, pp. 60-65.

7. Yarushkina N.G. *Osnovy teorii nechetkikh i gibridnykh system* [Fundamentals of the theory of fuzzy and hybrid systems]. Moscow, Finansy i statistika, 2004. 320 p.

8. Pupkov K. A., Egupov N. D., Gavrilov A. I., et al. *Metody robastnogo neiro-nechetkogo i adaptivnogo upravleniia* [Methods of robust neuro-fuzzy and adaptive control]. Moscow, Bauman MSTU Publ., 2001. 744 p.

9. Mamdani E.H., Assilian S. An Experiment in Linguistic Synthesis with Fuzzy Logic Controller. *Int. J. Man-Machine Studies*, 1975, vol. 7, no. 1, pp.1-13.

10. Rutkovskaia D., Pilin'skii M., Rutkovskii L. *Neironnye seti, geneticheskie algoritmy i nechetkie sistemy* [Neural networks, genetic algorithms and fuzzy systems]. Transl. from Polish. Moscow, Goriachaia liniia-Telekom Publ., 2004. 452 p.

11. Takagi T., Sugeno M. Fuzzy identification of systems and its applications to modeling and control. *IEEE Transactions on Systems, Man and Cybernetics*, 1985, vol. SMC-15, no 1, pp. 116-132. DOI: 10.1109/TSMC.1985.6313399

12. Haykin S. *Neural Networks: A Comprehensive Foundation*. 2nd ed. Prentice Hall, 1999. 823 p. (Russ. ed.: Haykin S. *Neironnye seti: polnyi kurs*. Moscow, Publishing House “Vil'iams”, 2006. 1104 p.).

13. Buldakova T.I. Neyrosetevaya zashchita resursov avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa [Neural network protection of automated systems’ resources from unauthorized access]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2013, no. 5. DOI: 10.7463/0513.0566210

14. Nesteruk F.G., Osovetskiy L.G., Nesteruk G.F., Voskresenskiy S.I. K modelirovaniyu adaptivnoy sistemy informatsionnoy bezopasnosti [Modeling of adaptive information security systems]. *Perspektivnye informatsionnye tekhnologii i intellektual'nye sistemy*, 2004, no. 4, pp. 25-31.

15. Borisov V.V., Kruglov V.V., Fedulov A.S. *Nechetkie modeli i seti* [Fuzzy models and networks]. Moscow, Goryachaya liniya-Telekom, 2007. 284 p.